S. HRG. 116–64

# OUTSIDE PERSPECTIVES ON THE COLLECTION OF BENEFICIAL OWNERSHIP INFORMATION

## HEARING

BEFORE THE

## COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ON

EXAMINING HOW THE COLLECTION OF BENEFICIAL OWNERSHIP INFORMATION AT THE TIME OF COMPANY FORMATION WOULD IMPACT AMERICAN BUSINESSES, BANKS, LAW ENFORCEMENT, AND OTHERS, AND TO EVALUATE THE MOST EFFECTIVE METHODS OF COLLECTION, ITS PERIODIC UPDATING, PRIVACY CONCERNS, AND PROTECTING THE ULTIMATE SECURITY OF THAT INFORMATION

JUNE 20, 2019

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: https://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
37–721 PDF WASHINGTON : 2019

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

| | |
|---|---|
| RICHARD C. SHELBY, Alabama | SHERROD BROWN, Ohio |
| PATRICK J. TOOMEY, Pennsylvania | JACK REED, Rhode Island |
| TIM SCOTT, South Carolina | ROBERT MENENDEZ, New Jersey |
| BEN SASSE, Nebraska | JON TESTER, Montana |
| TOM COTTON, Arkansas | MARK R. WARNER, Virginia |
| MIKE ROUNDS, South Dakota | ELIZABETH WARREN, Massachusetts |
| DAVID PERDUE, Georgia | BRIAN SCHATZ, Hawaii |
| THOM TILLIS, North Carolina | CHRIS VAN HOLLEN, Maryland |
| JOHN KENNEDY, Louisiana | CATHERINE CORTEZ MASTO, Nevada |
| MARTHA MCSALLY, Arizona | DOUG JONES, Alabama |
| JERRY MORAN, Kansas | TINA SMITH, Minnesota |
| KEVIN CRAMER, North Dakota | KYRSTEN SINEMA, Arizona |

GREGG RICHARD, *Staff Director*
LAURA SWANSON, *Democratic Staff Director*

JOHN O'HARA, *Chief Counsel for National Security Policy*
JIMMY GUILIANO, *Professional Staff Member*

COLIN MCGINNIS, *Democratic Policy Director*
PHIL RUDD, *Democratic Professional Staff Member*

CAMERON RICKER, *Chief Clerk*
SHELVIN SIMMONS, *IT Director*
CHARLES J. MOFFAT, *Hearing Clerk*
JIM CROWELL, *Editor*

# C O N T E N T S

## WEDNESDAY, JUNE 20, 2019



## WITNESSES



### ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

# OUTSIDE PERSPECTIVES ON THE COLLECTION OF BENEFICIAL OWNERSHIP INFORMATION

**WEDNESDAY, JUNE 20, 2019**

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
*Washington, DC.*

The Committee met at 10:02 a.m., in room SD–538, Dirksen Senate Office Building, Hon. Mike Crapo, Chairman of the Committee, presiding.

## OPENING STATEMENT OF CHAIRMAN MIKE CRAPO

Chairman CRAPO. This hearing will come to order.

Today the Committee will continue its discussion of how better collection of beneficial ownership information can deter such problems as money laundering, terrorist financing, and sanctions evasion through anonymous shell companies.

I will note at the outset, again, that while the vast majority of anonymous corporations can serve legitimate purposes, this type of incorporation can also be abused to aid and abet all manner of financial crime.

Last month, the Committee heard from witnesses from law enforcement and a banking regulator about what steps the U.S. should take to modernize its beneficial ownership regime and strengthen its enforcement.

Today we have invited a panel to give us some perspective from the business world on this difficult subject. With that, I would like to welcome Mr. Greg Baer, CEO of the Bank Policy Institute, whose members confront the ownership issue at account openings; Ms. Karen Harned of the National Federation of Independent Business, which speaks to the concerns of the hundreds of thousands of small businesses it comprises; and Mr. Gary Kalman of FACT, or the Financial Accountability and Corporate Transparency Coalition, an alliance of organizations that is working toward ending the use of anonymous shell companies as vehicles for illicit activity and increasing transparency for more informed tax policies.

During last month's hearing, our witnesses assessed the need to eliminate anonymous corporations by means of collecting beneficial ownership information to protect the U.S. financial system, its national security, and citizens from harm.

The Committee learned that according to estimates from the U.N. Office on Drugs and Crime, there is more illicit money flowing through the global and U.S. financial systems than ever before.

The U.N. estimate found that global illicit proceeds now total some $2 trillion and the proceeds of crime in the United States are over $300 billion.

All of that illicit money has several things in common: somebody has to make it, hide it, move it, clean it, and use it.

Despite efforts of U.S. law enforcement and the heavy U.S. regulatory framework of the Anti–Money Laundering/Bank Secrecy Act regime, which includes a mandate to collect beneficial ownership upon opening of a bank account, criminal elements in this country and from other countries can and do exploit weaknesses in the current U.S. corporate formation system to hide identities and illicit assets behind anonymous corporations.

In our last hearing, FinCEN Director Blanco testified that a necessary second critical step in closing this national security gap is collecting beneficial ownership information at the corporate formation stage.

In agreement with Blanco, FBI Financial Crimes Chief D'Antuono cited the need for a central repository to allow law enforcement to store and share the information.

OCC Senior Deputy Comptroller Gardineer also emphasized the need for a centralized database, so that businesses could provide, update, and verify beneficial ownership information. Importantly, she also recommended that foreign entities be required to report ownership information either at the time of State registration or upon establishing an account relationship with a U.S. financial institution.

Our hearing today comes at a time when bipartisan support for beneficial ownership legislation continues to build.

Last week, the House Financial Services Committee marked up H.R. 2513, the Corporate Transparency Act of 2019, which was reported out of committee on a 43–16 vote. And on the very same day, a bipartisan group of my Senate colleagues here on the Banking Committee circulated draft legislation, presently called the ILLICIT CASH Act, which provides a number of important measures to modernize the AML/BSA regime and to address the collection of beneficial ownership information.

I especially want to acknowledge the hard work of Senators Cotton, Warner, and Jones and their staffs, the work that they have put in over the last year on this effort, which the Committee as a whole shall take close notice of moving forward.

Each of these legislative vehicles share some of the broad themes brought out in the Committee's first hearing, such as a requirement for the collection of beneficial information at the time of a company's formation, periodic updating, storage of that information in FinCEN's secure database, and limiting access to that database to Federal law enforcement and its qualified State partners.

We turn now to our panel for their perspectives on the important issues underlying further collection of beneficial ownership information and how that might impact banking and business operations, including concerns that arise with regard to privacy and liability issues.

Given the facts presented to the Committee thus far, there are strong law enforcement and national security reasons supporting additional collection of beneficial ownership information.

Hopefully, our witnesses will provide some insight on how to collect this information at minimal cost and burden to businesses.

Now is the time to critically examine how the AML/BSA regime can be modernized and, in particular, how businesses can work effectively with Government to efficiently provide beneficial ownership information that will in turn provide a high degree of usefulness to combat terrorism and crime.

Senator Brown.

**OPENING STATEMENT OF SENATOR SHERROD BROWN**

Senator BROWN. Thank you, Mr. Chairman, for calling this important hearing, the latest in a series of hearings in this Committee on our Bank Secrecy Act and anti–money-laundering reform efforts and on critical changes to U.S. beneficial ownership laws to combat abuses by owners of anonymous shell companies, some of whom have been exploiting our system for criminal purposes for years, as we know.

Unlike in most areas of disclosure and transparency law, where the U.S. has led the way, on this issue we have long lagged behind other jurisdictions and failed to require uniform and clear ownership information for firms at the time of their incorporation.

It is critical to law enforcement. In the U.S., they have to spend precious time and resources issuing subpoenas, chasing down leads to secure even the most basic information about who actually owns a company. That makes no sense and must change.

Treasury's 2018 Money Laundering Risk Assessment estimates that some $300 billion in illicit proceeds from domestic financial crime is generated annually, making these funds ripe for money laundering through the system.

Criminals abuse the financial system to launder funds gained through narcotics trafficking, organized crime, the sale of counterfeit goods, Medicare fraud, Medicaid fraud, and other criminal activities. Much of the dirty money is funneled through anonymous shell corporations.

As many of us have observed before, none of the abuses we will discuss today—drug trafficking, human trafficking, Medicare fraud, money laundering—are victimless crimes. None of them are victimless crimes.

Money laundering for drug cartels has a direct line to the opioid crisis in Ohio, where cartel actors have been destroying thousands of families. Human traffickers who exploit the misery of runaways in truck stops, especially in northwest Ohio at the intersection of major interstate highways and across the country, use the financial system to launder their profits.

Medicare fraudsters cost the taxpayers $2.6 billion in 2017, according to the HHS Inspector General, and tarnish the reputation of this lifeline for seniors.

That is why anti–money laundering and beneficial ownership laws are so critical. They protect the integrity of our financial system. They provide critical intelligence to law enforcement.

Under Treasury's recent customer due diligence rule, bankers must already secure some of this information from account holders when they open accounts, and while banks must continue to play

a key monitoring role, it is important we require companies to provide basic information on their ownership when they are formed.

In today's hearing, we will hear from the Financial Accountability and Corporate Transparency Coalition—thank you for joining us—and from the banks on the many reasons to pursue these reforms, including the transparency, anticorruption and anti–illicit financing benefits that such reforms would offer.

I ask consent, Mr. Chairman, to include a number of reports and letters from outside stakeholders into the hearing record.

Chairman CRAPO. Without objection.

Senator BROWN. Thanks.

And we will hear from NFIB, some of whose members have expressed concern, about the paperwork burden of providing even simple ownership information: name, address, copy of a current passport or driver license.

Requiring companies' ownership information, storing it in a secure Federal database like FinCEN's, alongside its bank secrecy information, would help address longstanding problems for U.S. law enforcement. It would help them investigate cases involving counterterrorism, drug trafficking, Medicare fraud, human trafficking, and other crimes. It would provide ready access to this information under long-established and effective privacy rules.

Without these reforms, criminals, terrorists, rogue Nations, even, will continue to use layer upon layer of shell companies to disguise and launder illicit funds. That makes it much harder, surely, to hold bad actors accountable.

Chairman Crapo and I agree we must move forward to require complete ownership information, not front men, not from those companies on behalf of those who will pull the strings from behind the curtain, but the actual owners of these companies.

We can do this simply. We can do it efficiently and effectively, without unduly burdening small businesses or others.

Updating and strengthening our anti–money laundering and beneficial ownership laws will give us a 21st century system to combat these crimes.

Criminals have long been revising, adjusting, and amending their tactics to circumvent and evade those laws, often staying a step ahead of the sheriff. That is why we must move.

Thank you.

Chairman CRAPO. Thank you, Senator Brown.

Mr. Baer, we will begin with your testimony as CEO of the Bank Policy Institute. Next, we will turn to Ms. Harned for her statement on behalf of the National Federation of Independent Businesses and conclude with Mr. Kalman for his statement on behalf of the Financial Accountability and Corporate Transparency Coalition.

I want to thank you all for your written testimony. It is very helpful to us and will be made a part of the record.

The Committee has also received several written statements in support of today's proceedings that, absent any objection, will also be made a part of today's record. The eight statements I am referring to are submitted from the American Bar Association, the National Fraternal Order of Police, National District Attorneys Association, National Association of Manufacturers, the Consumer

Bankers Association, the National Association of federally Insured Credit Unions, the Independent Community Bankers of America, and the Credit Union National Association.

Without objection, those will be made a part of the record.

Finally, I want to ask our witnesses to remember to honor and follow the clock and remember your 5 minutes for your initial presentation and our Senators to remember your 5-minute limitation on your questioning period.

We will have votes called at some point that may cause us to have to move forward more quickly.

With that, Mr. Baer, please begin.

**STATEMENT OF GREG BAER, CEO, BANK POLICY INSTITUTE**

Mr. BAER. Chairman Crapo, Ranking Member Brown, Members of the Committee, my name is Greg Baer, and I am the CEO of the Bank Policy Institute.

BPI is a nonpartisan research and advocacy group, representing the Nation's leading banks. We strongly support legislation to end the use of anonymous shell companies and hope this hearing will prompt congressional action.

Anonymous shell companies are a key method used by criminals to hide assets for a wide range of illicit activities, including human trafficking, terrorist financing, money laundering, and kleptocracy. All too often, criminal investigators have hit a dead end when law enforcement encounters a company with hidden ownership and lacks the time and resources to peel back the many layers of secrecy. And the more sophisticated and sinister the criminal, the more layers there generally are.

In his testimony, Gary Kalman presents numerous cases that illustrate that this concern is very real, not hypothetical.

Legislation to allow law enforcement to look beyond the corporate veil, including the draft recently circulated by a bipartisan group of Senators on this Committee, would make our country safer and enhance the reputation of the United States as a country that fights against, not harbors, the worst people in the world.

It has been a pleasure to join on this issue with the Fraternal Order of Police and hundreds of former law enforcement and national security officials who have attested to its importance.

Currently, the Nation's banks assist law enforcement by determining the ownership of companies that open a bank account and then using this information to monitor the account for activity. However, that regulatory regime has been no substitute for beneficial owners of legislation.

First, it does not cover shell companies that never open a bank account because they conduct no business in this country. These pure shell companies are virtually invisible. Second, while banks gather ownership information from their customers, they do not disclose it to law enforcement. Law enforcement learns of it only if the bank identifies suspicious activity. Legislation would cure these two problems.

Furthermore, for banks and importantly for the business clients who must actually provide this information, legislation would centralize the ownership identification process and make it more efficient.

Two primary concerns have been expressed about such legislation—burden and privacy. But let us consider a few facts. First, the draft legislation requires a business owner to disclose only the most basic of information: name, address, date of birth, and some form of ID such as a driver's license or passport number. That is all. And since the great majority of American businesses have only one owner, it would be generally provided by and about one person.

Second, as noted, this information is generally already provided any time a company opens a bank account. Of course, any legitimate U.S. business, large or small, probably has a bank account because any business that earns money or pays expenses or employs people must have a bank account. Thus, for legitimate businesses, legislation would not increase reporting obligations and would likely decrease them.

Third, with respect to privacy, this basic information is already known to various arms of the Government, including the DMV and the IRS. Unauthorized disclosure by law enforcement or a bank employee would come with severe penalties, and banks have a record of keeping such information secret. A FinCEN directory should not worry legitimate business owners. It should, however, worry a drug trafficker or kleptocrat using a shell company to hold a multimillion-dollar condominium in West Palm Beach.

Most small business owners in fact are willing to share information to help keep our country safe. According to a poll conducted by Morning Consult on behalf of BPI released today, small business owners support measures to end anonymous shell companies. Of those who had an opinion, 75 percent of small business owners supported requiring business owners to provide their personal information when forming their company to help close this loophole in U.S. law. Furthermore, two-thirds of small business owners stated that providing their personal information when registering their company would not be burdensome.

Last, it is worth noting that the U.K., EU, and enumerable other Nations have adopted such a director without damage to their small businesses or any other unintended consequences. We can learn from their example.

The stakes here are very high, and the time has come for the United States to act. We look forward to working with you on this important issue, and I look forward to your questions.

Chairman CRAPO. Thank you very much.

Ms. Harned.

**STATEMENT OF KAREN HARNED, EXECUTIVE DIRECTOR, SMALL BUSINESS LEGAL CENTER, NATIONAL FEDERATION OF INDEPENDENT BUSINESS**

Ms. HARNED. Chairman Crapo, Ranking Member Brown, and Members of the Committee, on behalf of NFIB's 300,000 small business members, I appreciate the opportunity to testify today.

NFIB opposes proposal likes the Corporate Transparency Act of 2019 and the ILLICIT CASH Act. When NFIB surveyed its membership on this legislation last year, 80 percent of respondents opposed Congress requiring small business owners to file paperwork with the Treasury Department reporting on beneficial ownership.

According to the 2016 NFIB Small Business Problems and Priorities report, unreasonable Government regulation is the second most important problem that small business owners face.

Compliance costs, difficulty understanding regulatory requirements, and extra paperwork are the key drivers for their regulatory burdens. NFIB's research shows that the volume of regulations poses the largest problem for 55 percent of America's small employers.

The legislation you are contemplating would impose mandatory reporting requirements on those least equipped to handle that, America's small business owners. Both bills would mandate that every corporation or LLC with 20 or fewer employees and less than $5 million in gross receipts or sales file beneficial ownership information with FinCEN upon incorporation and periodically update that information.

Either the small business owner herself or the accountant or attorney that she pays is going to have to ensure these documents are filed. One new paperwork requirement may not sound that burdensome to someone who does not run a small business, but it is quite a different story for the individual just starting a business or the small business owner who is adding this form to the stack of forms he must already know about, fill out, and file.

Moreover, for many small business owners who have no idea what FinCEN is, there is a strong likelihood that they will just ignore the information request, and many are going to view it with great skepticism.

Every year, NFIB receives countless calls asking about the Census Bureau's Annual Business Survey and that form, whether that small business owner really needs to take the time to fill it out and provide the information required. It is unrealistic to assume that small business owners will simply submit personal information, including a passport or driver's license and date of birth, to a Government agency that none of them have never heard about.

A well-meaning small business owner who fails to file because she never finds out about this new requirement or is skeptical about the legitimacy or appropriateness of the form would be exposed to civil penalties of $10,000 and criminal penalties of up to 3 years in prison.

These proposals also require small business owners to determine and report who is and is not a beneficial owner. That is actually not a quick and easy ask for the typical small business owner. Calculating who owns 25 percent or more of a business should be straightforward, but determining who exercises substantial control or receives substantial economic benefit from a business many times will not be.

Imagine the small family run restaurant employing 10 persons. Their manager has been with them since the opening. The financial owners of the restaurant trust her 100 percent in all operations of the business. The owners are recent empty nesters, and they like to travel. As a result, the manager has complete control over the restaurant's operations for several weeks a year. She also receives an annual bonus that is strictly based on the gross receipts of the business.

Does she exercise substantial control, or does she receive substantial economic benefit from that business under either or both bills making her personal information, including driver's license and passport number, reportable? How is an average small business owner to determine the answer to that question on their own? And is that even a question that an outside lawyer that they pay could even be able to answer with the kind of certainty needed to ensure they are not subject to civil money penalties and years in prison for the wrong answer?

NFIB also has serious privacy concerns with these proposals, which are antithetical to the current statutes on the books, that even for sensitive kinds of national security activities require the Federal Government to focus its investigative interest in someone in particular, some business in particular, or some account in particular before compelling a bank or other business to produce relevant information.

Finally, NFIB questions whether imposing significant and costly beneficial ownership reporting requirements on America's small business owners, like your local independent grocer to dry cleaner, will stop or deter money laundering or other illicit activities.

NFIB opposes this legislation because it would impose even more regulatory burdens on small business.

Thank you for the opportunity to testify, and I look forward to answering your questions.

Chairman CRAPO. Thank you.

Mr. Kalman.

**STATEMENT OF GARY KALMAN, EXECUTIVE DIRECTOR, FINANCIAL ACCOUNTABILITY AND CORPORATE TRANSPARENCY COALITION**

Mr. KALMAN. Chairman Crapo, Ranking Member Brown, distinguished Members of the Committee, on behalf of the FACT Coalition, I thank you and appreciate the opportunity to talk about a foundational reform in the global anticorruption movement.

FACT Coalition is a nonpartisan alliance of more than 100 State, national, and international organizations working to combat the harmful impacts of corrupt financial practices.

There is now overwhelming data detailing the use of anonymous companies for money laundering and other criminal purposes. In its 2017 "Tariff Financing Briefing Book", the Foundation for the Defense of Democracies found that anonymous companies are being abused by rogue Nations like Iran and sanctioned organizations like Hezbollah.

The anticorruption group Global Witness found that a U.S. company had contracted with the Pentagon to supply services to troops in Afghanistan and was secretly owned by interests associated with the Taliban. We were literally supplying funds that could be used to purchase guns and other weapons aimed at our troops.

These chilling reports are why nearly 100 civilian and former military national security experts signed a recent letter to Congress in support of collection of beneficial ownership information.

Additionally, in the 2018 National Money Laundering Risk Assessment, the U.S. Department of Treasury wrote that the nature of synthetic drug trafficking has changed with the rise of China as

a primary supplier if fentanyl. U.S. Drug Enforcement Agency has determined that there is an Asian version of the Back Market Peso Exchange with goods being exports to China by U.S. front companies as payment for drugs.

Anonymous companies are also used to undermine markets and disrupt legitimate businesses. There are numerous examples in which anonymous companies disrupt supply chains, fraudulently compete for contracts, and engage in illicit commerce through the selling of counterfeit and pirated goods.

Not surprisingly, when businesses were asked, without context, if they would support additional regulation, they did not.

However, entrepreneurs understand and manage risk every day. When the organization Small Business Majority asked small business owners if they were more concerned about the risks and burdens of reporting ownership of their businesses or the potential loss of contracts to anonymous companies, 76 percent said that they were more concerned about losing contracts than about the regulatory burdens.

New data and negotiations over a decade with multiple parties have helped to make current proposals more workable and compliance easier for businesses.

An analysis of data collected by the British Beneficial Ownership Directory found that the average number of owners per business in the U.K. is 1.13, and the most common number of owners is one. According to the U.S. Small Business Administration, approximately 78 percent of all businesses in the United States are nonemployer firms, meaning there is only one person in the entity. This suggests that the experience of the U.S. would be similar to that of the U.K.

To address privacy concerns, current proposals place information at FinCEN. FinCEN is our Nation's financial intelligence unit with the responsibility of housing and reviewing data to protect our financial system. The FinCEN directory has strict limitations on who can access the information and how that information can be used. The directory is accessed through a physical portal, meaning that a local police officer could not logon during a routine traffic stop. Users must be trained and certified and must undergo a background check. All searches must be done as part of an ongoing investigation, and every file that is reviewed is logged so that there is a record of who accessed what information. Misuse of that information is a criminal act.

Like all laws, there would be penalties for violating this law; however, under all the current proposals in Congress, negligence is not a punishable offense. That means that honestly forgetting to add a family member who joins a business is not punishable. In fact, the standards in the bills provide greater protections for filers against errant prosecutions than the American Bar Association's model guidelines in this area recommend.

The U.S. is particularly vulnerable to the abuses of anonymous companies. The most recent financial secrecy index ranks the U.S. second only to Switzerland among the world's secrecy jurisdictions. Progress in the rest of the world means the U.S. is likely to become an even more attractive haven for illicit cash unless we act.

We hope this hearing provides Members with an opportunity to better understand the dangers posed by anonymous companies and move swiftly to address them.

I am happy to answer your questions.

Chairman CRAPO. Thank you, Mr. Kalman.

I will begin with a question relating to the storage of this information if it is mandated to be collected, and I realize there is some discussion about whether this new regime of data collection should be adopted.

But assuming that there will be some kind of beneficial ownership storage requirement, there has been some discussion about whether the central repository, if you will, should be FinCEN, whether it should be the IRS, whether it should be banks, whether it should be the States.

Could each of you just quickly, please, tell me if you have an opinion on where that function should be located?

Mr. Baer.

Mr. BAER. Thank you, Senator.

I think FinCEN is the obvious and best candidate. They have experience with this type of information. They have the database.

Banks are not really an option because this would include filings for companies that, again, do not have bank accounts and are simply shell companies. So the bank would not even be aware that that company existed, and it certainly would not be its client.

I think the IRS is problematic on a variety of fronts and opens up a bunch of new issues.

FinCEN seems perfectly well suited to do this, and most importantly, law enforcement is used to go into FinCEN if they need data.

Chairman CRAPO. Thank you.

Ms. Harned.

Ms. HARNED. I cannot really speak to an opinion on who should house it. Again, I would say, like I did in my testimony, that our members do not know who FinCEN is, and our bigger issue is just the access to the information and ensuring that it is secure.

Chairman CRAPO. All right. Thank you.

Mr. Kalman.

Mr. KALMAN. We also would agree that FinCEN is the right repository. We think that it is a good mix of protecting the privacy but allowing law enforcement the appropriate access that they need in a timely fashion.

Chairman CRAPO. All right. Thank you very much.

And there has been some comment also today that the United States is lagging far behind in terms of having the kind of structure to deal with beneficial ownership on a global basis.

How do most of the other Nations who are ranked as having a more effective system operate? I guess the question I am asking is, Do they collect the same level of data and so forth, and do they have a central repository? And how does that work? Any of you, just jump in on that.

Mr. KALMAN. Just quickly. So the first directory that is sort of up and running is in the U.K. It is a public directory, actually. They do collect similar information.

There are some exceptions to the publication of that data where there is an appropriate reason to do so.

The European Union has voted that all 28 member States are to have a directory up in the next few years, and that also includes the Economic Zone. So that is the additional three countries. The U.K.'s Crown dependencies and the overseas territories are also in line to bring on beneficial ownership, and it is all very similar information.

Chairman CRAPO. All right. Thank you.

I will let you choose among yourselves who wishes to respond to this question. Banks already generate and file sensitive suspicious activity reports, SARs, and under the current CDD rule, they already collect some of this beneficial ownership information at the account opening. How do banks treat this information and keep it private, and how would this legislation keep similar information private?

Mr. Baer.

Mr. BAER. Sure, Senator. I mean, with respect to SAR filings, there is a whole special regime just around that act, where a bank is criminally prohibited from disclosing the existence of that SAR to anyone, including the subject of the SAR.

With respect to the information gathered in the account opening process, which includes this type of information and a lot of other information, historically you have the Right to Financial Privacy Act, which is really more directed at keeping it private from Government, but also under the Gramm–Leach–Bliley Act, there was actually a title of that law that established important privacy protections for U.S. citizens and bank account holders. And under that, banks not only have to keep that private, but they have to, under the FTC safeguards rule, have a demonstrated way of ensuring that it is safe and sound.

Chairman CRAPO. All right. Thank you.

Senator Brown.

Senator BROWN. Thank you.

Mr. Kalman, I want to follow up on your answer to Senator Crapo about other countries. Understanding what you said, that we lead in a number of things, perhaps on combating terrorism, financing terrorism and drug trafficking and other crimes, but do not on this, and that Britain especially has moved, the current gaps in U.S. laws, how do those affect U.S. efforts to enlist international partners in this?

Mr. KALMAN. Actually, in several ways. Thank you for the question.

Let me actually say there are numerous law enforcement officials that have told this story in various settings, where they go overseas to work with our partners to try and help them negotiate and try and strengthen anti–money-laundering laws or to train them on how to do these investigations.

Inevitably, at the end of those trainings, people come up to them and say, "Hey, could you help me with an investigation? We have traced the money back to, say, Delaware," or one of the other States in the country. And they are very embarrassed that they cannot help them because there is no information.

So, in short, it not only undermines our ability to find this information, but it also inhibits our ability to work with other Nations and make this more of a global norm.

Senator BROWN. Thank you.

Let me ask you about real estate. The abuse of shell companies obviously is a real problem. Some of them, we have seen the involvement of Russian oligarchs and other authoritarians. There are pools of money flowing into cities and buying up U.S. real estate. These investments do more than just allow fraudulent actors to park illicit money into our country. They also potentially—and we have seen examples of raising prices and pushing out illegitimate buyers.

Explain how creating national beneficial ownership disclosure requirements and a shared database would strengthen efforts to counter that kind of illicit foreign money flowing into U.S. real estate.

Mr. KALMAN. The real estate markets are particularly vulnerable. They are obviously large attractive ways of investing money. It not only drives up prices, but is also drives out small businesses that actually rely on people living in those entities. And when these buyers come in, they do not buy it to live there. They are not residences. They are actually using them as bank accounts, and so entire neighborhoods are being hollowed out. And you can see that in New York and Miami.

If there was a crime to file beneficial ownership information, then the banks would be able to check that database. If there were suspicious activity and law enforcement figured it out, then they would be able to go and check those registries.

What is interesting is the geographic targeting orders issued by FinCEN showed that 30 percent of the transactions covered by the geographic targeting orders involved people with suspicious activity reports. So this information would be valuable to law enforcement.

Senator BROWN. Thank you.

Ms. Harned, thank you for your concerns representing your 300,000 members. I have a couple of comments, and then I want to ask how we can—this is pretty clearly a bipartisan effort, and we want you on board, if at all possible, making easier particularly for people, maybe in both parties, but especially Republicans to support this effort.

According to the Census Bureau, 94 percent of firms with paid employees have fewer than five owners, the kind of membership I know that you thrive on. As you know, we are asking for name, address, date of birth, nationality, driver's license, or passport.

Considering that the example you gave us of the restaurant owner couple and then the woman who got the bonus when she was doing such a good job, that only she would have to only file, name, address, date of birth, nationality, driver's license, or passport. How do we mitigate your concerns on this so that the burden—I know there is always one burden, another burden, another burden, but this is pretty simple. It is in our national interest. It is to help all of us be more safe, and to some of us, it does not seem like a huge burden. Walk through what we could do to make you want to support something like this.

Ms. HARNED. Well, I just think there are still so many questions with this legislation, quite frankly. I mean, again, you are starting with the premise that our members are not going to support a new paperwork requirement. I mean, we must start with that premise.

But then moving forward from there—you know, I am here for the law-abiding, 90-plus percent members or businesses that are not—you know, the vast majority that are not criminals. We are very concerned that this is very broadly tailored. It is more of just let us make everybody report and not really going after——

Senator BROWN. Well, can you identify your 1/100th of 1 percent of NFIB members who might be terrorists?

Ms. HARNED. I do not think we have any.

Senator BROWN. Of course, you cannot, no.

Ms. HARNED. Yeah.

Senator BROWN. But my point is that that is the way these things work. Keep going.

Ms. HARNED. I guess my point also is even the bankers during the CDD rule comment phase noted that this was going to be very hard for small business owners, and when you are looking at things like gifting a business to a family member, a multigenerational business, and forgetting to fill out the form, you are slowly transitioning the son or daughter to become more of an owner of the business, take more ownership, a divorce, there are so many things that can happen that are going to trigger this. If you get that answer wrong, and it is a matter of enforcement discretion whether or not you are going to see a civil penalty and/or jail time.

I just think at the end of the day, it seems like a very big hammer for a very little nail. I am not doing a good job of my analogy, but it is just such a broad—making all the small business owners report, rather than just when they are—as we currently have under the CDD rule, the bank is doing the reporting. It is just very hard for our members because, again, when you are asking them for this information—let us say it is done through the Secretary of State through a letter. They are going to get this letter, and a lot of them are going to be like—they might freak out, quite frankly. They might wonder, "Who is FinCEN? Do I really need to do this?" I mean, there is just going to be a lot of—a lot of questions, and I just am very concerned there is going to be rampant noncompliance.

Senator BROWN [presiding]. I would hope if this passes—and, again, it has got a lot of bipartisan interest—if it passes that you would help us in allaying some of the fears of your members of your constant "preaching," for want of a better term, or educating that Government regulation is always evil and that Washington is always a bad actor, that you would—and to help make America great, perhaps you would help to teach people that sometimes to fight terrorism, maybe this is what you have to do.

But we will continue to work with you.

Senator Reed.

Senator REED. Thank you, Mr. Chairman. Thank you, Mr. Ranking Member, to be accurate, and the lady and gentlemen, thank you for your testimony.

Mr. Kalman, I think we understand that this is a grave national security issue. Can you give us an idea of what you believe the most important tools would be for us to provide to deal with this issue of beneficial ownership?

Mr. KALMAN. Thank you for the question, Senator.

Just yesterday in the Judiciary Committee, Adam Szubin, the former Acting Treasury Secretary and Under Secretary for Terror Finance, said that collection of the beneficial ownership information is perhaps the single most important thing that Congress can do to combat the problems associated with anonymous companies and national security. Simply collecting this information and putting it in an accessible place for law enforcement and for the financial institutions that are seeking to protect our financial systems seems like the most important thing we can do.

Senator REED. Very good.

And we are seeing this problem in terms of infiltrating our industrial base, as you pointed out. The Afghan Taliban company that was supplying our forces to fight the Taliban is a bitter irony. We are seeing it in our political space where we do not know some of the corporations who are funding campaigns through super PACs. We are seeing it in terms of potentially media ownership or other aspects that face the social fabric.

So this is an issue that is profound. I would hope you would agree.

Mr. KALMAN. I would.

Senator REED. And I think we can agree on the dimension of the problem. We might differ on solutions, but this is not going to go away. It is going to get much, much worse.

In that regard, there is a related issue in my mind—I mentioned it to Senator Brown—is that a lot of these sham companies are using Bitcoin and other devices to, again, undermine our economy in other respects.

Mr. Kalman, any ideas about improving transparency related to these currencies?

Mr. KALMAN. Thank you for the question.

Two things, I guess I would say on that. First, I should say I am not an expert on cryptocurrency, just to be clear, but as far as I understand, there is multiple steps, one of which is there are entities when you first purchase the cryptocurrency. Right now, anonymous companies can get into the system. Once they are in there, I am less familiar with how it operates, but just to literally get into the system, an anonymous company can do that.

The second thing I would say is it is also yet another reason to pass legislation as opposed to just relying on the CDD rule. Cryptocurrencies are not going through banks, and so it creates another vulnerability.

Senator REED. I think interesting is just the announcement that Facebook is proposing to create a cryptocurrency, Libra. They have 2 billion members all across the world. There are no national lines. The potential—and again, 10 years ago, if you talked about this nice little application where you could talk to your buddy, you would not assume it would gather so much power as it has.

But there is a real danger in terms of the economy that the dollar could literally be displaced as the world currency if this

cryptocurrency spreads rapidly, and that raises profound issues. I think the Committee is going to be prepared to grapple with them, but both in terms of—I think we have two issues here. We have got to fix this beneficial ownership problem. All the evidence that we have seen shows it is a vulnerability that is significant.

If you marry that up now with a worldwide cryptocurrency which essentially eliminates the Federal Reserve as a moderator of economic policy in the United States, we will have a new world economy and world power structure that we have never anticipated, and that could happen, the way things move, within months, or years, not within decades.

So thank you all for your comments today.

Thank you, Mr. Chair.

Senator BROWN. Thank you, Senator Reed.

As you suggested, we have all been talking about this, and the Chairman has called a hearing on cryptocurrency, on this issue, I believe in July.

Senator Warner.

Senator WARNER. Thank you, Senator Brown.

Let me first of all—I appreciate you and the Chairman bringing this issue up and recognizing the broad bipartisan support. Senator Cotton, Senator Jones, and I have been working on legislation called the ILLICIT CASH Act that at least is a starting point that I hope you and the Chairman would look at.

I also want to pick up a little bit where you left off. I find it remarkable, Ms. Harned, that any business organization would have such a knee jerk reaction. I think the vast majority of NIFB businesses in Virginia know that there is abuse, know that there are shell companies that are being manipulated.

We are not talking about putting in place requirements for financial records. We are looking for name, ID, pretty basic stuff.

Mr. Kalman, your testimony has done a great job on how this approach can strengthen also about national security and fighting terrorism, but let us face it. This would also have implications well beyond national security and fighting terrorism. How can this, the kind of database we are creating in our legislation and other proposed legislation, take on issues around sex trafficking, opioids, tax evasion, counterfeit materials, all concerns that most small businesses have?

And I would point out—and maybe some of the groups have not done their full research—that all independent analysis shows that America is at the absolute bottom of the pile, second from the worst of any Nation in the world, in having too much secrecy in our laws.

So I would be happy to introduce the representative from NFIB to Virginia businesses who actually, I think, would recognize if we do this in an appropriate way—and I think our legislation tries to take those small businesses concerns more than maybe what is going on in the House—that they would do their patriotic reporting.

With FinCEN, you have an organization that is not, by any means, a gotcha-type organization. They have worked well with people. They try to make sure if there is a forgotten filing or missed filing, you do not move to penalty. Some of the over-the-top

rhetoric about, well, you are going to get put in jail is either an evidence of ignorance or really not very helpful.

So, Mr. Kalman, if you could speak about this beyond some of the national security and terrorism issues, I would be grateful.

Mr. KALMAN. Sure. Thank you for that question.

The anti–human-trafficking organization Polaris joined our coalition last year specifically because of the connection and the nexus between human trafficking and anonymous companies. In fact, they did a study where they looked at 6,000 illicit massage businesses and actually did a deep dive into illicit massage businesses in Virginia and found that in over 80 percent of the cases, there was no individual listed on the ownership line. In 21 percent, they did list someone, but it was unclear if it was the owner.

So the found anonymous ownership being one of the leading drivers of preventing law enforcement from being able to crack down on illicit massage businesses and the human trafficking that goes on through there, so that is just one example.

Senator WARNER. And there is some more examples of fake fronts, I know, in Southwest Virginia around opioid distribution.

Now, again, many of the small businesses want to get the right workforce, I think would like to see a shutdown of those kind of enterprises.

One of the things that we have also tried to address is that this information might be used to go after political opponents that have not done any—created any criminal wrongdoing.

I think you are aware in our legislation, we exempt (c)(3)s and (c)(4)s, but can you speak again to our legislation and how we preclude that kind of—any potential for political manipulation?

Mr. KALMAN. As I understand it, this bill is not meant to address political spending issues, and to be clear, if individuals or entities are moving money into the political system legally if people are—we may have a debate, a different debate over political finance, then this is not going to get it. That there is no public release of this information.

If an actor in a State did somehow get access to the FinCEN database, an Attorney General or what have you, who had access to the FinCEN database and used it purely to find out dirt on their political opponent, that is a criminal act, and they would have to be willing to jeopardize their political career.

I will say, though, that foreign interference in the election, if in fact money is coming in from Russia, North Korea, or China to influence our elections, and law enforcement finds out about it, this would be a way of combating that.

Senator WARNER. Let me also get in one, and let me be clear. We are very concerned about undue burden on small business. It is why we tried to make sure, unlike the House direction, that this reporting was supposed to be integrated into the existing processes and procedures and that you would only need an additional filing if there is that change in ownership.

I would like to have you comment on that, but I also do think, echoing what Senator Brown has said, that if we are second worst in the world on this, if we have evidence of terrorism and other bad actors, if we have evidence of sex trafficking, opioids and other levels of abuse, and we have seen a proliferation of these shell compa-

nies using these tools—I can tell you from the intelligence community side, we have seen that proliferation—I would be very anxious to talk to any small business about the need for this and work with every small business to make sure that we do this in the least burdensome way possible.

But to have simply a knee jerk reaction of any new reporting requirement, by definition, is not worth the value of that report is frankly a not very sophisticated or helpful view.

So, Mr. Kalman, how else can we make sure we do a better job on protecting small businesses from not doing this in a burdensome way?

Mr. KALMAN. Well, in your legislation, in the ILLICIT CASH Act, I think you all did take some really important steps that are new and different ways of collecting this information than had been proposed in the past.

Let me just give you one example, since we have limited time. The change to requirement the updates every 90 days instead of 60 days, businesses do not interact with Government every 60 days. They do interact——

Senator WARNER. Right. They do it on a quarterly basis.

Mr. KALMAN. Most businesses interact on a 90-day basis, which means that they do not have to remember independently. They do not have to think about this, and when they go on and file their payroll taxes or their quarterly estimated taxes or what have you, there could be a button on the IRS website that takes you to FinCEN. You check the thing going "Yes, that is still me" or make the updates, and it is a seamless process.

Senator WARNER. Again, that information is not financials; it is simply identify.

Mr. KALMAN. It is simply identification, and we think that that truly removes one of the burdens for small business and makes it a very seamless process in things they are already doing.

Senator WARNER. Thank you so much.

Thank you, Mr. Chairman.

Senator BROWN. I have one more question actually for Mr. Baer and for Mr. Kalman, if you would each answer about privacy concerns.

Some have expressed a concern requiring actual ownership information that company formation would unnecessarily infringe on American's privacy rights. Obviously, it underscores the importance of ensuring the information is lodged in a secure database where it can only be accessed by law enforcement officials with a legitimate public purpose.

Describe, each of you—start with Mr. Baer—and my really only question, could you describe precisely what ownership information will be required of companies' information? For example, under the Maloney bill in the House, do you think current FinCEN safeguards on data privacy are sufficient to ensure strict privacy for this kind of beneficial ownership information?

Mr. Baer.

Mr. BAER. Thank you, Senator.

Yeah, I believe existing safeguards have proven to work and would be sufficient in this area. As Mr. Kalman noted, access to FinCEN data is limited to a physical portal. You have to be author-

ized. You have to be pursuing a legitimate investigation. This cannot be a fishing expedition or just a fun frolicking detour. There are penalties in the event that that does happen.

And, again, we have a track record with FinCEN of success in that area, as well, of course, with the banking industry where this information is held and has been kept confidential until the end of time.

Senator BROWN. Thanks.

Mr. Kalman.

Mr. KALMAN. Specifically, the information is name, address, date of birth, and identification number. So just to answer that question, we think it is limited pieces of information that are valuable to law enforcement, without overly providing information about finances or other issues.

And I would just remind that the kind of fishing expeditions or concerns about this carry criminal penalties. This is a very serious issue.

One of the things they did in the House bill, which might be helpful, is when people—originally they had you access the FinCEN database through existing protocols, and people did not understand what that means. And so they actually listed out a number of the protocols to help people understand the privacy protections, and that, I think, gave people with privacy concerns a lot more comfort that when they are spelled out in the bill that that actually—when they saw it, they said, "Oh, that actually is a reasonable set of protections."

Senator BROWN. Thank you, Mr. Chairman.

Chairman CRAPO [presiding]. Senator Tills.

Senator TILLIS. Thank you, Mr. Chairman.

Thank you all for being here.

I have one question. Anytime we are looking at potential investments that are maybe questionable, we want to make sure that we have collected the appropriate information, make sure these transactions and investments are in the best interest of the United States.

The flip side of it is sometimes, let us say, with CFIUS, we know the vast majority of the applications go through the process are proven to be valid for the foreign direct investments. So when we get on this subject, we have frequent investors and those that—if you could think of almost TSA preclearance, the concept I am sure you are all familiar with and the trusted natural person. Can you give me any thought on how you could implement that so that the ones that you have based on track record would be fined, actually move them into the express line, so that we have more resources to go after potential investors and investments that are the ones that we are seeking to identify? Just go down the line.

Mr. BAER. Senator, I think you are right, and this certainly is an area where the vast number, vast majority of those who file in fact will not ever be objects of law enforcement interest. So, clearly, you want to minimize the burden on the great majority for whom this information eventually will not be that useful to law enforcement.

But I think the way you do that is by greatly simplifying the amount of information that they have to disclose, which especially in this day and age, when I am putting this—more information

than this on every website I seem to visit, to have to do that once at formation as part of a bunch of other things you are going to be doing anyway and quarterly only if there is a change, again, as part of an existing interaction with your Government, that seems the best way to minimize this obligation.

It is tough to do precheck when there is so little required. They are not doing cavity searches here for anybody. So it is really a minimal intrusion, I think, to start with.

Ms. HARNED. Well, again, we are very concerned about the burden, and we are concerned about the exposure. It is leaving honest American small business owners with—you noted the criminal penalties again. If you make a mistake, the way the current law is constructed in the legislation we are looking at, there are criminal penalties attached. You are now dealing with enforcement discretion to make sure that a mistake is not penalized that way.

We just also think that criminals are going to lie, and even in the hearing that you all held, I think, last week, Mr.—what is his last name?—Blanco said that even FinCEN was not going to be able to verify all of this data, and so then our question is why are you requiring every small business owner in this country to provide it.

Mr. KALMAN. We would be happy to talk with you about figuring that out. I think, as Mr. Baer said, because we are talking about such a limited set of information, I am not sure how you could streamline it further, but we would certainly be willing——

Senator TILLIS. Not much.

Mr. KALMAN. But we would be certainly willing to talk about that.

I think that the improvements like in the ILLICIT CASH Act that try and match up reporting episodes with existing business interactions with Government is a good way of making sure that you are minimizing the amount of burden on businesses, but happy to talk to you.

Senator TILLIS. Yeah. The issue, when you are a small business and you are the CEO, the CFO, the head of marketing, the head of regulatory affairs and sales, it may seem like only a little bit of information. But when you are acting or interacting with Big Government, I have no doubt that there are some who may want to move capital, simply will not, because it is just one more layer on top of a small business base that is already overburdened with just running their businesses.

So I think just looking at it, trying to figure out a way to do it efficiently, because I do know, just like foreign direct investment, the vast majority of the transactions are not maligned, and the more the merrier. That is how we continue our great story to tell in terms of growth.

Thank you all.

Chairman CRAPO. Thank you.

I am going to ask one more question too, and then we will be done with the questioning, maybe one more quick line of questions.

It focuses on this. I think Ms. Harned has raised legitimate questions from the small business concern about whether this is yet again another regulatory burden being imposed on our many small businesses in the country.

The response to her has been that this is a very minimal set of data and it is not really a significant increased burden.

I can see some concern on the part of the business community in the United States that maybe that is what we think, that it may not be what it becomes. I am familiar in—I am not going to use specifics here, but I am familiar in other regulatory arenas where what should have been just filling out a little bit of data about somebody has turned into a regulatory nightmare for those being regulated because—I will use an example that is a real example.

Penalties imposed for failure to capitalize the State in an address, I do not think we contemplate here having FinCEN or IRS examiners come into every small business in the United States to make sure that they go over their records and be sure that they are accurately reporting. I do not need you to—other than just give me a yes, that is what you are not contemplating. Is that correct, Mr. Baer and Mr. Kalman?

Mr. BAER. Correct, Senator. There is no examination function here.

And I would also add that at least under the Senate and—the draft Senate bill and the House legislation, there is no penalty for a mistake. It has to be a knowing, willful act.

Chairman CRAPO. So is there a knowing and willful standard in the legislation being proposed?

Mr. BAER. In the ILLICIT CASH Act, yes, there is.

Chairman CRAPO. OK. So, Ms. Harned, would you feel better—maybe I should not say "feel better." Would it be acceptable if there were a very solid and clear knowing and willful and material standard so that an immaterial or inadvertent mistake would not trigger penalties, and if we made it very clear that we do not intend for the regulators who will be enforcing this system to be stepping up this basic requirement that we are putting together and expanding it through rule and regulation or what have you?

Ms. HARNED. Well, I cannot negotiate today, right?

Chairman CRAPO. Sure.

Ms. HARNED. But, I mean, that would—what you are describing would be something we would definitely want to look at because, again, that is a concern. Just saying willful and knowing, that does not always come out the way that you might think it would for—you know, somebody may still not have bad intent there and still get caught up in it or at least have to defend themselves and pay money to do that. So we would want to look at that language.

Chairman CRAPO. All right. Thank you.

Either Mr. Baer or Mr. Kalman, would you like to comment on that any further, just the general issue here that I raised?

Mr. BAER. I guess, Mr. Chairman, the only thing I would add is, I mean—and to go back to my original testimony, this is information that small businesses and large businesses are already providing to their banks under the FinCEN Customer Due Diligence Rule instead of—it is actually the Social Security number instead of the passport or driver's license ID, but everything else is the same. That has not proven to be an insuperable burden. I do not think you have seen prosecutions.

So it is something they are already doing, at least any small business that has a bank account, which is, in other words, any le-

gitimate small business. So that seems to be a pretty good foundation on which to believe that this is not something that is going to get out of control or be a very large burden.

Chairman CRAPO. All right. Well, thank you.

I see we have a couple of other Senators arrive. Did you want to ask questions?

OK. Then I did not see who was here first. Oh, Senator Jones, go ahead.

Senator JONES. Thank you, Mr. Chairman. I appreciate the witnesses being here. Thank you, Mr. Chairman, for calling this hearing.

I know that—and I apologize for being late this morning, but I know that there have been a number of concerns raised about added paperwork for small business. But when talking about information that has the potential for saving lives, I am not sure that that—I do not want to get overburdened with paperwork, but at the same time, this is really important.

The bill that we have pending right now makes clear that FinCEN should take every step available to combine the beneficial ownership reporting with existing procedures that a business might already engage with at a State and Federal level.

So let me give you an example. In Alabama, every year, an LLC has to file an annual report and business privilege tax return. It costs a minimum of $100, and there are multiple forms to fill out. This does not even count the various business licenses that they have to fill out, the permits that are required often to actually conduct business.

I guess this really—anybody can answer this, or all of you can. If the filing of the beneficial ownership, three or four names and addresses, could be done alongside processes that already exist, like the ones I just described, is this going to be a substantial burden on those businesses?

Ms. HARNED. Well, I would argue that you are also kind of making my point because you are suggesting all of the reports that the small business owner is already having to fill out.

I hear what you are saying on the protocols that——

Senator JONES. But you are not suggesting that they should not fill those forms out. I mean, a business——

Ms. HARNED. No. I am just saying that that is already—one of their biggest burdens on small business is just paperwork compliance.

Senator JONES. OK. Sure.

Ms. HARNED. And when you are talking about adding this to existing protocols, my other concern that I raised in my testimony is—again, you click on a button that takes you to FinCEN. My members do not know who FinCEN is, and they may be very skeptical that this is something that they really need to do. Are they being scammed? Is this some malware situation?

I could see that reaction happen often because I have been at NFIB for 17 years and we still get numerous calls on the Small Business Survey that the Census Bureau does.

Senator JONES. Right.

Ms. HARNED. "Do I really need to do this? Do I really need to provide this information?"

So I just—you need to understand that for a business that just has five employees, they are very skeptical of these questions that are coming from——

Senator JONES. Is that any reason not to do it, though?

Ms. HARNED. I am sorry?

Senator JONES. Just because there would be some businesses that might be skeptical of doing it and may be afraid to push the Send button, is that a reason not to do it? If 90 percent of the businesses out there do it and they do not have a problem with it, should we just throw the baby out with the bath water and let the 10 percent control?

Ms. HARNED. Right. But then there is criminal and significant civil penalties for noncompliance.

Senator JONES. No, I agree with that. Look, I get that, that we, you know—but I have also been a prosecutor, and I understand that when you see something like that and you have a business, you talk to them. You do not run out and prosecute somebody just simply because they screw up the first time.

So I do not think there is a real likelihood, given what my history has been with prosecutions, that if somebody does not do it as this process gets implemented that they would immediately be prosecuted.

Now, if they do not do it three, four, or five times in a row, that is a different story, but I hesitate to not put something like this in there just because somebody might be hesitant to do it when I think overwhelmingly the small businesses out there get it, and they would understand exactly why we do it.

I do not think that this—from my view, it does not increase the burden very much. There is a burden on small businesses, and I think everybody on this Committee would love to see that burden lightened in some way, but yet some of the information that they have is just incredibly important. It is important for transparency. It is important for people to see what is going on in their State.

So how do you balance that? Do you just not do it? Do you just not collect this?

Ms. HARNED. Again, I mean—but now the solution that is being proposed is so broad. I mean, it is every single business owner.

Senator JONES. Well, what do you suggest? Give me a suggestion on how we narrow it.

Ms. HARNED. Well, were there not businesses that are more likely than not? Like we have talked about real estate or things like that. Can we not target where we are seeing the actual problem?

Senator JONES. We have excluded a bunch of those. We have excluded a bunch of businesses in this bill. For that very reason, we have excluded a bunch of these businesses.

Ms. HARNED. No, but where you are seeing more of the problems, I guess, is what I am saying.

Senator JONES. Yeah, but if we see more of the problems—just like when I was—if we arrested a drug dealer, when I was a prosecutor, on this corner, somebody is going to pop up on this corner. So if we start excluding those businesses, guess what? Somebody is going to start moving into those businesses that have been excluded.

I think what we have done with this bill is we have put some exclusions in there because, historically, there has never been an issue, and the burden would be great.

But we cannot start cherry-picking those exclusions so much because I am telling you the bad guys will go there. I know that. I have been there. I have done that, and they will go there.

So I am happy to work with you and your staff to try to help to tailor this to allay your concerns, but at the same time, I do not want to get the fear of a few people who might be concerned about hitting a button on the internet to stop what I think and what I think my colleagues that have worked on this for over a year have done, an incredibly important thing that we can collect that might help save lives down the road.

But thank you. Thank you very much.

Thank you, Mr. Chairman.

Chairman CRAPO. Senator Cotton.

Senator COTTON. Thank you, Mr. Chairman.

Thank you to our witnesses for appearing today.

I have been working on the ILLICIT CASH Act now since last summer, and I want to thank Senator Jones, Senator Warner, Senator Rounds, the Chairman and Ranking for their assistance, as well as some of the other Senators not on this Committee, like Senator Gramm and Senator Feinstein on the Judiciary Committee, who held a hearing on this topic yesterday.

I also want to thank the Bank Policy Institute and the Financial Accountability Corporate Transparency Coalition for their support for the draft bill we have introduced.

The bill includes an overhaul of our outdated anti–money-laundering laws, and most of it was done months ago, but we still have only released a draft, even after consulting with more than 50 different stakeholders, like privacy groups and law enforcement, FBI, FinCEN, and business groups, because we still want more feedback. We do expect to introduce a final version later this summer, but we look forward to hearing feedback and input from our colleagues here in the Senate as well as the organizations who are represented here at this hearing and many other representatives of the business community.

We need a beneficial ownership registry for national security purposes. I have heard that repeatedly from the FBI, from the Department of Justice, from the intelligence communities I oversee on the Intelligence Committee. It can help not only things like terrorism, but human trafficking and other crimes.

I am also very mindful, however, of the potential burden that such a registry could impose on businesses, especially small businesses. That is why I have made it a priority over the last year to try to find ways to minimize those burdens, while also ensuring that our registry helps meet the needs of law enforcement in our intelligence communities.

I think it is better that we work now to create a best-in-the-world system if a registry is going to be inevitable rather than wait around to have a system that ultimately will hurt small businesses.

That is why we have taken many steps to include sensible provisions that will alleviate the potential burdens on small business.

First, the beneficial ownership registration will be attached to things that businesses are already doing, like creating or renewing their entities at the State level.

Second, there will be no additional annual reports required. After filing a registration, companies do not have to do anything more unless there are changes to the company's ownership.

Third, there will be exemptions to the registry that are self-effectuating. Things like nonprofits, churches, and other regulated entities will not have to prove that they are exempt. They will simply be exempt.

Fourth, going to the points that Senator Jones was making, there will be a cure provision. Everyone will get due process, which should have the benefit of also getting quality data into the database. So if there is any kind of minor discrepancy in a company's beneficial ownership registry, that company will have the opportunity to address and correct that issue. That also means that they will not face the risk of certain penalties without the ability to correct inadvertent or good-faith honest mistakes or errors.

Fifth, there will be an ombudsman-like process for any business who has questions or complaints about the process as well as a semiannual report to Congress summarizing Inspector General's activities related to beneficial ownership.

Sixth, strict protocols for who can access the beneficial ownership registry will be adopted. We have also included very severe penalties, even prison time, for the improper disclosure of any company's beneficial ownership data.

Seventh, we will have a clear definition of what it actually means to be a beneficial owner, clearer than the bill that just passed the House Financial Services Committee.

Eighth and final, it will be easier for companies to open bank accounts. Opening business bank accounts ought to be easier than it is today, and it will be once companies—or once financial institutions can access the high-quality beneficial ownership registration.

So I would like to ask the witnesses—Do these changes make it easier to get a beneficial ownership registry up and running with minimal disruption and also minimal long-term burden to businesses, especially small businesses?

We will start with Mr. Baer and just go down the panel.

Mr. BAER. Senator, I think they absolutely would, and I should hasten to add, although the focus today has been the beneficial ownership portion of the bill, the rest of the ILLICIT CASH Act is extremely important and we believe extremely well considered and is a very, I think, innovative and thoughtful approach to a lot of very difficult issues.

But with respect to the beneficial ownership provisions in particular, we believe this is a very well-thought-through approach to mitigating any potential costs and burdens and yet still getting law enforcement and national security the information they need.

Senator COTTON. Thank you.

Ms. Harned.

Ms. HARNED. Well, what you have articulated does sound like it would address some of our concerns. We would want to see that statutory language and really want those protections clearly in the statute for small business owners.

Senator COTTON. Yeah. Thank you.

Mr. KALMAN. Yes. And thank you for your leadership on this and your colleagues.

We do think the concerns and the issues that have been added to the bill improve the bill and does help to strike that appropriate balance between privacy, ease of business, and making sure that law enforcement has what it needs.

Senator COTTON. Thank you.

So my time has expired. As I said, this is draft legislation. We want to work together, especially we want to work with small businesses. Everyone on this panel, no matter what State we come from, represent thousands of small businesses like pizza shops and dry cleaners and lawn care companies that have very legitimate reasons to need these kind of entities. We want to find ways to separate them out with the minimal burden while also stopping terrorists and drug traffickers and deadbeat dads and people trying to hide assets before they get a divorce and all of the other malicious reasons that people use these entities.

So we will appreciate your continued input and feedback on the legislation. Thank you.

Chairman CRAPO. Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you.

And I agree in the sense that the goal here is to minimize the burden to our businesses but still allow our law enforcement agencies to go after that criminal element when it comes to these shell companies.

And as somebody who was a former Attorney General of the State of Nevada, I agree with my colleagues, particularly Senator Jones, that this is happening, and it has been very difficult for law enforcement to get the information to really take on that criminal element.

I am talking transnational crime. We do not know, without the information, the extent of the criminal activity that is going on.

So let me ask you, Mr. Kalman. We have heard—or the Committee has heard from the Fraternal Order of Police, the National District Attorneys Association, Federal Law Enforcement Officers Association, two dozen State Attorneys General, and others that the lack of beneficial ownership information in the U.S. frustrates officers and stymies this criminal investigation, as I have said. Can you share any examples to help us understand why that lack of information has stymied criminal investigation?

Mr. KALMAN. Yes. Thank you for the question, Senator.

I mean, there are thousands of examples of how anonymous companies are now being used for everything from fueling the opioids crisis to human trafficking, as you said, sanctions evasion.

I think one of the more famous examples that gets batted around is how Iran had used a series of anonymous companies, including some in New York, through which to purchase property in Manhattan. And to think about that just for a second, that the safest place in the world for Iran to evade our sanctions, our economic sanctions, was to park money in the United States and in New York, that should be pretty chilling to folks.

So we think that while the considerations of privacy and small businesses burdens, absolutely we want to work with people to

make sure we are putting in the appropriate protocols, we do think that this is critically important information, and law enforcement continues to say it is.

Senator CORTEZ MASTO. And can you also address—I believe in your written testimony, you note a report from the Global Witness. The report "Hidden Menace" found numerous incidents in which the U.S. Department of Defense had contracted with anonymous companies that at best defrauded the U.S. military and at worst endangered the lives of troops serving overseas. Can you expand a little bit on what the "Hidden Menace" report found about Pentagon contracts?

Mr. KALMAN. I mentioned this a little earlier, but just to say I share with you, one of the more chilling stories was that the Defense Department had contracted with a U.S. company to provide services to troops in Afghanistan. It turns out that that company was secretly owned by folks affiliated with the Taliban, and so we were literally providing the funding to potentially buy weapons and other arms, guns and other arms that are being aimed at our troops.

Senator CORTEZ MASTO. Thank you.

And I appreciate the conversation today. I am sorry I had to step out. I have a competing Energy and Natural Resources hearing going on at the same time. But please know that this is an issue that is so important for us to address, and as somebody who was responsible for law enforcement in the State of Nevada, it truly is an issue. We know it is happening, and we have got to figure out how we stop it.

I think working with our small businesses and working with the businesses, there has got to be a way that we can minimize that burden but at the same time give the information to our law enforcement to weed out and stop and hold accountable anybody, whether it is a foreign adversary or drug cartels or anybody that wants to utilize a shell company to defraud others or violate the criminal laws of this country.

So I am looking for that balance. I appreciate the legislation that has been introduced and the draft legislation that I have seen. We are looking at it right now. I appreciate you being here, look forward to more input, but I am hopeful at the end of the day, we can all come together and really look at good legislation that is going to address the issues that we have heard about today as well.

So thank you.

Chairman CRAPO. Senator Sinema.

Senator SINEMA. Thank you, Mr. Chairman, and thank you to our witnesses for being here today.

At the last beneficial ownership meeting, I spoke about how the Sinaloa Cartel and other criminal groups move millions of pounds of methamphetamines and heroin from Mexico through Arizona. These groups tear our communities apart, and it is clear that Arizonans bear the brunt of Washington's failure to address the crisis at our southern border.

So, in the last hearing, we learned how beneficial ownership information can help focus and improve the efforts of law enforcement to stop these dangerous criminals, and I am grateful for the

opportunity today to hear from non-Government stakeholders about the best way to obtain beneficial ownership information.

So, Mr. Kalman, thank you for being here today. Under the proposed ILLICIT CASH Act, what types of information would businesses provide to the financial crimes enforcement network upon incorporation?

Mr. KALMAN. There are four basic pieces of information, which would be the name of the owner, the address, the date of birth, and an identification number. There is no financial or other information about the company that is being provided.

Senator SINEMA. Great. Thank you.

Mr. Baer, thank you for being here as well. How much overlap is there between disinformation and the information that businesses provide to banks when they open a bank account?

Mr. BAER. Thank you, Senator.

It is fairly heavy on overlap. The only difference is under the customer due diligence rule, the bank would collect the Social Security number rather than a passport or a driver's license ID.

The important thing here is that those banks do not collect information from a company unless it forms a bank account. So if you have a pure shell company that does not employ anybody, does not pay anybody, you do not need to have a bank account, and you do not ever need to provide that information to your bank.

Also, the bank does not provide that information to law enforcement unless they have some reason to file a suspicious activity report.

So if law enforcement is suspicious, they do not have that information. They only get the information if the bank is suspicious.

Senator SINEMA. That is important to know. Thank you.

Mr. Kalman, to what extent do drug cartels like Sinaloa use shell corporations to conceal their illicit holdings?

Mr. KALMAN. One of our coalition members called Fair Share did two reports on this called "Anonymity Overdose", documenting numerous cases of where drug cartels and drug traffickers were using anonymous companies here in the United States to push drugs into various communities, and we are happy to provide that information to you.

Senator SINEMA. Thank you.

And how difficult is it, Mr. Kalman, for law enforcement to interdict drug cartel financing that is hidden in these shell corporations when they do not have comprehensive beneficial ownership information?

Mr. KALMAN. Our law enforcement partners say that this is a significant priority for them. They begin investigations, and all too often, they will hit the brick wall of finding an anonymous company. And they will have to drop the case.

Now, sometimes if there is an enormous amount of resources and they have the time and the ability to do that and can divert the resources, then they can ferret it out in the long term. But most often, as you know, our law enforcement has limited resources, and they have to make decisions about what they do. These kinds of lengthy investigations unfortunately are not getting followed up on, and it is not for lack of want or effort. It is literally because they cannot get through the brick wall.

Senator SINEMA. So given what you have just described as the brick wall and the fact that most law enforcement entities do not have unlimited resources in time, would you conclude that a beneficial ownership information would be a key tool for helping law enforcement, for instance, in Arizona stop drug cartels like the Sinaloa Cartel?

Mr. KALMAN. Yes. And the fact that, as I think has been said, the National District Attorneys, the Fraternal Order of Police, the sheriffs, law enforcement, retired law enforcement officials, and also almost 100 civilian and former military national security experts to add that lawyer into it as well have signed letters saying that this is a top priority. It is something that Congress should do.

And I think as was mentioned earlier, just yesterday in the Judiciary Committee, Adam Szubin, former Treasury official, top official, said that this is the single most important thing that Congress could do.

Senator SINEMA. Wow. Thank you.

So, Mr. Chairman and Ranking Member Brown, it is clear that we need to improve our anti–money-laundering efforts through the collection of beneficial ownership information, and I hope that we can do so in a way that makes it straightforward for small businesses but also crack down on drug cartels and others who would do Arizonans harm.

I, of course, am committed to working with our Committee to get this done.

Thank you. I yield back.

Chairman CRAPO. Thank you, Senator.

That does conclude our questioning, and for Senators wishing to submit questions for the record, those questions are due in 1 week, on Thursday, June 27th, and to the witnesses, we ask that you respond to the questions you may receive as quickly as you can.

Again, thank you for being here today, and this hearing is adjourned.

[Whereupon, at 11:24 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

## PREPARED STATEMENT OF CHAIRMAN MIKE CRAPO

Today, the Committee will continue its discussion of how better collection of beneficial ownership information can deter such problems as money laundering, terrorist financing, and sanctions evasion through anonymous shell companies.

I will note at the outset, again, that while the vast majority of anonymous corporations can serve legitimate purposes, this type of incorporation can also be abused to aid and abet all manner of financial crime.

Last month, the Committee heard from witnesses from law enforcement and a banking regulator about what steps the U.S. should take to modernize its beneficial ownership regime and strengthen its enforcement.

Today, we have invited a panel to give us some perspective from the business world on this difficult subject.

With that, I welcome Mr. Greg Baer, President, of the Bank Policy Institute, whose members confront the ownership issue at account openings; Ms. Karen Harned, of the National Federation of Independent Business, which speaks to the concerns of the hundreds of thousands of small businesses it comprises; and, Mr. Gary Kalman, of FACT, or the Financial Accountability and Corporate Transparency Coalition, an alliance of organizations that is working toward ending the use of anonymous shell companies as vehicles for illicit activity, and increasing transparency for more informed tax policies.

During last month's hearing, our witnesses assessed the need to eliminate anonymous corporations by means of collecting beneficial ownership information to protect the U.S. financial system, its national security, and citizens from harm.

The Committee learned that according to estimates from the U.N. Office on Drugs and Crime, there is more illicit money flowing through the global and U.S. financial systems than ever before.

The U.N. estimate found that global illicit proceeds now total some $2 trillion and the proceeds of crime in the United States are over $300 billion.

All of that illicit money has several things in common: somebody has to make it, hide it, move it, clean it, and use it.

Despite efforts of U.S. law enforcement and the heavy U.S. regulatory framework of the Anti–Money Laundering/Bank Secrecy Act (AML/BSA) regime, which includes a mandate to collect beneficial ownership upon opening of a bank account, criminal elements in this country and from other countries can and do exploit weaknesses in the current U.S. corporate formation system to hide identities and illicit assets behind anonymous corporations.

In our last hearing, FinCEN Director Blanco testified that a necessary "second critical step in closing this national security gap is collecting beneficial ownership information at the corporate formation stage."

In agreement with Blanco, FBI Financial Crimes Chief D'Antuono cited the need for a "central repository," to allow law enforcement to store and share the information.

OCC Senior Deputy Comptroller Gardineer, also emphasized the need for a centralized database, so that businesses could provide, update, and verify beneficial ownership information.

Importantly, she also recommended that "foreign entities be required to report ownership information either at the time of State registration or upon establishing an account relationship with a U.S. financial institution."

Our hearing today comes at a time when bipartisan support for beneficial ownership legislation continues to build.

Last week, the House Financial Services Committee marked up H.R. 2513, the Corporate Transparency Act of 2019, which was reported out of committee on a 43–16 vote.

And, on the very same day, a bipartisan group of my Senate colleagues here on the Banking Committee circulated draft legislation, presently called the ILLICIT CASH Act, which provides a number of important measures to modernize the AML/BSA regime and to address the collection of beneficial ownership information.

I especially want to acknowledge the hard work Senators Cotton, Warner, Rounds, and Jones, and their staffs, put in over the last year on this effort, which the Committee, as a whole, shall take close note of, moving forward.

Each of these legislative vehicles share some of the broad themes, brought out in the Committee's first hearing, such as a requirement for the collection of beneficial information at the time of a company's formation, periodic updating, storage of that information in FinCEN's secure database, and limiting access to that database to Federal law enforcement and its qualified State partners.

We turn now, to our panel, for their perspectives on the important issues underlying any further collection of beneficial ownership information, and how that might

impact banking and business operations, including concerns that arise with regard to privacy and liability issues.

Given the facts presented to the Committee thus far, there are strong law enforcement and national security reasons supporting additional collection of beneficial ownership information.

Hopefully, our witnesses will provide some insight on how to collect this information at minimal cost and burden to businesses.

Now is the time to critically examine how the AML/BSA regime can be modernized, and, in particular, how businesses can work effectively with Government to efficiently provide beneficial ownership information that will in turn provide a high degree of usefulness to combat crime and terrorism.

---

**PREPARED STATEMENT OF SENATOR SHERROD BROWN**

Thank you, Mr. Chairman, for calling this important hearing. This is the latest in a series of hearings in the Committee on our Bank Secrecy Act and anti–money-laundering reform efforts, and on critical changes to U.S. beneficial ownership laws to combat abuses by owners of anonymous shell companies, some of whom have been exploiting our system for criminal purposes for years.

Unlike in most areas of disclosure and transparency law, where the U.S. has lead the way, on this issue we have long lagged behind other jurisdictions, and failed to require uniform and clear ownership information for firms at the time of their incorporation.

This is critical to law enforcement. In the U.S. they have to spend precious time and resources issuing subpoenas and chasing down leads to secure even the most basic information about who actually owns a company. That makes no sense. And it must change.

Treasury's 2018 Money Laundering Risk Assessment estimates that about $300 billion in illicit proceeds from domestic financial crime is generated annually, making these funds ripe for money laundering through the system.

Criminals abuse the financial system to launder funds gained through narcotics trafficking, organized crime, the sale of counterfeit goods, Medicare and Medicaid fraud, and other criminal activities. Much of this dirty money is funneled through anonymous shell corporations.

As I've observed before, none of the abuses we'll discuss today—drug trafficking, human trafficking, Medicare fraud, money laundering—are victimless crimes.

Money laundering for drug cartels has a direct line to the opioid crisis in Ohio, where Sinaloa cartel actors have been destroying thousands of families.

Human traffickers who exploit the misery of runaways in truckstops at the intersections of major interstate highways in Ohio and across the country, use the financial system to launder their profits.

Medicare fraudsters cost the taxpayers $2.6 billion in 2017, according to the HHS Inspector General, and tarnish the reputation of this lifeline for seniors.

That's why anti–money-laundering and beneficial ownership laws are so critical: they protect the integrity of our financial system, and provide critical intelligence to law enforcement to combat crime.

Under Treasury's recent customer due diligence rule, banks must already secure some of this information from account holders when they open accounts.

And while banks must continue to play a key monitoring role, it's also important that we require companies to provide basic information on their ownership when they're formed.

In today's hearing, we'll hear from the Financial Accountability and Corporate Transparency Coalition, and from the banks, on the many reasons to pursue these reforms, including the transparency, anticorruption and anti–illicit financing benefits such reforms would offer. I ask consent to include a number of their reports into the hearing record.

And we'll hear from NFIB, some of whose members have expressed concern about the paperwork burden of providing even simple ownership information—name, address, and a copy of a current passport or driver license.

Requiring companies' ownership information and storing it in a secure Federal database like FinCEN's, alongside its bank secrecy information, would help address longstanding problems for U.S. law enforcement.

It would help them investigate cases involving counterterrorism, drug trafficking, Medicare and Medicaid fraud, human trafficking, and other crimes. And it would provide ready access to this information under long-established and effective privacy rules.

Without these reforms, criminals, terrorists and even rogue Nations will continue to use layer upon layer of shell companies to disguise and launder illicit funds. That makes it much harder to hold bad actors accountable.

Chairman Crapo and I agree—we must move forward to require complete ownership information—not front men, not those forming companies on behalf of those who will pull the strings from behind the curtain—but the actual owners of companies.

We can do this simply, efficiently, and effectively, without unduly burdening small businesses or others.

Updating and strengthening our AML and beneficial ownership laws will give us a 21st century system to combat these crimes. I guarantee you criminals have long been revising, adjusting, and amending their tactics to circumvent and evade those laws.

I welcome today's witnesses to the Committee, and look forward to hearing your perspectives.

---

## PREPARED STATEMENT OF GREG BAER

CEO, BANK POLICY INSTITUTE

JUNE 20, 2019

Chairman Crapo, Ranking Member Brown, and Members of the Committee, my name is Greg Baer and I am president and CEO of the Bank Policy Institute. BPI is a nonpartisan public policy, research and advocacy group, representing the Nation's leading banks. Our members include universal banks, regional banks, and major foreign banks doing business in the United States. Collectively, they employ nearly 2 million Americans, make 72 percent of all loans and nearly half of the Nation's small business loans, and serve as an engine for financial innovation and economic growth. BPI strongly supports legislation to end the use of anonymous shell companies and welcomes this hearing in the hope that it will prompt swift Congressional action.

### Introduction

Anonymous shell companies are a key method used by criminals to hide assets for a range of dangerous and illicit activities, including human trafficking, terrorist financing, money laundering, and kleptocracy. All too often criminal investigations hit a dead end when law enforcement encounters a company with hidden ownership and lacks the time and resources to peel back the many layers of secrecy currently permitted by U.S. law.[1] And the more sophisticated and sinister the criminal, the more layers there generally are.

This problem is not difficult to solve. It has been solved by most countries around the world. While as a general matter our country does more than any other to identify and block the proceeds of crime, we are among the worst when it comes to allowing criminals to use the corporate form to cloak ownership; as a result, the United States has become a safe haven for those who wish to hide the proceeds or instruments of illegal activity. We have therefore been repeatedly criticized by the Financial Action Task Force, an intergovernmental AML standard-setting body, for this deficiency in our system.

Legislation to allow law enforcement to look behind the corporate veil, including the draft recently circulated by a bipartisan group of Senators on this Committee, would thus reduce crime and terrorist activity, and enhance the status of the United States as a country that fights against, not harbors, the worst people in the world.

The Nation's banks already provide significant assistance to law enforcement by determining the ownership of most companies that open a bank account and then using that information to monitor the account for suspicious activity. The requirement for banks to determine corporate ownership was put in place by the Treasury Department as a workaround to close this gap in the U.S. AML/CFT regime. For banks, and, importantly, for the clients who must provide this information, legislation now has the potential to centralize that process and make it more efficient. Most importantly, this legislation can provide law enforcement a first look at true shell companies that never open a bank account because they conduct no business—employ no people, earn no money, pay no taxes—but rather just hold assets.

---

[1] See Statement of Steven M. D'Antuono before the Committee on Baking, Housing, and Urban Affairs, United States Senate, (May 21, 2019); available at *www.banking.senate.gov/imo/media/doc/D'Antuono%20Testimony%205-21-19.pdf*.

Two relevant concerns have been expressed about such legislation, however: potential burdens on small business and privacy. To evaluate those concerns, we should consider a few key facts.

First, the draft Senate legislation requires an individual who owns more than 25 percent of a covered company or exercises substantial control to, at the most, disclose five pieces of information: (1) name, (2) address, (3) date of birth, (4) nationality, and (5) unique identifying number (e.g., driver's license or passport number). That is all. The House bill includes similar requirements. It is less information than one must provide to book a flight on any airline. And since the great majority of American businesses have only one owner, it would be generally provided by and about one person.

Second, under current U.S. law, this information is generally already provided any time a company opens a bank account, except in most cases a social security number is provided in lieu of a driver's license or passport number. And it must be provided for each account, and to every bank used by the company, separately. Of course, any legitimate U.S. business, large or small, probably has a bank account, because any business that earns money or pays expenses or employs people must have a bank account. Thus, for small businesses, legislation would not increase reporting obligations.

Third, with respect to privacy, establishment of a directory for corporate ownership would mean that a law enforcement official could obtain an address, date of birth, and driver's license or passport number. However, this is information already known to various arms of Government, including the DMV and the IRS. It is important to note that, unlike beneficial ownership directories established in other countries, the bills currently being considered in Congress would keep ownership information private from the general public and would only be accessible to law enforcement and financial institutions performing due diligence requirements. Again, it is difficult to understand how this would be a concern of legitimate businesses. It would, however, be a concern to a drug trafficker or kleptocrat using a shell company to hold a multimillion-dollar condominium in West Palm Beach.

Most small business owners in fact agree that ending anonymous shell companies should be a priority and are willing to share additional information to help prevent the abuse of our financial system. According to a poll conducted by Morning Consult on behalf of BPI, small business owners across the aisle support measures to end anonymous shell companies. Of those who had an opinion, 75 percent of small business owners surveyed support requiring business owners to provide their personal information when forming their company to help close this loophole in the U.S. AML/CFT regime. Further, two-thirds of small business owners agree that providing their personal information when registering their company would not be burdensome. [2]

With the potential benefits and cost of legislation now in mind, let me turn to the details of such legislation.

**Current Law**

FinCEN finalized in 2016 its customer due diligence rule, which requires banks of all sizes to identify and verify the beneficial owners of their corporate customers each time they open a new account or when a triggering event occurs. [3] In particular, institutions are generally required to collect and certify information on two ownership prongs for most business customers: (i) an equity prong that requires the identification and verification of individuals who directly or indirectly own 25 percent or more; and (ii) a control prong that requires the identification and verification of an individual with "significant responsibility to control" the legal entity. [4]

The FinCEN rule has three gaps that legislation could fill. First, while institutions are generally able to rely on the beneficial ownership information provided by the business customer, they have no reliable, complete external source against which to verify the information. Second, information provided under FinCEN's CDD rule is not reported to law enforcement. Third, many criminals avoid the banking system and launder money by forming LLCs and using them to hold real estate, art,

---

[2] See *The Bank Policy Institute*, "Small Business Owners Say Yes To Ending Anonymous Shell Companies", (June 2019); available at *https://bpi.com/wp-content/uploads/2019/06/Ending-Anonymous-Shell-Companies-Survey-Infographic.pdf*.

[3] See 81 FR at 29, 398.

[4] While the focus of this hearing is on ending anonymous shell companies, BPI remains concerned about the CDD rule's requirement that covered financial institutions must reconfirm the beneficial owners of an existing customer each time that same customer opens an additional account. There is no reason to believe that the opening of a new account, in and of itself, is an indication that the beneficial ownership of the customer has changed.

jewelry, or other valuables—all without having to open a bank account. For them, no one collects this information.

**Key Principles for Legislation**

Weighing these costs and benefits, BPI supports legislation built on the following principles.

First, in order to fulfill their obligations under the Bank Secrecy Act and FinCEN's customer due diligence rule, financial institutions should be able to rely on the information in the directory to fulfill their CDD requirements. Banks are committed to helping law enforcement catch criminals and have spent almost 50 years developing methods and tools to identify suspicious activity. Indeed, the purpose of the BSA is to provide law enforcement with highly useful leads on illicit activity.

Second, any filing requirements for this directory should mirror FinCEN's customer due diligence rule in terms of who must provide the information and what information must be provided.

Third, covered entities should only be required to provide minimal, but key, information during the incorporation process, which is a cornerstone of both the House and Senate bills. With both drafts, we believe that small businesses would be required to provide identifying information once, at the time they become bank customers, instead of each time they open an account, which currently happens under the CDD rule.

Fourth, reporting requirements should be clear and easy to comply with. Businesses routinely file documents with State or Federal Government, who could assist in educating covered businesses about their beneficial ownership reporting obligations.

Fifth, legal risk for businesses should be minimal. Both the House and Senate bills achieve this goal because the legal standard that must be met for the imposition of penalties is very high: knowingly providing, or attempting to provide, false or fraudulent beneficial ownership information or willfully failing to provide complete or updated beneficial ownership information to FinCEN. Furthermore, policymakers continue to explore various avenues, examples of which are included in both the House and Senate bills, to ensure that violations that are not knowing or willful can be easily remedied.

Sixth, the privacy of the information submitted should be protected. Under the current bills, the directory as currently envisioned would only be accessible by law enforcement and financial institutions; it would not be a public directory like those employed in other countries such as the United Kingdom. Furthermore, both the House and Senate bills impose criminal penalties for the misuse or unauthorized disclosure of beneficial ownership information. Of course, banks generally already maintain this information under existing law.

In sum, under these principles, the only type of company that would see additional burden are those that have no U.S. bank account—in other words, a shell company that spends no money in the United States, produces no goods, and employs no Americans.

**The Need for AML Reform**

As I've raised previously with this Committee, banks are spending an inordinate amount of resources complying with U.S. AML/CFT obligations but are not able to effectively protect our country.[5] Instead, today's regime is geared towards compliance expectations that bear little relationship to the actual goal of preventing or detecting financial crime, and fail to consider collateral consequences for national security, global development, and financial inclusion.

BPI recently conducted an empirical study to better understand the effectiveness of the current BSA/AML and sanctions regime.[6] The goal of the BSA regime is to provide information that is of a "high degree of usefulness"[7] to law enforcement, yet BPI's study found that almost 50 percent of AML personnel are not involved in

---

[5] See Testimony of Greg Baer before the Before the Senate Committee on Banking, Housing, and Urban Affairs "Combating Money Laundering and Other Forms of Illicit Finance: Opportunities To Reform and Strengthen BSA Enforcement", (January 9, 2018); available at *www.banking.senate.gov/imo/media/doc/Baer%20testimony%201-9-18.pdf*.

[6] Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML and Sanctions Compliance, (October 29, 2018); available at *bpi.com/recent-activity/getting-to-effectiveness-report-on-u-s-financial-institution-resources-devoted-to-bsa-aml-sanctions-compliance/*.

[7] See 31 U.S.C. §5311.

tasks directly focused on reporting to law enforcement.[8] Instead, they are performing other tasks such as issuing policies and procedures; conducting quality assurance over data and processes; and auditing of such programs and systems, among other things. Furthermore, in 2017, survey participants reviewed approximately 16 million alerts and filed over 640,000 suspicious activity reports (SARs). Institutions that record data regarding law enforcement inquiries reported that a median of 4 percent of SARs resulted in follow-up inquiries from law enforcement. There is no data on how many prompted an arrest or conviction, or whether SAR data proved important when sought, as the industry does not have such data.[9]

We are pleased by the bicameral, bipartisan efforts to address this imbalance as well as recent efforts by regulators to encourage banks to adopt innovative AML compliance methods.[10] As you are aware, Congress vested exclusive authority to implement the BSA in Treasury, and the Secretary has delegated that authority to FinCEN.[11] Therefore, the Treasury Department should take a more prominent role in coordinating AML/CFT policy across the Government to set priorities for the regime.[12] The existing system, where priorities are not clearly established and examinations are compliance focused, with zero tolerance across all types of activity, does not produce an effective U.S. AML/CFT regime.

Furthermore, as the data shows, bank resources could be more effectively deployed, so we also recommend that Treasury conduct a broad review of current BSA requirements and guidance and prioritize the reporting of highly useful information to law enforcement.[13] Critically evaluating, updating, and streamlining requirements would not only improve the utility of SARs, but would also make more resources available to other higher value AML/CFT efforts, such as more proactively identifying and developing techniques to combat emerging trends in illicit activity. Finally, Treasury must take a more prominent role in coordinating AML/CFT policy and examinations, which is presently dispersed amongst multiple Federal and State regulatory agencies. The draft Senate legislation offers a thorough, thoughtful response to this state of affairs.

BPI urges Congress to quickly adopt AML reform legislation that puts an end to anonymous shell companies and stands ready to engage with members of Congress to assist in making the U.S. AML/CFT regime more effective.

I look forward to your questions.

---

## PREPARED STATEMENT OF KAREN HARNED

EXECUTIVE DIRECTOR, SMALL BUSINESS LEGAL CENTER, NATIONAL FEDERATION OF INDEPENDENT BUSINESS

JUNE 20, 2019

Chairman Crapo, Ranking Member Brown, and Members of the Committee, on behalf of NFIB, I appreciate the opportunity to submit for the record this testimony for the Senate Banking, Housing, and Urban Affairs Committee hearing entitled, "Outside Perspectives on the Collection of Beneficial Ownership Information".

My name is Karen Harned, and I serve as the executive director of the NFIB Small Business Legal Center. NFIB is the Nation's leading small business advocacy association, representing members in Washington, DC, and all 50 State capitals. Founded in 1943 as a nonprofit, nonpartisan organization, NFIB's mission is to promote and protect the right of its members to own, operate, and grow their businesses. NFIB proudly represents approximately 300,000 members nationwide from every industry and sector.

---

[8] For example, developing suspicious activity models, screening transactions, investigating potentially suspicious activity and filing SARs.

[9] As discussed in BPI's study, because there is no established metric for measuring whether banks' BSA reports are "useful" to law enforcement a proxy was used, which was derived from tracking instances where law enforcement reached out to institutions, including through subpoenas, national security letters or requests for SAR backup documentation.

[10] See "Joint Statement on Innovative Efforts To Combat Money Laundering and Terrorist Financing", (December 3, 2018); available at *www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29__508.pdf.*

[11] See Treasury Order 108-01 (July 1, 2014).

[12] The production of the National Security Strategy and the National Intelligence Priorities Framework both use interagency processes to establish priorities.

[13] See The Clearing House letter to FinCEN on its "Request for Comments Regarding Suspicious Activity Report and Currency Transaction Report Requirements", (April 10, 2018), available at *bpi.com/wp-content/uploads/2018/04/20180410-tch-comment-letter-to-fincen-on-sar-and-ctr-requirements.pdf.*

The NFIB Small Business Legal Center is a nonprofit, public interest law firm established to provide legal resources and be the voice for small businesses in the Nation's courts through representation on issues of public interest affecting small businesses.

The Financial Crimes Enforcement Network's (FinCEN) Customer Due Diligence Rule (CDD) took effect in May of 2018. Although this regulation has only been Federal law for just over a year, Congress is considering replacing the rule with significant statutory expansions. Congress does not have any data on the effectiveness of the CDD Rule in combating money laundering. Yet last week the House Financial Services Committee favorably reported H.R. 2513, the Corporate Transparency Act of 2019. Disappointingly, that committee did not invite testimony from any organizations representing small businesses—the only stakeholders that would be negatively impacted by the legislation.

NFIB appreciates the opportunity to speak for the millions of small business owners who would be negatively impacted by a new small business beneficial ownership reporting requirement and registry. My testimony today will focus on the small business concerns with the Corporate Transparency Act of 2019, and the draft ILLICIT CASH Act—two significant beneficial ownership bills under discussion in the 116th Congress. NFIB opposes legislative proposals such as the Corporate Transparency Act of 2019 and the ILLICIT CASH Act because they impose burdensome, costly, and intrusive requirements to file yet more reports with the Government and threaten the constitutionally protected privacy rights of law-abiding small business owners.

**A Significant New Regulatory Burden for Small Business**

According to the 2016 NFIB Small Business Problems and Priorities report, "unreasonable Government regulations" ranks second—only behind taxes—as the most important problem small business owners face. [1]

In a Small Business Poll on regulations, NFIB found that almost half of small businesses surveyed viewed regulation as a "very serious" (25 percent) or "somewhat serious" (24 percent) problem. [2] NFIB's survey was taken at the end of 2016, and, at that time, 51 percent of small business owners reported an increase in the number of regulations impacting their business over the last 3 years. [3]

Compliance costs, difficulty understanding regulatory requirements, and extra paperwork are the key drivers of the regulatory burdens on small business. [4] Understanding how to comply with regulations is a bigger problem for those firms with one to nine employees, since 72 percent of small business owners in that cohort try to figure out how to comply themselves, as opposed to assigning that responsibility to someone else. [5]

NFIB's research shows that the volume of regulations poses the largest problem for 55 percent of small employers, as compared to 37 percent who are most troubled by a few specific regulations. [6]

Both the Corporate Transparency Act of 2019 and the ILLICIT CASH Act would impose mandatory reporting requirements on those least equipped to handle them—America's small business owners. First, both bills would impose a new paperwork requirement on small business owners by mandating every corporation or LLC with 20 or fewer employees and less than $5 million in gross receipts or sales file beneficial ownership information with FinCEN upon incorporation. Updates would be required annually, under the Corporate Transparency Act of 2019, and within 90 days of the business making any ownership changes under the ILLICIT CASH Act. Either the small business owner, herself, or the accountant or attorney she pays, will have to ensure these documents are filed. One new paperwork requirement may not sound that burdensome to someone who does not run a small business, but it is quite a different story for the individual just starting a business or the small business owner who is adding this new form to the stack of forms he must already fill out and file.

Importantly, it is unclear how small business owners will even find out about these requirements. For many, who have no idea who FinCEN is, there is a strong likelihood they will just ignore the request. And, regardless of their familiarity with

---

[1] Holly Wade, "Small Business Problems and Priorities", NFIB Research Foundation, 17, (August, 2016), available online at *https://www.nfib.com/assets/NFIB-Problems-and-Priorities-2016.pdf*

[2] Holly Wade, "Regulations", Vol. 13, Issue 3, 2017, 6, available online at *http://411sbfacts.com/files/Regulations%202017.pdf* (last visited May 16, 2018).

[3] Id.

[4] Id.

[5] Id. at 10.

[6] Id. at 9.

FinCEN, many small business owners will view this data collection request with great skepticism. For example, every single year NFIB receives countless calls asking about the Census Bureau's Annual Business Survey form and whether the small business owner really needs to take the time to fill out and divulge the information required. It is unrealistic to assume that small business owners will simply fill out this new form and submit personal information, including a passport number/driver's license and date of birth, to a Government agency many have not heard of before with no questions asked. A well-meaning small business owner who fails to file because she (1) never finds out about this new reporting requirement or (2) is skeptical about the legitimacy and appropriateness of this new form would be exposed to civil penalties of up to $10,000 and criminal penalties of up to 3 years in prison.

In addition to finding out about this new reporting requirement and accepting it as a legitimate information request, small business owners would then be tasked with determining what information to provide. Determining who is and is not a "beneficial owner" to be reported will not be a quick and easy task for the average small business owner. Although the calculation of anyone who owns 25 percent or more of the corporation or LLC should be straightforward, determining who "exercises substantial control" of, or "receives substantial economic benefit" from the corporation or LLC many times will not be. Imagine the small, family-run restaurant employing 10–15 persons. After 15 years of operation, the manager of the restaurant is the same person who helped open it. The financial owners of the restaurant trust her 100 percent in all operations of the business. The financial owners are recent empty-nesters and like to travel. As a result, the manager has complete control over the restaurant's operations for several weeks each year. She also receives an annual bonus based on the gross receipts of the business. Does she "exercise substantial control" under either or both bills thereby making her personal information, including driver's license/passport number, reportable? How is an average small business owner to determine the answer to that question on his own? And, is that even a question his outside, paid lawyer would be able to answer with the kind of certainty needed to comply with a law imposing civil and criminal penalties for the wrong answer?

Most important, when NFIB surveyed its membership on this specific type of legislation in August of 2018, the opposition was overwhelming. Specifically, 80 percent of respondents opposed Congress requiring small business owners to file paperwork with the Treasury Department reporting on beneficial ownership.[7]

**Unprecedented Privacy Concerns**

These legislative proposals also raise serious privacy concerns for small business owners. Both bills require the Treasury Department to keep the beneficial ownership information for the life of the business plus 5 years and grant broad access to the information to Federal, State, local, or tribal government agencies[8] through a simple request.[9]

Under the CDD Rule, law enforcement is required to acquire a subpoena in order to obtain a company's beneficial ownership information from a financial institution unless that information is submitted to FinCEN with a suspicious activity report. The Corporate Transparency Act would allow any law enforcement agent access to this information without a subpoena or warrant. The ILLICIT CASH Act would allow "any Government agency" access to this information without a warrant or a subpoena.

These bills are antithetical to current statutes on the books, which—even for sensitive kinds of national security activities, such as protection against international terrorism or clandestine intelligence activities—require the Federal Government to focus its investigative interest on someone in particular, some business in par-

---

[7] When asked, "Should Congress require small business owners to file paperwork with the Financial Crimes Enforcement Network each time they form or change ownership of a business?" a mere 11 percent said "yes" and a resounding 80 percent said "no," with 9 percent undecided. (NFIB survey, August 2018).

[8] The Corporate Transparency Act of 2019 would allow Federal, State, and local law enforcement agencies to access information.

[9] See proposed 31 U.S.C. 5333(a)(4)(A) (retention for 5 years after entity termination) and (B) (disclosure upon request from Federal, State, local, or tribal agency). Indeed, the legislation raises (H.R. 2513) the specter of having the U.S. Government spy on Americans for foreign Governments, as it requires disclosure of the beneficial ownership information in certain circumstances to assist foreign agency investigations and foreign tribunals. See proposed 31 U.S.C. 5333(a)(4)(B)(ii).

ticular, or some account in particular before compelling a bank or other business to produce relevant information. [10]

**Questionable Value to Law Enforcement**

Finally, NFIB questions whether imposing significant and costly beneficial ownership reporting requirements on America's small businesses—from mom and pop groceries to local plumbers—will stop or deter money laundering or other illicit activities. At a hearing before this Committee on this same topic on May 21, 2019, Mr. Kenneth A. Blanco, the Director of FinCEN, said the following in response to questioning from Senator Warner regarding verification of information, "Senator, that gets a little bit more complicated. If what you're asking us to do is verify the information, I'll just be candid with you. That would be a big mistake. There would be no way that FinCEN could be able to verify that information." Without verifying the accuracy of millions of data points being entered into a new FinCEN database, law enforcement could not trust the accuracy of the information collected until they investigate a suspected criminal shell company. Both the Corporate Transparency Act and the draft ILLICIT CASH Act carve out millions of businesses from reporting requirements, including sole-proprietors, partnerships, and business trusts. If a criminal money launderer has any level of sophistication, they will simply set up their new shell company as a partnership or trust and evade law-enforcement detection.

Proponents of these legislative vehicles often cite a Financial Action Task Force (FATF) report from 2016 that identified the "lack of timely access to adequate, accurate and current beneficial ownership information" as a fundamental gap in United States efforts to combat money laundering and terrorist finance. [11] What proponents fail to mention is that this report was published well before the CDD Rule took effect, and beneficial ownership information started to be collected. Law enforcement now has access to this beneficial ownership information through a subpoena. The report also has very flattering words for the current U.S. anti–money-laundering system, including, "The AML/CFT framework in the U.S. is well developed and robust. Domestic coordination and cooperation on AML/CFT issues is sophisticated and has matured since the previous evaluation in 2006."

Proponents continue to fail to comprehend that FinCEN has no way of verifying the accuracy of beneficial ownership information today and has no plan to verify the accuracy in the future. A key component of FATF's recommendations is the verifiable accuracy of beneficial ownership information. This legislation would not solve that problem. As Director Blanco has admitted, FinCEN has no way of verifying beneficial ownership information.

NFIB opposes both the Corporate Transparency Act and the draft ILLICIT CASH Act because both bills would impose even more regulatory burdens on America's small businesses and establish an unprecedented intrusion into the privacy and civil liberties of millions of small business owners.

Thank you for the opportunity to testify today. I look forward to answering any questions you may have.

---

## PREPARED STATEMENT OF GARY KALMAN

EXECUTIVE DIRECTOR, FINANCIAL ACCOUNTABILITY AND CORPORATE TRANSPARENCY COALITION

JUNE 20, 2019

Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you for holding this important hearing and for inviting me to testify today.

On behalf of the Financial Accountability and Corporate Transparency (FACT) Coalition and our member organizations, I appreciate the opportunity to talk about a foundational reform in the global anticorruption movement and the nexus between secrecy jurisdictions, crime, corruption, human rights, and national security.

---

[10] See, for example, Stored Communications Act, 18 U.S.C. 2709; Fair Credit Reporting Act, 15 U.S.C. 1681u and 1681v; Right to Financial Privacy Act, 12 U.S.C. 3414; and National Security Act, 50 U.S.C. 3162.

[11] The Financial Action Task Force and The Asia-Pacific Group on Money Laundering, "Anti–Money Laundering and Counterterrorist Financing Measures—United States", December 2016.

The FACT Coalition is a nonpartisan alliance of more than 100 State, national, and international organizations working to combat the harmful impacts of corrupt financial practices. [1]

**What Is an Anonymous Company?**

When people create companies in the United States, they are not required to disclose who really profits from their existence or controls their activities—the actual "beneficial owners" of the business. Instead, individuals who benefit can conceal their identity by using front people, or "nominees," to represent the company. For instance, the real owner's attorney can file paperwork under his or her own name even though the attorney has no control or economic stake in the company. Finding nominees is not terribly difficult—there are corporations whose entire business is to file paperwork and stand in for company owners. Additionally, some jurisdictions do not require ownership information at all and other jurisdictions allow for companies to be listed as the owners of companies, adding layers to an opaque corporate structure that makes it difficult—in some cases impossible—to identify the true owners.

**Threats Posed by Anonymous Companies**

There is now overwhelming evidence of the use of anonymous companies for money laundering and other criminal purposes. In addition to human trafficking, drug trafficking, grand corruption, and other criminal enterprises, there is growing evidence that anonymous structures are used to threaten our national security.

In a 2018 advisory, the Financial Crimes Enforcement Network (FinCEN) issued a warning:

> The Iranian regime has long used front and shell companies to exploit financial systems around the world to generate revenues and transfer funds in support of malign conduct, which includes support to terrorist groups, ballistic missile development, human rights abuses, support to the Syrian regime, and other destabilizing actions targeted by U.S. sanctions. [2]

The Center for Sanctions and Illicit Finance at the Foundation for the Defense of Democracies (FDD) described in its 2017 "Terror Finance Briefing Book" how anonymous companies are being abused by rogue Nations and sanctioned organizations. [3] They wrote:

> In February 2017, Treasury sanctioned the Vice President of Venezuela, Tareck El Aissami, for his involvement with the drug trade. That same month, CNN reported that a 2013 confidential intelligence report by a group of Latin American Nations assessed that El Aissami had ordered Venezuelan passports to be fraudulently issued to 173 people in the Middle East, including individuals connected to Hezbollah.
>
> Latin American intelligence officials reportedly told an American researcher that El Aissami created a network of nearly 40 shell companies to launder money, including some that were based in Miami. This network was used by Hezbollah supporters (including the Lebanese Canadian bank), Colombian and Mexican cartels, and Ayman Joumaa, discussed above.

Later in the report, they note:

> Hezbollah supporters run an extensive network of commercial and illicit businesses around the globe, including in South America and Africa, which may morph into new enterprises to avoid scrutiny. By using shell companies, and by renaming companies to avoid U.S. sanctions, Hezbollah-linked groups can continue to access the international financial system and transact with an ever-growing network of companies. The U.S. Treasury Department has designated dozens of Lebanon-based firms for supporting Hezbollah, including real estate firms and auto care companies. It is likely the group will continue its money laundering operations, growing into new fields and businesses in the future. [4]

---

[1] A full list of FACT Coalition members is available at *http://thefactcoalition.org/about/coalition-members-and-supporters/*.

[2] FinCEN, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts To Exploit the Financial System", October 11, 2018, *https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2018-a006*.

[3] Yaya J. Fanusie and Alex Entz, "Terror Finance Briefing Book: Hezbollah Financial Assessment", *Foundation for Defense of Democracies*, September 2017, *http://bit.ly/2ZxNfjf*.

[4] Ibid.

Another disturbing story comes from a report by the anticorruption organization (and FACT Coalition member) Global Witness. In their report, "Hidden Menace", they found numerous incidents in which the U.S. Department of Defense had contracted with anonymous companies that, at best, defrauded the U.S. military and, at worst, endangered the lives of troops serving overseas. In one case, the Pentagon contracted with a U.S. company to supply services to troops in Afghanistan. The company was secretly owned by interests associated with the Taliban. We were literally supplying funds that could be used to purchase guns and other weapons aimed at our troops. [5]

These reports are why nearly 100 civilian and former military national security experts signed a recent letter to Congress in support of the collection of beneficial ownership information.

Alarmingly, these individual stories are not isolated incidents but are part of a larger collection of threats to the safety and security of our communities and our Nation.

According to a 2011 study by the Stolen Asset Recovery Initiative, a joint effort of the World Bank and U.N. Office on Drugs and Crime, anonymous companies were used to hide the proceeds of corruption in 85 percent of the grand corruption cases reviewed, with U.S. entities being the most common. [6]

According to a 2018 study by the anti–human-trafficking group Polaris, anonymous companies play an outsized role in hiding the identities of the criminals behind trafficking enterprises, specifically illicit massage businesses. [7] The report found that:

- Of the more than 6,000 illicit massage businesses for which Polaris found incorporation records, only 28 percent of these illicit massage businesses have an actual person listed on the business registration records at all.
- Only 21 percent of the 6,000 business records found for illicit massage parlors actually specifically name the owner—although, even in those cases, there is no way to know for sure if that information is legitimate.

In the 2018 "National Money Laundering Risk Assessment", the U.S. Department of Treasury wrote that, "The nature of synthetic drug trafficking, and associated financial flows, has changed with the rise of China as a supplier of fentanyl and its analogues and precursors. China is the primary source of fentanyl and fentanyl analogues." The Assessment noted that the U.S. Drug Enforcement Agency determined there is an Asian version of the Black Market Peso Exchange "with goods being exported to China by U.S. front companies as payment for drugs."

Anonymous companies are also used to undermine our markets and disrupt legitimate business. There are numerous examples in which anonymous companies disrupt supply chains, fraudulently compete for contracts, and engage in illicit commerce through the selling of counterfeit and pirated goods.

In a recent FACT Coalition report authored by David M. Luna, a former U.S. national security official and the current chair of the Anti–Illicit Trade Committee of the United States Council for International Business, examined the role of anonymous companies in facilitating a growing global illegal economy valued at between $500 billion and $3 trillion. [8] We found:

- Anonymous companies have helped criminals across the United States sell in recent years several billion dollars in fake and counterfeited luxury handbags and apparel accessories branded as Burberry, Louis Vuitton, Gucci, Fendi, Coach, and Chanel, as well as sportswear and gear from the NFL, NBA, and MLB including Nike, Adidas, and Under Armour, among many others.
- Anonymous companies were used to import and sell to American consumers, through internet pharmacies, counterfeit medicines from India and China worth hundreds of millions of dollars. These counterfeits included fake versions of Arimidex, a breast cancer treatment, Lipitor, the cholesterol drug, Diovan, for high blood pressure, and other medications such as illicit OxyContin, Percocet, Ritalin, Xanax, Valium, and NS Ambien.

---

[5] *Global Witness*, "Hidden Menace: How Secret Company Owners Are Putting Troops at Risk and Harming American Taxpayers", July 12, 2016, *http://bit.ly/HiddenMenace.*

[6] Stolen Asset Recovery (StAR) Initiative, "The Puppet Masters", World Bank and UNODC, Nov. 2011, pp. 34 and 121, *http://bit.ly/PuppetMasters.*

[7] Polaris, "Hidden in Plain Sight: How Corporate Secrecy Facilitates Human Trafficking in Illicit Massage Parlors", April 2018, *http://bit.ly/2JEO4lB.*

[8] David M. Luna, "Anonymous Companies Help Finance Illicit Commerce and Harm American Businesses and Citizens", The FACT Coalition, May 2019, *http://bit.ly/2LCOV99.*

- Anonymous companies assisted in selling knock-off parts to the Pentagon that have cost the U.S. military tens of millions of dollars.
- Anonymous companies helped an organized criminal network sell counterfeit cellphones and cellphone accessories on Amazon.com and eBay.com. They also misrepresented goods worth millions of dollars as new and genuine Apple and Samsung products.
- Anonymous companies were leveraged to help criminals sell millions of dollars' worth of counterfeit computer antivirus software over the internet.

Not surprisingly, when businesses were asked, without context, if they would support additional regulation, they did not. However, entrepreneurs understand and manage risk every day. When the organization Small Business Majority asked small business owners if they were more concerned about the risks and burden of reporting ownership of their businesses or the potential loss of contracts to fraudulent anonymous companies, 76 percent said they were more concerned about losing contracts than about the regulatory burden. [9]

The collection of beneficial ownership information strengthens our national security, assists law enforcement, and creates a safer business environment for the vast majority of honest businesses.

**The U.S. Is Particularly Vulnerable to the Abuses of Anonymous Companies**

A 2017 report by the Government Accountability Office (GAO) found that, "GAO was unable to identify ownership information for about one-third of GSA's 1,406 high-security leases as of March 2016 because ownership information was not readily available for all buildings." [10] This finding was a leading factor in Congress voting to adopt a provision in the FY2018 National Defense Authorization Act for the Department of Defense to collect beneficial ownership information for all high security office space it leases.

A 2014 study by academics from the University of Texas-Austin (UT-Austin), Brigham Young University (BYU), and Griffith University found that among the 103 countries they studied, the United States is the easiest place for suspicious individuals to incorporate an anonymous company. [11]

According to a 2019 Global Financial Integrity analysis, "The Library Card Project: The Ease of Forming Anonymous Companies in the United States", in all 50 States and the District of Columbia, "more personal information is needed to obtain a library card than to establish a legal entity that can be used to facilitate tax evasion, money laundering, fraud, and corruption." [12]

It is data like these that led the Financial Action Task Force—the world's recognized body for establishing anti–money-laundering standards and of which the U.S. is a founding member—to find in its 2016 mutual evaluation of the U.S. that the lack of beneficial ownership information was a significant gap in the U.S. anti–money-laundering framework. [13]

Progress in the rest of the world means the U.S. is likely to become an even more attractive haven for illicit cash unless we act. In 2016, the United Kingdom became one of the first countries to collect beneficial ownership information. In 2015, the European Union agreed that all 28-member States would establish beneficial ownership directories.

**Addressing Concerns, Negotiating Workable Proposals**

Throughout a decade long debate, some concerns have been raised about various proposals. Negotiations with multiple parties have made the current proposals, like the ILLICIT CASH Act, more workable and compliance easier for businesses. The changes have led several organizations and constituencies to drop their earlier opposition and others to become advocates for reform.

---

[9] Small Business Majority, "Opinion Poll: Small Business Owners Support Legislation Requiring Transparency in Business Formation", April 4, 2018, *https://smallbusinessmajority.org/our-research/government-accountability/small-business-owners-support-legislation-requiring-transparency-business-formation.*

[10] Government Accountability Office, "GSA Should Inform Tenant Agencies When Leasing High Security Space From Foreign Owners", Jan. 3, 2017; *http://bit.ly/2JiDFwI.*

[11] Michael Findley, et al. "Global Shell Games: Experiments in Transnational Relations, Crime, and Terrorism", *Cambridge University Press* (March 24, 2014), p. 74. *http://bit.ly/2uTLptQ.*

[12] Press Release, "Report Demonstrates Ease of Establishing Anonymous Shell Companies", Global Financial Integrity, March 21, 2019, accessible at *https://www.gfintegrity.org/press-release/report-demonstrates-ease-of-establishing-anonymous-shell-companies/.*

[13] Financial Action Task Force, "Anti–Money Laundering and Counterterrorist Financing Measures—United States", Fourth Round Mutual Evaluation Report, Dec. 2016; *http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.*

*Small Business*

The proposals call for the collection of four pieces of readily known and accessible information—name, address, date of birth, and a drivers' license or other identification number of the owner. This is less information than is required for an individual to obtain a library card in any of the 50 States. [14]

In the U.K., an analysis by Global Witness of data collected by the British beneficial ownership directory found that the average number of owners per business in the U.K. is 1.13. The most common number of owners is one. More than 99 percent of businesses listed less than six owners. [15]

According to the U.S. Small Business Administration, approximately 78 percent of all businesses in the U.S. are nonemployer firms, meaning there is only one person in the enterprise. [16] This suggests that the experience in the U.S. would be similar to that of the U.K.

Additionally, to my knowledge, there has not been a problem in implementing the beneficial ownership rules now in place in the U.S. Defense Department when leasing high security office space. And a main concern regarding the Treasury Department's Geographic Targeting Orders (GTOs), a pilot program to collect beneficial ownership information for high-end, cash-financed real estate transactions in 12 metropolitan areas, is that they are temporary and keep changing in scope and location. One consistent, predictable rule would seem to be preferable.

New proposals, such as the bipartisan discussion draft of the ILLICIT CASH Act [17] and the House of Representative's Corporate Transparency Act of 2019 (H.R. 2513, which was reported favorably out of the Committee on Financial Services last week with a strong bipartisan vote [18]), have found creative ways to use, where practicable, existing structures though which companies can update their information.

This is why, when asked, more than three quarters of small business owners felt the tradeoff—reporting burden vs. benefits—was worth it. [19]

*Privacy*

While there are disagreements about whether this information should be made public, the proposals introduced over the last decade chose to keep the information private. The discussion draft of the ILLICIT CASH Act and the Corporate Transparency Act of 2019 both see FinCEN as the best repository of this information.

The rationale behind that decision is that FinCEN is our Nation's financial intelligence unit with the responsibility of housing and reviewing data to protect our financial system from abuse by terrorist networks and other criminals who seek access to our markets and our strong and stable economy. Law enforcement officials and financial institutions with legally required anti–money-laundering responsibilities have existing relationships with FinCEN.

FinCEN also has a strong track record of safeguarding sensitive data. According to public information on FinCEN's portal system, it appears that the database has strict limitations on who can access information and how that information can be used. The database is accessed through a physical portal, meaning that a local police officer could not log on during a routine traffic stop. Users must be trained and certified and must undergo a background check. All searches must be done as part of an ongoing investigation, and every file that is reviewed is logged so that there is a record of who accessed what information. Misuse of the information is a criminal act. [20]

---

[14] Global Financial Integrity.

[15] Global Witness, "Hard Data on Lessons Learned From the U.K. Beneficial Ownership Register", May 2019; *http://bit.ly/2FhwX6u*.

[16] Small Business Administration, "Frequently Asked Questions", September 2012; *https://www.sba.gov/sites/default/files/FAQ__Sept__2012.pdf*.

[17] Senator Mark Warner, "Warner, Cotton, Jones, Rounds, Unveil Draft Legislation To Improve Corporate Transparency and Combat Financing of Terrorism, Money Laundering", U.S. Senate, June 10, 2019, *http://bit.ly/2ZsmGfo*.

[18] Committee on Financial Services, "Committee Passes Legislation To Protect Housing Rights, Reform National Flood Insurance Program and Strengthen the Financial System", U.S. House of Representatives, June 12, 2019, *https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=403895*.

[19] Small Business Majority, "Opinion Poll: Small Business Owners Support Legislation Requiring Transparency in Business Formation", April 4, 2018, *https://smallbusinessmajority.org/our-research/government-accountability/small-business-owners-support-legislation-requiring-transparency-business-formation*.

[20] Global Witness, "Memo: Basic Information on Use and Access to the FinCEN Portal (a.k.a., the FinCEN Database, or Gateway)", June 1, 2019; *http://bit.ly/2ILqp0M*.

*Accountability*

Like all laws, there are penalties for violating the law. However, the proposals over the last decade have ensured that mistakes by honest businesses will not be penalized. Negligence is not a punishable offense. That means that honestly forgetting to update the information—if, for example, a family member joins a business—is not punishable.

The proposals specifically state that only knowing and willfull violations are punishable. In fact, the standards in the bill provide greater protections for filers against errant prosecutions than the American Bar Association's model guidelines in this area recommend.[21]

**Collecting Beneficial Ownership Information Has an Impact**

The limited data available, since there are very few examples of collecting the information to date, suggests the policy will have a measurable impact.

In 2016, FinCEN implemented Geographic Targeting Orders (GTOs). In an early analysis, FinCEN found that, "Within this narrow scope of real estate transactions covered by the GTOs, FinCEN data indicate that about 30 percent of reported transactions involve a beneficial owner or purchaser representative that was also the subject of a previous suspicious activity report. This corroborates FinCEN's concerns about this small segment of the market in which shell companies are used to buy luxury real estate in "all-cash" transactions. In addition, feedback from law enforcement indicates that the reporting has advanced criminal investigations."[22]

A second study of the impact of the GTOs, in 2018, by the New York Federal Reserve and the University of Miami found, "After anonymity is no longer freely available to domestic and foreign investors, all-cash purchases by corporations fall by approximately 70 percent, indicating the share of anonymity-seeking investors using LLCs as 'shell corporations.'"[23]

*The British Experience*

The United Kingdom implemented the first beneficial ownership directory, and their experience can be instructive. As I previously mentioned, Global Witness did an analysis of the U.K. data in 2019.[24] Among the many findings was the successful early collaboration between Companies House (the Government agency hosting the beneficial ownership directory) and law enforcement.

They found:

- ". . . a huge spike in Suspicious Activity Reports filed by Companies House, with 2,264 reports being filed between April 2017 and April 2018, as compared with 426 reports the preceding year."
- ". . . enquiries from law enforcement to Companies House for help in investigations increased from an average of 11 requests per month to 125 per month in the last 3 years. While the increase has slowed, it continues to grow by more than 50 percent (2017/18)."
- A "major drop" in U.K.-incorporated "vehicles previously associated with crime[.] After becoming part of the new transparency rules, incorporation levels of Scottish Limited Partnerships—a vehicle previously implicated in countless money-laundering scandals—plummeted by 80 percent in the last quarter of 2017 from their peak at the end of 2015. [Global Witness's] analysis this year [in 2019] confirms it remains at historically low levels."

*Cutting Off Legitimate Channels to the Financial System for Illicit Actors*

We also need to recognize that, today, criminals have open access to our financial system. Legitimate gatekeepers in the legal and accounting professions assist clients

---

[21] See: "A Lawyer's Guide To Detecting and Preventing Money Laundering", American Bar Association, International Bar Association, and Council of Bars and Law Societies of Europe, October 2014; accessible at *http://bit.ly/ABA-AML-Guide.*

[22] Steve Hudak, "FinCEN Targets Shell Companies Purchasing Luxury Properties in Seven Major Metropolitan Areas", FinCEN, August 22, 2017; *https://www.fincen.gov/news/news-releases/fincen-targets-shell-companies-purchasing-luxury-properties-seven-major.*

[23] Hundtofte, C. Sean, and Rantala, Ville, "Anonymous Capital Flows and U.S. Housing Markets" (May 28, 2018). University of Miami Business School, Research Paper No. 18-3. Available at SSRN: *https://ssrn.com/abstract=3186634* or *http://dx.doi.org/10.2139/ssrn.3186634.*

[24] Global Witness, "Getting the U.K.'s House in Order", May 6, 2019; *https://www.globalwitness.org/en/campaigns/corruption-and-money-laundering/anonymous-company-owners/getting-uks-house-order/.*

that may well be laundering money but have no responsibility to ask even the most basic questions.[25]

Earlier in my testimony, I referenced a 2014 study by academics at UT-Austin, BYU, and Griffiths University that found that the United States is the easiest place in the world for suspect individuals to establish an anonymous company. The researchers sent out thousands of inquiries to corporate formation agents in over 100 countries with details that should have raised red flags for the recipients. An agent in Florida responded to a request in an email saying:

> Your stated purpose could well be a front for funding terrorism . . . if you wanted a functioning and useful Florida corporation, you'd need someone here to put their name on it, set up bank accounts, etc. I wouldn't even consider doing that for less than 5k a month . . .[26]

While clearly crossing ethical lines, this individual did nothing illegal. By requiring the collection of beneficial ownership information, gatekeepers across the country would no longer engage with these shady clients—thereby cutting off access to the U.S. financial system through legitimate channels.

**Conclusion**

The FACT Coalition came together in 2011. One primary concern among the international development and antipoverty groups that formed the core of the Coalition's leadership was the wealth drain from the developing world. Corrupt leaders were siphoning money from their national treasuries leaving few resources for basic services, impoverishing local populations and propping up dictators and autocrats who engaged in widespread abuses of human rights. The realization that the illicit proceeds were being moved into the U.S. through anonymous companies gave rise to the effort to rein in corporate secrecy.

Over the years, leaks and a number of painstaking investigations, including several by the Senate Permanent Subcommittee on Investigations, uncovered the ubiquitous use of anonymous companies for a wider array of illicit acts—terrorist financing, sanctions evasion, human trafficking, drug trafficking, the illicit trade in counterfeit and pirated goods, Medicare fraud, tax evasion, and more. The threats to our local communities and our Nation has brought together an unprecedented set of allies all calling for reform.

Support for ending the incorporation of anonymous companies has expanded beyond the core anticorruption community to now include national security experts,[27] cops,[28] sheriffs,[29] local prosecutors,[30] State Attorneys General,[31] Federal prosecutors,[32] human rights advocates,[33] anti–human-trafficking groups,[34] faith-based networks,[35] international development NGOs,[36] CEOs,[37] big businesses,[38] small

---

[25] Steve Kroft (60 Minutes), "Anonymous, Inc.", CBS News, January 31, 2016; accessible at *https://www.cbsnews.com/news/anonymous-inc-60-minutes-steve-kroft-investigation/*.

[26] Findley, et al.

[27] Bipartisan Letter from 91 National Security Experts, June 10, 2019, available at *http://bit.ly/2ZvJECj*.

[28] Letter from the Fraternal Order of Police, May 6, 2019, available at *http://bit.ly/2KoYC9W*.

[29] Letter from the National Sheriffs' Association, May 7, 2019, available at *http://bit.ly/2Fk7vxd*.

[30] Letter from the National District Attorneys Association, May 6, 2019, available at *http://bit.ly/2KoJDg9*.

[31] Bipartisan Letter from Two Dozen State Attorneys General, August 2, 2018, available at *http://bit.ly/2J5Bla3*.

[32] Letter from the National Association of Assistant United States Attorneys, May 6, 2019, available at *http://bit.ly/2L0fkvU*.

[33] Letter from Amnesty International USA, EarthRights International, EG Justice, Enough Project, Freedom House, Global Witness, Human Rights First, Human Rights Watch, International Corporate Accountability Roundtable, and the International Labor Rights Forum, April 11, 2019, available at *https://www.hrw.org/news/2019/04/11/letter-chairwoman-waters-and-ranking-member-mchenry-re-corporate-transparency-act*.

[34] See, for example, Letter from Polaris, May 2, 2019, available at *http://bit.ly/2WSJeUS*; and Letter from Street Grace, March 10, 2019, available at *http://bit.ly/2WOoti6*.

[35] Letter from Jubilee Network USA, March 12, 2019, available at *http://bit.ly/2IXMXLU*.

[36] Letter from ActionAid USA, Bread for the World, Jubilee USA Network, The ONE Campaign, and Oxfam America, June 7, 2019, available at *http://bit.ly/2MYVPpY*.

[37] Letter from the CEOs of a dozen major companies, April 30, 2019, available at *http://bit.ly/31Gcd1L*.

[38] Richard Sawaya, "A Maximum Pressure Campaign Against the Kremlin", *The Hill*, April 30, 2019, *https://thehill.com/opinion/international/441350-a-maximum-pressure-campaign-against-the-kremlin*.

businesses,[39] banks,[40] credit unions,[41] real estate professionals,[42] insurance companies,[43] over 125 nongovernmental organizations,[44] and scholars at both conservative[45] and liberal think tanks,[46] among others.

We hope this hearing provides members an opportunity to better understand the dangers posed by anonymous companies and move to address them. We thank you for this opportunity to share our views, and we look forward to working with you on this important issue.

[39] Letter from Small Business Majority, April 25, 2019, available at *http://bit.ly/2KtteqK.*

[40] See, for example: Letter from nine banking associations, May 7, 2019, available at *http://bit.ly/2XpRlwx*; Letter from the Independent Community Bankers of America, May 8, 2019, available at *http://bit.ly/31Rbc7o*; and Letter from 51 State Banking Associations, June 10, 2019, available at *http://bit.ly/2Kow6Fh.*

[41] Letter from the Credit Union National Association, June 11, 2019, available at *http://bit.ly/2KttIgy.*

[42] Letter from the American Escrow Association, American Land Title Association, National Association of REALTORS, and Real Estate Services Providers Council, Inc. (RESPRO), May 7, 2019, available at *http://bit.ly/2E2KQoq.*

[43] Letter from the Coalition Against Insurance Fraud, April 15, 2019, available at *http://bit.ly/2KYYygz.*

[44] Letter from 127 Groups Supporting Corporate Transparency Act of 2019, June 10, 2019, available at *http://bit.ly/2L7yjon.*

[45] See, for example: Clay R. Fuller, "Dealing With Anonymity in Business Incorporation", American Enterprise Institute, March 29, 2019, *https://www.aei.org/publication/dealing-with-anonymity-in-business-incorporation/.*

[46] See, for example: Molly Elgin-Cossart and Trevor Sutton, "The Real Scandal Behind the Panama Papers", Center for American Progress, May 10, 2016, *https://www.americanprogress.org/issues/security/news/2016/05/10/137191/the-real-scandal-behind-the-panama-papers/.*

## RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM GREG BAER

**Q.1.** As the ranking member of the Senate Foreign Relations Committee and an author of several pieces of sanctions legislation, I do not believe the transparency rules on shell companies in our country are enough to catch criminal foreign actors such as kleptocratic oligarchs, drug cartels, and rogue Governments or individuals seeking to evade sanctions. The fact is, the U.S. is still an easy place to hide money.

Would you agree that anonymous companies formed in the U.S. make it more difficult for law enforcement and national security officials to enforce sanctions and combat kleptocracy? If so, please explain.

**A.1.** Yes, as I noted in my testimony, the U.S. is an easy and safe place for criminals to hide behind the corporate veil by keeping their ownership secret from law enforcement, national security, and banks tasked with doing due diligence on their clients.

Anyone in the world looking to disguise the source or ownership of their funds can establish a U.S. shell company and keep the ownership of that company anonymous. That anonymity serves as a wall for law enforcement and national security officials tasked with safeguarding our system. Sophisticated criminals operate through multiple shell companies, whose linkages are not clear.

Every year financial institutions spends billions of dollars to prevent and detect money laundering. Such efforts target those engaged in organized crime, terror financing, human trafficking, kleptocracy, and other offenses, and attempt to thwart those seeking to avoid sanctions. Yet those efforts are thwarted by the loophole in the U.S. regulatory framework that permits the evasion of sanctions, enabling kleptocrats and other illicit actors to access the U.S. financial system despite the best efforts of law enforcement and national security officials.

**Q.2.** Would you agree that this has undermined the effectiveness of our sanctions regimes on Russia, Venezuela, Iran, North Korea, and others? If so, please explain.

**A.2.** Yes, the Bank Policy Institute agrees that the lack of a beneficial ownership requirement in the United States represents a gaping hole in our AML/CFT framework and undoubtedly contributes to the evasion of sanctions by illicit State actors, including the countries you referenced. As detailed by the Center for New American Security in their December 2018 report, "Financial Networks of Mass Destruction", "the efforts to prevent the financing of [weapons of mass destruction] proliferation are only in their infancy. The legal framework to prevent the financing of proliferation is weak, and implementation across the world is spotty . . . . Stepping up action to combat the financing of proliferation will take legal change at home, including financial transparency measures and new methodologies to facilitate information sharing between banks and between banks and national authorities."

**Q.3.** Would requiring companies to disclose their true beneficial owners at the time of formation assist law enforcement in their investigations and help keep Americans safe from national security threats? If so, please explain.

**A.3.** Yes. As I detailed in my testimony, anonymous shell companies are a key method used by criminals to hide assets for a range of dangerous and illicit activities, including human trafficking, terrorist financing, money laundering, and kleptocracy. All too often criminal investigations hit a dead end when law enforcement encounters a company with hidden ownership and lacks the time and resources to peel back the many layers of secrecy currently permitted by U.S. law. And the more sophisticated and sinister the criminal, the more layers there generally are.

This problem is not difficult to solve. It has been solved by most countries around the world. Generally, our country does more than any other to identify and block the proceeds of crime, however we are among the worst when it comes to allowing criminals to use the corporate form to cloak ownership; as a result, the United States has become a safe haven for those who wish to hide the proceeds or instruments of illegal activity. We have therefore been repeatedly criticized by the Financial Action Task Force, an intergovernmental AML standard setting body, for this deficiency in our system.

Requiring companies to disclose their true beneficial owners at the time of formation would provide law enforcement, and the financial institutions required to collect this information, with the key information required to pursue investigations and protect national security.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM KAREN HARNED**

**Q.1.** As the ranking member of the Senate Foreign Relations Committee and an author of several pieces of sanctions legislation, I do not believe the transparency rules on shell companies in our country are enough to catch criminal foreign actors such as kleptocratic oligarchs, drug cartels, and rogue Governments or individuals seeking to evade sanctions. The fact is, the U.S. is still an easy place to hide money.

Would you agree that anonymous companies formed in the U.S. make it more difficult for law enforcement and national security officials to enforce sanctions and combat kleptocracy? If so, please explain.

Would you agree that this has undermined the effectiveness of our sanctions regimes on Russia, Venezuela, Iran, North Korea, and others? If so, please explain.

Would requiring companies to disclose their true beneficial owners at the time of formation assist law enforcement in their investigations and help keep Americans safe from national security threats? If so, please explain.

**A.1.** As the Executive Director of the NFIB Small Business Legal Center, I have expertise in how regulatory and legal statutes and proposals affect small business owners. I am not an expert on law enforcement, national security, foreign policy, or international sanctions. Therefore, I cannot comment with authority on any of the questions you proposed.

However, I will direct you to the comments of an expert. FinCEN Director Blanco testified at a hearing before this Committee on

May 21, 2019. In response to questioning from Senator Warner regarding verification of information he said, "Senator, that gets a little bit more complicated. If what you're asking us to do is verify the information, I'll just be candid with you. That would be a big mistake. There would be no way that FinCEN could be able to verify that information." Without verifying the accuracy of millions of data points being entered into a FinCEN database, law enforcement could not trust the accuracy of the information collected until they begin an investigation into a suspected criminal entity.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SINEMA FROM KAREN HARNED**

**Q.1.** Under the ILLICIT CASH Act, what kind of information would small businesses need to supply the Financial Crimes Enforcement Network (FinCEN) upon incorporation? Would this beneficial ownership information be different from other information business owners are currently required to provide to financial institutions when opening an account?

**A.1.** Under the draft ILLICIT CASH Act businesses with 20 or fewer employees and less than $5 million in gross receipts would need to file the following information of all beneficial owners:

- full legal names,
- business or residential addresses,
- dates of birth,
- jurisdictions of formation,
- dates of formation,
- Employer Identification Numbers (EIN), or, if the business is not an employer, driver's license or passport number.

Under the Financial Crimes Enforcement Network's (FinCEN) Customer Due Diligence (CDD) Rule, an individual opening an account must provide their name and title, as well as the name and address of the legal entity for which the account is being opened. Businesses must report the following information of all beneficial owners to financial institutions when opening new accounts:

- full legal names,
- dates of birth,
- business or residential addresses,
- Social Security numbers, or passport number for noncitizens. [1]

The draft ILLICIT CASH Act would require similar information but differs in that it requires jurisdictions of formation, dates of formation, EINs, and driver's license or passport numbers instead of Social Security numbers for a U.S. citizen.

Only businesses opening new accounts since the CDD Rule became applicable (May 11, 2018) have been required to report this information to financial institutions. The draft ILLICIT CASH Act would require all existing businesses to submit reports. Small businesses would report more beneficial owners as it contains a broader

[1] See Appendix A to section 1010.230—Certification Regarding Beneficial Owners of Legal Entity Customers, Customer Due Diligence Rule, (May 11, 2016) available online at *https://www.regulations.gov/document?D=FINCEN-2014-0001-0183.*

definition of beneficial ownership, including those who receive substantial economic benefits from the assets of an organization.

**Q.2.** What kind of privacy concerns would sharing this information with FinCEN raise?

**A.2.** The draft ILLICIT CASH Act raises serious privacy concerns for small business owners. This draft bill requires the Treasury Department to keep the beneficial ownership information for the life of the business plus 5 years and grant broad access to the information to Federal, State, local, or tribal government agencies through a simple request.

Under the CDD Rule, law enforcement is required to acquire a subpoena to obtain a company's beneficial ownership information from a financial institution unless that information is submitted to FinCEN with a suspicious activity report.[2] The ILLICIT CASH Act would allow "any Government agency" access to this information without a warrant or a subpoena.

These bills are antithetical to current statutes on the books, which—even for sensitive kinds of national security activities, such as protection against international terrorism or clandestine intelligence activities—require the Federal Government to focus its investigative interest on someone in particular, some business in particular, or some account in particular before compelling a bank or other business to produce relevant information.[3]

A Federal database with personally identifiable information of small business owners would be a target for hacks and leaks, despite the proposed increase penalties for leaks.

**Q.3.** Under the ILLICIT CASH Act, what would be the estimated cost of compliance with new beneficial ownership reporting requirements?

**A.3.** NFIB does not have an estimated cost of compliance for new beneficial ownership reporting requirements under the draft ILLICIT CASH Act. FinCEN estimated that the CDD Rule would cost between $700 million and $1.5 billion over a decade.[4] FinCEN estimated that the CDD Rule would impact 13,952 small entities (banks, credit unions, brokers, and mutual funds).

The draft ILLICIT CASH Act massively expands the number of impacted entities and the frequency of reports. The draft bill would capture many more entities than the CDD Rule, including businesses that have yet to open a new account since May 11, 2018. According to the U.S. Census Bureau, there are more than 5.3 million businesses with 20 or fewer employees. The draft bill would also require these businesses to update their information more frequently than the CDD Rule, requiring updates within no more than 90 days if ownership information changes. Due to these factors, we can reasonably estimate increased compliance costs.

Some commenters to the CDD Rule suggested the process would look like applying for an Employer Identification Number (EIN)

---

[2] FinCEN did not estimate the cost of privacy loss of the CDD Rule.

[3] See, for example, Stored Communications Act, 18 U.S.C. 2709; Fair Credit Reporting Act, 15 U.S.C. 1681u and 1681v; Right to Financial Privacy Act, 12 U.S.C. 3414; and National Security Act, 50 U.S.C. 3162.

[4] Regulatory Impact Assessment for FinCEN Notice of Proposed Rulemaking: "Customer Due Diligence Requirements for Financial Institutions", Docket No. FinCEN-2014-0001.

from the IRS. The IRS estimates that applying for an EIN takes 10 hours and 10 minutes in total:

- 8 hours and 36 minutes for recordkeeping
- 42 minutes for learning about the law or the form
- 52 minutes for preparing, copying, assembling, and sending the form to the IRS[5]

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM GARY KALMAN**

**Q.1.** Just last month the FACT coalition released a report on how anonymous shell companies fuel trade in counterfeit goods. The FACT report points out alarming examples of how criminals used shell companies to funnel the profits of counterfeit medicines made in China, India, and elsewhere that were sold online to unsuspecting U.S. consumers. Some of the medicines involved were well-known drugs like OxyContin, Lipitor, Xanax, and others. These cases had real health impacts on Americans that thought buying online could save them money, only to find out later that the medicines had incorrect active ingredients or the wrong dose.

How would beneficial ownership legislation help crack down on our country's growing problem of counterfeit medicines and other goods sold online?

**A.1.** Counterfeit goods pose a series of threats to Americans. A 2017 report from the International Chamber of Commerce and the International Trademark Association projected that the global economic value of counterfeit and pirated goods alone will reach close to $3 trillion by 2022—enriching criminals, undercutting legitimate businesses, threatening jobs and public health and safety. The same study predicts that total employment losses globally due to counterfeiting and piracy will rise from 2–2.6 million jobs lost in 2013 to 4.2–5.4 million jobs lost in 2022.[1]

Beyond the direct economic damage, the illicit trade in counterfeit and pirated goods is a major threat to public health and consumer safety. In the case of counterfeit pharmaceuticals, incorrect ingredients or doses may not work or, perhaps worse, they can be physically harmful. Counterfeit food products have been known to include potentially toxic ingredients, and counterfeit electronics have exploded—causing physical injury. Honest American businesses lose money when counterfeit or pirated goods steal market share from them, and they risk reputational damage when products sold in their name don't work or cause physical harm.

The problem faced by law enforcement is that the products are often marketed and sold through anonymous corporate structures. Corporate secrecy makes it harder, sometimes impossible, for law enforcement to track down the perpetrators. Delayed investigations mean more U.S. consumers are exposed to potentially harmful

---

[5] See Privacy Act and Paperwork Reduction Act Notice, Instructions for Form SS-4, Application for Employer Identification Number, IRS, available online at *https://www.irs.gov/pub/irs-pdf/iss4.pdf*.

[1] *Frontier Economics*, "The Economic Impacts of Counterfeiting and Piracy—Report prepared for BASCAP and INTA", February 6, 2017, *https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf*.

products, and businesses continue to lose money and risk longer term reputational damage.

Should law enforcement get close to identifying the bad actors behind these scams, these individuals can shut down one anonymous company and quickly open another to continue to sell their potentially dangerous products.

Beneficial ownership transparency would make it far more difficult for criminals to access U.S. markets and the U.S. financial system. Some criminals may take the risk. If they do, law enforcement would be able to more quickly shut down the operation and hold the criminals accountable. Others will not take the risk. Some will look for nominee directors or stand in owners. Under current law, nominees can and do sign their names on the proper forms on behalf of illicit actors and have no liability. If the legislation is passed, those nominees would be criminally liable. The legislation would either chase the counterfeiters from U.S. markets or make it far more difficult to find front line accomplices.

As I mentioned in my testimony, beneficial ownership transparency is not the only reform necessary to prohibit this type of illicit activity, but it is the necessary foundation on which to build. We can stiffen fines and penalties but if we allow anonymous companies to legally abuse our corporate formation laws in this fashion, law enforcement will not have the necessary tools to do their jobs to protect the American people.

**Q.2.** Is there not a danger that foreign actors can engage in political money laundering by using anonymous LLCs incorporated in the United States to contribute money to super PACs, and thereby illegally influence U.S. elections?

What steps can be taken, both by Congress and the Administration, to remove this threat?

**A.2.** There have been reported instances of foreign actors using anonymous companies to influence our elections. The anonymity allows foreign agents to do an end run around existing laws against foreign expenditures in U.S. elections.

Like the issue of counterfeit goods, beneficial ownership transparency will guard against easy and open access to the U.S. financial system. In relation to foreign political interference, the impact would be even more immediate than with counterfeit goods. A company registered in the Cayman Islands may do business in the U.S., but that same company cannot engage in election spending. If foreign agents seek to spend on our elections, the only way to escape accountability is to incorporate U.S.-based anonymous companies and channel the foreign funds through them. Our current laws enable this type of abuse of our corporate formation system.

**Q.3.** As the ranking member of the Senate Foreign Relations Committee and an author of several pieces of sanctions legislation, I do not believe the transparency rules on shell companies in our country are enough to catch criminal foreign actors such as kleptocratic oligarchs, drug cartels, and rogue Governments or individuals seeking to evade sanctions. The fact is, the U.S. is still an easy place to hide money.

Would you agree that anonymous companies formed in the U.S. make it more difficult for law enforcement and national security of-

ficials to enforce sanctions and combat kleptocracy? If so, please explain.

**A.3.** Yes. There are numerous examples of anonymous companies being used to undermine our national security. Here are just a few examples taken from a fact sheet produced by my Coalition:[2]

- *Anonymous companies facilitate the financing of weapons of mass destruction.* Anonymous companies have been featured in proliferation financing cases involving North Korea, Syria, and Pakistan. In a particularly notable example of a "serial proliferator," a Chinese national named Li Fang Wei (a.k.a. Karl Lee) repeatedly formed anonymous entities to carry out procurement activity, even as his businesses were sanctioned by the U.S.
- *Anonymous companies were used to lease high security space to the Government, creating security risks.* The Government Accountability Office "was unable to identify ownership information for about one-third of GSA's 1,406 high-security leases as of March 2016 because ownership information was not readily available for all buildings." This included the FBI—renting space owned by a corrupt Malaysian official and his family. In addition to providing funding to money-laundering operations that the FBI was supposed to be investigating, potential risks include security breaches and cyberattacks.
- *Anonymous companies assisted an illegal weapons dealer when moving hardware into war zones.* Viktor Bout, a.k.a. "the Merchant of Death", used a global network of anonymous shell companies, including at least 12 incorporated in Delaware, Florida, and Texas, to disguise weapons trafficking into conflict zones around the world.
- *Anonymous companies defrauded the U.S. military, put our troops at risk, and overcharged for basic supplies.* A former America's Most Wanted fugitive made millions by defrauding the U.S. taxpayers of $11.2 million during a time of armed conflict. He supplied shoddy, dangerous parts essential to well-functioning weapons and to the safety of troops under the disguise of nominee companies created in California, Florida, New Jersey, New York, Nevada, Oregon, Texas, Washington, and Canada. Separately, a U.A.E.-based anonymous company was used to overcharge American taxpayers in a $48 million scheme to supply food and water to troops in Afghanistan.

In addition, the Kleptocracy Initiative at the Hudson Institute has produced numerous reports linking anonymous companies to the enabling of kleptocrats. The Kleptocracy Initiative's research features studies—including "Weaponizing Kleptocracy: Putin's Hybrid Warfare",[3] "How Non-State Actors Export Kleptocratic Norms

[2] The FACT Coalition, "FACT Sheet: Anonymous Companies and National Security", May 17, 2019, *https://thefactcoalition.org/fact-sheet-anonymous-companies-and-national-security-may-2019?utm__medium=policy-analysis/fact-sheets.*

[3] Marius Laurinavicius, "Weaponizing Kleptocracy: Putin's Hybrid Warfare", *Hudson Institute*, June 6, 2017, *https://www.hudson.org/research/13666-weaponizing-kleptocracy-putin-s-hybrid-warfare.*

to the West",[4] and "Countering Russian Kleptocracy",[5] among others—that highlight the different ways kleptocracies can infiltrate Western institutions and undermine U.S. national security.

**Q.4.** Would you agree that this has undermined the effectiveness of our sanctions regimes on Russia, Venezuela, Iran, North Korea, and others? If so, please explain.

**A.4.** Yes. There are numerous examples in which anonymous companies have been used to evade sanctions. Corporate secrecy allows rogue Nations and individuals to easily do so.

As I mentioned in my testimony, Iran was able to evade economic sanctions by purchasing property in Manhattan through the use of anonymous companies, including one registered in New York.

According to a report by the Foundation for the Defense of Democracies, "In February 2017, Treasury sanctioned the Vice President of Venezuela, Tareck El Aissami, for his involvement with the drug trade. That same month, CNN reported that a 2013 confidential intelligence report by a group of Latin American Nations assessed that El Aissami had ordered Venezuelan passports to be fraudulently issued to 173 people in the Middle East, including individuals connected to Hezbollah. Latin American intelligence officials reportedly told an American researcher that El Aissami created a network of nearly 40 shell companies to launder money, including some that were based in Miami. This network was used by Hezbollah supporters (including the Lebanese Canadian bank), Colombian and Mexican cartels, and Ayman Joumaa, discussed above."[6]

In 2016, McClatchy News ran a story that began: "In her passport, Nesita Manceau lists her occupation as 'housewife.' But she does oh-so-much more. On paper at least, she's a corporate titan. And she's been tangled in an arms-running scandal involving North Korea and Iran."[7]

The story goes on to explain how nominee owners are used to mask the identities of the beneficial owners engaged in nefarious activities who, in fact, control the anonymous enterprises.

These are just few examples to demonstrate that anonymous companies are used by rogue Nations and individuals to undermine sanctions.

**Q.5.** Would requiring companies to disclose their true beneficial owners at the time of formation assist law enforcement in their investigations and help keep Americans safe from national security threats? If so, please explain.

**A.5.** Yes. As stated above, there are now volumes of evidence of anonymous corporate structures being abused in ways that potentially threaten our national security. Additional studies and arti-

---

[4] Ilya Zaslavskiy, "How Non-State Actors Export Kleptocratic Norms to the West", *Hudson Institute*, September 7, 2017, *https://www.hudson.org/research/13875-how-non-state-actors-export-kleptocratic-norms-to-the-west.*

[5] Ben Judah and Nate Sibley, "Countering Russian Kleptocracy", *Hudson Institute*, April 5, 2018, *https://www.hudson.org/research/14244-countering-russian-kleptocracy.*

[6] Yaya J. Fanusie and Alex Entz, "Terror Finance Briefing Book: Hezbollah Financial Assessment", *Foundation for Defense of Democracies*, September 2017, *http://bit.ly/2ZxNfjf.*

[7] Tim Johnson, "Did This Panama Papers Housekeeper Really Direct a North Korean Arms Deal?" *McClatchy*, May 10, 2016, *https://www.mcclatchydc.com/news/nation-world/national/article76635047.html.*

cles from scholars at the Atlantic Council, American Enterprise Institute, Brookings Institution, Carnegie Endowment for International Peace, Center for a New American Security, Center for Strategic and International Studies, Council on Foreign Relations, Foundation for the Defense of Democracies, Hoover Intuition, Hudson Institute and others have all detailed how anonymous companies threaten our national security and frustrate U.S. efforts to counter those threats.

This is why more than 100 former military and civilian national security experts signed letter to Congress urging the adoption of beneficial ownership transparency legislation. In March, General David Petraeus coauthored a guest opinion piece in the *Washington Post* with Senator Sheldon Whitehouse describing the threats posed by anonymous companies and calling for reform. The U.S. Department of Justice and the U.S. Department of Treasury in both Republican and Democratic Administrations have spoken out on the need for reform. Twenty-four State Attorneys General sent a letter to Congress last year and the following law enforcement organizations have all called for beneficial ownership transparency:

- ATF Association
- Federal Law Enforcement Officers Association (FLEOA)
- National Association of Assistant United States Attorneys (NAAUSA)
- National District Attorneys Association (NDAA)
- National Fraternal Order of Police (FOP)
- National Sheriff's Association
- Society of Former Special Agents of the FBI
- U.S. Marshals Service Association

---

## RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN FROM GARY KALMAN

**Q.1.** Boston is experiencing a building boom, especially in the luxury sector. According to a recent report, 35 percent of units in the 12 highest-priced luxury developments built in Boston from 2008–2018 were purchased by limited liability companies or trusts that obscure the beneficial owners.[1] A large number of those units were purchased by anonymous foreign buyers with cash.[2]

What role does high-cost real estate play in the international money-laundering framework?

**A.1.** High cost real estate plays an increasingly prominent role in international money laundering. In the Boston report that you mention, "Towering Excess", researchers determined that, "These [high-priced condominium buildings], however, play a key role in the global hidden wealth infrastructure, a shadowy system that's hiding wealth and masking ownership, all for the purpose of helping the holders of private fortunes avoid taxes and oversight of il-

---

[1] Institute for Policy Studies, "Towering Excess: The Perils of the Luxury Real Estate Boom for Bostonians", Chuck Collins and Emma de Goede, September 2018, *https://ips-dc.org/wp-content/uploads/2018/09/ToweringExcessReport-Sept10.pdf.*

[2] Id.

licit activities. Many Boston luxury properties are functioning, in effect, as wealth storage lockers for global capital."

This report is consistent with others done in other U.S. cities and cities abroad. Transparency International U.K. had similar findings in two reports, *Faulty Towers*[3] and *Corruption on your Doorstep*,[4] regarding the London real estate market.

In Manhattan, eight blocks between Lenox Hill and Central Park is nearly 40 percent unoccupied, and on the Upper East Side more than a quarter of the properties are owned but vacant.[5] These properties could be occupied by permanent low- and moderate-income residents, but instead they are being priced out by those looking to hide or protect assets.

In San Francisco, the South Beach neighborhood is one-fifth unoccupied,[6] and—in the competitive California housing market—the rent crisis is affecting low- and moderate-income families.

Wealthy bad actors from abroad use anonymous companies to purchase real estate to undermine economic sanctions, avoid fund transfer limits out of their home Nations, evade taxes, launder money, and store corrupt cash.

These rogue individuals, along with rich speculators, bid up prices on properties, and then use them as a "bank" rather than a home. This helps to fuel the loss of affordable housing in growing numbers of communities due to skyrocketing real estate prices and vastly inflated markets.

**Q.2.** Why might Boston be a destination for foreign illicit investment?

**A.2.** Massachusetts, like every State in the country, allows for the incorporation of anonymous companies. Delaware's corporate secrecy may be more infamous, but no State collects beneficial ownership information.[7] However, Boston is particularly attractive because, like New York and Miami, the real estate market is strong. It is a comparatively safe investment over time. Or, should the illicit investors need their money, they have a reasonably high assurance of selling quickly.

From my time in the Boston area, it is a terrific place to live, but these individuals are not concerned about the quality of the schools or access to job opportunities. They are solely focused on safely parking their money until such a time as they need it.

**Q.3.** What impact does the purchase of real estate through anonymous shell companies play in housing prices across the country?

**A.3.** A 2016 story in the *Miami Herald* about the impact of offshore money on the local housing market found that, " . . . the boom also sent home prices soaring beyond the reach of many working- and

---

[3] Transparency International U.K., "Faulty Towers: Understanding the Impact of Overseas Corruption on the London Property Market", March 2017, *https://www.transparency.org.uk/publications/faulty-towers-understanding-the-impact-of-overseas-corruption-on-the-london-property-market/*.

[4] Transparency International U.K., "Corruption on Your Doorstep", February 2015, *https://www.transparency.org.uk/publications/corruption-on-your-doorstep/*.

[5] Joseph Lawler, "Money Laundering Is Shaping U.S. Cities", *Washington Examiner*, March 27, 2017, *https://www.washingtonexaminer.com/money-laundering-is-shaping-us-cities.*

[6] Id.

[7] Press Release, "Report Demonstrates Ease of Establishing Anonymous Shell Companies", *Global Financial Integrity*, March 21, 2019, accessible at *https://www.gfintegrity.org/press-release/report-demonstrates-ease-of-establishing-anonymous-shell-companies/*.

middle-class families. Locals trying to buy homes with mortgages can't compete with foreign buyers flush with cash and willing to pay the list price or more." [8]

Inflated housing prices from these foreign investors create multiple problems. Higher prices lock middle-income households out from purchasing in neighborhoods close to jobs and schools. The increased demand for high-end housing also incentivizes developers to build more high-end properties, further reducing the affordable housing stock.

In addition to the national security and law enforcement concerns that receive the most attention, anonymous companies are playing an increasing role in the lack of affordable housing in certain jurisdictions in the United States.

**Q.4.** In November 2018, the Treasury Department's Financial Crimes Enforcement Network issued a Geographic Targeting Order for Boston, which requires title insurance companies to identify the individual who is purchasing a property above $300,000. [9] Is that sufficient to keep illicit money from being parked in Boston real estate?

**A.4.** The Geographic Targeting Orders (GTOs) are an important step in protecting against illicit actors purchasing real estate, but they are not perfect. The GTOs collect ownership information through title insurance agents but cash financed transactions do not necessarily involve purchasing title insurance. The definition of beneficial owner in the GTOs is not as strong and comprehensive as in various legislative proposals. The GTOs are, by statute, temporary and, while they have been extended, they cannot be extended forever.

The FACT Coalition strongly supports the GTOs and encourages their continued extension and expansion, but there are limitations.

---

[8] Nicholas Nehamas, "How Secret Offshore Money Helps Fuel Miami's Luxury Real-Estate Boom", *Miami Herald*, April 3, 2016, *https://www.miamiherald.com/news/business/real-estate-news/article69248462.html.*

[9] *Financial Crimes Enforcement Network*, "FinCEN Reissues Real Estate Geographic Targeting Orders and Expands Coverage to 12 Metropolitan Areas", November 15, 2018, *https://www.fincen.gov/news/news-releases/fincen-reissues-real-estate-geographic-targeting-orders-and-expands-coverage-12.*

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

## LETTER SUBMITTED BY THE NATIONAL ASSOCIATION OF FEDERALLY-INSURED CREDIT UNIONS

NAFCU
3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org
National Association of Federally-Insured Credit Unions

June 19, 2019

The Honorable Michael Crapo
Chairman
Committee on Banking, Housing
& Urban Affairs
United States Senate
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing
& Urban Affairs
United States Senate
Washington, DC 20510

**Re: Tomorrow's Hearing: Outside Perspectives on the Collection of Beneficial Ownership Information**

Dear Chairman Crapo and Ranking Member Brown:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) in regard to tomorrow's hearing entitled "Outside Perspectives on the Collection of Beneficial Ownership Information." NAFCU advocates for all federally-insured not-for-profit credit unions that serve over 117 million consumers with personal and small business financial service products.

Credit unions support efforts to combat criminal activity in the financial system. NAFCU has consistently recognized the importance of the Financial Crimes Enforcement Network (FinCEN), *Bank Secrecy Act* (BSA), and Anti-Money Laundering (AML) requirements in assisting in the prevention of tax evasion, money laundering, and terror financing. Our members maintain a good relationship with FinCEN and consistently inform us that the publication of AML/BSA guidance is very helpful. However, BSA requirements remain a burden to implement. We urge the Committee to continue to look for ways to provide credit unions with regulatory relief by reforming and strengthening BSA laws.

We are pleased that the discussion draft of a reform bill recently released by Senators Mark Warner, Tom Cotton, Doug Jones, and Mike Rounds addresses beneficial ownership. Among other provisions, NAFCU supports language that would assist credit unions and other financial institutions in complying with the new Customer Due Diligence (CDD) Rule by requiring companies to disclose to FinCEN their true beneficial ownership information. FinCEN would use this information to create a database that would be available to law enforcement agencies and financial institutions. However, we would strongly urge the Committee to consider language allowing customer consent for financial institutions to access such a database, similar to the text found in H.R. 2513, the *Corporate Transparency Act of 2019*, from Representative Carolyn Maloney.

NAFCU appreciates the Committee's focus on ways to improve BSA/AML regulatory compliance, and we look forward to collaborating with the Committee on this important issue. Should you have any questions or require additional information, please do not hesitate to contact me or Max Virkus, NAFCU's Associate Director of Legislative Affairs, at 703-842-2261.

Sincerely,

Brad Thaler

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Senate Banking Committee

**LETTER SUBMITTED BY THE AMERICAN BAR ASSOCIATION**

AMERICAN BAR ASSOCIATION

Robert M. Carlson
President
321 N. Clark Street, Chicago, IL 60654-7598
T 312.988.5109 • F 312.988.5100
abapresident@americanbar.org
americanbar.org

June 19, 2019

The Honorable Michael Crapo
Chairman
Committee on Banking, Housing,
and Urban Affairs
United States Senate
Washington, D.C. 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing,
and Urban Affairs
United States Senate
Washington, D.C. 20510

Re: Hearing on "Outside Perspectives on the Collection of Beneficial Ownership Information" and Concerns Regarding S. ____, the "Improving Laundering Laws and Increasing Comprehensive Information Tracking of Criminal Activity in Shell Holdings Act" (ILLICIT CASH Act)

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the American Bar Association (ABA), I write to express our views regarding the draft "Improving Laundering Laws and Increasing Comprehensive Information Tracking of Criminal Activity in Shell Holdings Act" (ILLICIT CASH Act). We ask that this letter be included in the record of the hearing on "Outside Perspectives on the Collection of Beneficial Ownership Information" that the Committee has scheduled for June 20.

The ABA supports reasonable and necessary domestic and international measures to combat money laundering and terrorist financing. We commend the sponsors of the draft bill for their efforts in this regard and would welcome the opportunity to continue to meet and discuss workable options for addressing these problems. However, the ABA opposes the overly broad language in Section 402 ("Expansion of Geographic Targeting Orders") requiring attorneys representing clients in real estate transactions to file detailed reports with the Treasury Department, as well as the proposed regulatory approach set forth in Section 401 ("Beneficial Ownership"), for the following important reasons.

**First, the ABA opposes Section 402 of the draft bill because it is overly broad and would undermine client confidentiality, the attorney-client privilege, and the confidential attorney-client relationship.**

Section 402 of the bill instructs the Treasury Secretary to issue a new rule requiring "any person involved in a transaction related to the purchase and sale of real estate" to file a detailed report containing the name of the natural person purchasing the real estate, the amount and source of the funds received, the date and nature of the transaction, and "such other information, including the identification of the person filing the report, as the Secretary may prescribe." Because transactional attorneys often represent and assist clients in the purchase and sale of real estate, Section 402 would cover many attorneys engaged in the practice of law and subject them to this reporting requirement.

Although the ABA takes no position on whether the buyers or sellers of real estate should be required to file these types of reports with the Treasury Department's Financial Crimes Enforcement Network

(FinCEN), the ABA is concerned that by requiring attorneys to report the identity of their clients, the amount and source of funds used by clients in real estate transactions, and other confidential client information to FinCEN, Section 402 is plainly inconsistent with ABA Model Rule of Professional Conduct 1.6 dealing with "Confidentiality of Information" and with the many binding state rules of professional conduct that closely track the ABA Model Rule.[1]

The range of client information that attorneys are not permitted to disclose under ABA Model Rule 1.6 is broader than that covered by the attorney-client privilege. Although Model Rule 1.6 prohibits attorneys from disclosing information protected by the attorney-client privilege and the work product doctrine, it also forbids attorneys from voluntarily disclosing other non-privileged information that the client wishes to keep confidential. In most jurisdictions, this category of non-privileged, confidential client information includes the identity of the client as well as other information related to the legal representation that the client may choose to reveal to the attorney but does not wish to be revealed to third parties.[2] Because Section 402 would require attorneys representing clients in real estate transactions to disclose the identity of those clients and other confidential information concerning the transaction, the legislation conflicts with Model Rule 1.6 and the binding state rules of professional conduct that mirror the ABA Model Rule.

These reporting requirements in Section 402 would also undermine the attorney-client privilege, the confidential attorney-client relationship, and the right to effective legal representation by discouraging full and candid communications between clients and their attorneys.

Although the identity of the client is not protected by the attorney-client privilege in most jurisdictions, other information specifically required to be disclosed by Section 402—such as details about the real estate transaction, the amount or source of its funding, or "other information…the Secretary may prescribe"—could be privileged in certain circumstances. Therefore, requiring transactional attorneys to disclose this information to FinCEN would undermine the attorney-client privilege.

In addition, attorneys for clients buying or selling real estate play a key role in helping those clients to understand and comply with the applicable law and to act in their best interest. To fulfill this important societal role, attorneys must enjoy the trust and confidence of their clients, must be provided with all relevant information necessary to properly represent them, and must be able to consult with them confidentially. Only in this way can the attorney engage in a full and frank discussion of the relevant legal issues with the client and provide appropriate legal advice.

---

[1] ABA Model Rule of Professional Conduct 1.6 states that "a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent…" or unless one or more of the narrow exceptions listed in the Rule is present. See ABA Model Rule 1.6, and the related commentary, available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html. See also Charts Comparing Individual Professional Conduct Rules as Adopted or Proposed by States to ABA Model Rules, at http://www.americanbar.org/groups/professional_responsibility/policy.html.

[2] See, e.g., Alabama Ethics Op. 89-111 (1989) (attorney may not disclose name of client to funding agency).; Texas Ethics Op. 479 (1991) (law firm that obtained bank loan secured by firm's accounts receivable may not tell bank who firm's clients are and how much each owes); South Carolina Ethics Op. 90-14 (1990) (attorney may not volunteer identity of client to third party); and Virginia Ethics Op. 1300 (1989) (in absence of client consent, nonprofit legal services corporation may not comply with federal agency's request for names and addresses of parties adverse to certain former clients, since that may involve disclosure of clients' identities, which may constitute secret).

By requiring transactional attorneys to file detailed reports with FinCEN stating the identity of their clients, the amount and source of funds used by the clients in real estate transactions, and other confidential or privileged client information, Section 402 would chill and undermine the confidential attorney-client relationship. In addition, by imposing these unfair reporting burdens on transactional attorneys, the legislation will discourage many buyers and sellers of real estate from seeking the expert legal representation that they need, thereby effectively denying them their fundamental right to counsel.

**Second, the ABA opposes Section 401 of the draft bill because it would impose burdensome, costly, and unworkable new regulatory burdens on millions of small businesses.**

Section 401 of the bill would require small businesses with twenty or fewer employees and gross receipts or sales of $5 million or less to disclose detailed information about their beneficial owners—including their legal names; dates of birth or formation; business or residential addresses; nationalities or jurisdictions of formation; and passport, driver's license, personal identification card, or employer identification numbers—to FinCEN and then update that information continuously during the lifespan of those businesses. Failure to timely submit this information or to update it within 90 days of any change could subject the businesses to harsh civil and criminal penalties, including stiff fines and prison sentences, for essentially paperwork violations.

Unlike the definition of "beneficial owner" under FinCEN's Customer Due Diligence (CDD) rule (as discussed below), the bill's definition of "beneficial owner" is vague, overly broad, and unworkable. The bill's definition includes every natural person who directly or indirectly exercises "substantial control" over the company, owns 25 percent or more of its equity interests, or receives "substantial economic benefits" from its assets, subject to several exceptions. The bill further defines a person with "substantial control" to mean a natural person who "has an entitlement to the funds or assets of the entity that, as a practical matter, enables the person, directly or indirectly, to control, manage, or direct the entity" or is otherwise able to control the entity as defined by a future Treasury Department rule. But other key phrases—such as "directly or indirectly" and "as a practical matter"—remain undefined, making the definition even more ambiguous and unworkable. Because the beneficial owner definition is so expansive and unclear and would cover many individuals whose personal information is not even within the businesses' knowledge or control, it would be almost impossible for many small businesses to comply with the bill's disclosure requirements.

The new federal regulatory regime created by the bill, combined with the broad and confusing definition of beneficial owner, would be costly, impose onerous burdens on legitimate businesses, and subject them to harsh civil and criminal penalties if they fail to comply. In addition, it is difficult to see how the legislation would be effective in fighting money laundering, terrorist financing, or other crimes.

**Third, the draft bill raises serious privacy concerns for small businesses and the many individuals who would be designated as beneficial owners.**

Section 401 of the bill would require FinCEN to maintain this sensitive personal information in a government database and disclose it upon request to any federal, state, tribal or local governmental agency or to any foreign law enforcement agency if certain conditions are met. While similar

beneficial ownership legislation considered by the 115th Congress would have required an agency to secure a criminal or civil subpoena or summons before obtaining the information, the current draft bill would require FinCEN to disclose the information in response to a simple agency request pursuant to undefined "appropriate protocols."

FinCEN would also be required to disclose the information to any financial institution with "customer consent." But because financial institutions will likely require all customers to provide such one-time consent when opening new accounts, the beneficial owners' identities and other personal information will be freely shared with the financial institutions and their affiliates without further permission by, or knowledge of, the customers. As this personal information is shared with more and more entities, the potential for cybersecurity breaches, misuse, or unauthorized disclosure will grow exponentially.

In recognition of these risks, the draft bill would create criminal penalties for the misuse or unauthorized disclosure of beneficial ownership information and would require the Treasury Department's Inspector General to investigate cybersecurity breaches that result in "substantial unauthorized access and disclosure of sensitive beneficial ownership information." But because both remedies would address the problems only *after* the damage has already occurred, the relief is simply too little, too late.

**Fourth, the burdensome beneficial ownership reporting requirements in Section 401 of the draft bill are unnecessary and duplicative because the federal government already has other, more effective tools to fight money laundering and terrorist financing.**

In 2016, FinCEN issued its new CDD rule requiring banks and other covered financial institutions to collect certain specific beneficial ownership information regarding entities that establish new accounts, and the rule became fully effective in May 2018.[3] But unlike the draft bill, the CDD rule includes a specific, understandable, sensible definition of "beneficial owner" consisting of each individual who owns 25 percent or more of the entity and a single individual with significant responsibility for managing the entity. Other FinCEN regulations also require financial institutions to collect or update beneficial ownership information on certain customers with existing accounts on a risk basis during normal monitoring if the institution becomes aware of information relevant to assessing or reassessing the customer's risk profile. Therefore, FinCEN's existing rules already require the collection of information about key individuals who own or control most business entities with a new bank account, as well as the beneficial owners of existing account holders with an elevated risk profile.

In addition to the beneficial ownership information collected under FinCEN's CDD rule and other regulations, the Internal Revenue Service (IRS) collects entity-related information needed to fight money laundering and terrorist financing, and that information is currently available to law enforcement authorities. Since 2010, the IRS has required every business that obtains an Employer Identification Number to submit IRS Form SS-4, which includes the name of a "responsible party"

---

[3] See FinCEN's Final Rule on Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016), available at https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf. For additional information concerning the CDD Rule, see FinCEN's "Frequently Asked Questions" available at https://www.fincen.gov/sites/default/files/2016-09/FAQs_for_CDD_Final_Rule_%287_15_16%29.pdf and https://www.fincen.gov/sites/default/files/2018-04/FinCEN_Guidance_CDD_FAQ_FINAL_508_2.pdf.

within the business, i.e., an individual who is able to "control, manage, or direct the entity and the disposition of its funds and assets."

Together, FinCEN's CDD rule and other regulations, combined with the IRS' SS-4 Form, provide the federal government with access to substantial beneficial ownership information on almost every business entity in the United States (i.e., almost all business entities with at least one employee, a new account, or an existing account with elevated risk). Unlike the draft bill, which requires small corporations, LLCs, and other similar entities to disclose their beneficial owners, the CDD rule and SS-4 Form are more expansive and require many more types of businesses of all sizes—including not just corporations and LLCs, but also general and limited partnerships, business trusts, and other entities—to report their beneficial owners. Therefore, because federal law enforcement authorities are already able to access the information they need to fight money laundering and terrorist financing, it is unnecessary to create a duplicative new regulatory regime that would impose unfair burdens, excessive costs, and the risk of severe civil and criminal liability on millions of small businesses.

For all these reasons, the ABA urges you to amend Section 402 of the draft bill by exempting attorneys representing clients in the purchase or sale of real estate. In addition, we urge you to oppose Section 401 of the draft bill and any similar legislation. Thank you for considering our views on these important issues, and if you have any questions or would like to meet to discuss other possible measures to combat money laundering and terrorist financing, please contact ABA Associate Governmental Affairs Director Larson Frisby at (202) 662-1098 or larson.frisby@americanbar.org.

Sincerely,

Robert M. Carlson

cc: Members of the Senate Banking, Housing, and Urban Affairs Committee

**LETTER SUBMITTED BY THE CONSUMER BANKERS ASSOCIATION**

100 CONSUMER BANKERS ASSOCIATION CENTENNIAL

CBA

HELPING FINANCE THE AMERICAN DREAM SINCE 1919.

June 19, 2019

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the Consumer Bankers Association (CBA), we thank you for holding the hearing entitled, "Outside Perspectives on the Collection of Beneficial Ownership Information." CBA is the voice of the retail banking industry whose products and services provide access to credit for consumers and small businesses. Our members operate in all 50 states, serve more than 150 million Americans and collectively hold two-thirds of the country's total depository assets.

CBA's members serve the critical function of monitoring, identifying and reporting suspicious activity to law enforcement, ensuring criminals do not access the American financial system to launder ill-gotten gains. Our members promote national security and deter financial crimes by committing significant resources towards the compliance of the Bank Secrecy Act (BSA), the USA PATRIOT Act, related anti-money laundering laws (AML) and the recently implemented FinCEN Customer Due Diligence (CDD) rule that requires financial institutions to collect beneficial ownership information on potential business customers and report this information to FinCEN and law enforcement agencies.

We encourage the Committee to consider proposals that would end the use of anonymous shell companies who engage in illegal activities with the purpose of undermining our financial infrastructure. Modernizing the AML/countering the financing of terrorism (CFT) regulations to shift the collection of beneficial ownership information from banks to FinCEN will provide law enforcement with more tools to pursue bad actors. FinCEN is appropriately suited to perform these duties as its purpose is to safeguard the financial system, combat money laundering, and collect, analyze and disseminate financial intelligence.

In addition, Congress should permit FinCEN to create a federal database for financial institutions and law enforcement to use for the purpose of verifying the legitimacy of a company and its owners. A federal database of beneficial ownership information would provide transparency, enable financial institutions and law enforcement to search and rely on the government's information to more efficiently deploy resources in the fight against money laundering, and better protect the nation's financial system from corruption, terrorism, and criminal activity.

1225 EYE STREET, NW, SUITE 550, WASHINGTON, D.C. 20005
consumerbankers.com

CBA welcomes draft bipartisan legislation entitled the "Illicit Cash Act" sponsored by Senators Cotton (R-AR), Warner (D-VA), Rounds (R-SD) and Jones (D-AL) that would bring needed updates to AML/CFT laws and assist law enforcement in combating illicit financial activity. The proposed legislation will make important improvements to the AML/CFT framework and provide lenders with increased regulatory clarity, enhanced communication between stakeholders, greater use of technology and enable FinCEN to collect and verify beneficial ownership information of businesses.

Enhancing law enforcement's ability to prevent criminals from accessing the financial system and conducting illicit activities through the use of anonymous shell companies is a goal we all share. CBA stands ready to work with the Committee to pass legislation that will bring meaningful reforms to the AML/CFT framework and allow for the collection of beneficial ownership legislation at FinCEN.

Sincerely,

Richard Hunt
President and CEO
Consumer Bankers Association

**LETTER SUBMITTED BY THE CREDIT UNION NATIONAL ASSOCIATION**

Credit Union National Association
CUNA

Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

99 M Street SE
Suite 300
Washington, DC 20003-3799

June 19, 2019

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing,
and Urban Affairs
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing,
and Urban Affairs
Washington, DC 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of America's credit unions, I am writing to express our views ahead of the hearing titled "Outside Perspectives on the Collection of Beneficial Ownership Information." The Credit Union National Association (CUNA) represents America's credit unions and their 115 million members.

Credit unions support efforts to track money laundering and terrorist financing, but also believe it is important to strike the right balance between the compliance costs to financial institutions, like credit unions, and the benefits to the federal government. Thus, we are encouraged by the draft legislation *The Improving Laundering Laws and Increasing Comprehensive Information Tracking of Criminal Activity in Shell Holdings (ILLICIT CASH) Act*. This draft bill addresses the redundancies, unnecessary burdens, and opportunities for efficiencies within the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) statutory framework. However, it is important to note that regulatory regimes like the Bank Secrecy Act can cause an undue burden, particularly for smaller financial institutions, and should be a scalable framework.

We appreciate several of the areas addressed in the draft bill, including the following provisions:

Title I:

- Requires that Treasury establish national exam and supervision priorities intended to supplement and guide financial institutions, financial regulators, and law enforcement on handling AML-CFT (combatting the financing of terrorism) threats.

- Establishes a Treasury financial institution liaison to seek and receive comments from financial institutions regarding AML-CFT rules and regulations and examinations, including regarding the banking regulators.

Title II:

- Requires annual reports from DOJ to Treasury on the use of BSA reporting by law enforcement.

- Requires periodic law enforcement feedback to financial institutions on their suspicious activity reports. This periodic feedback shall also be coordinated and conducted in the presence of financial regulators.

- Reviews and streamlines reporting requirements to ensure a "high degree of usefulness" for CTR/ SAR filings, including a review of reporting fields, as well as a review of appropriate ways to promote financial inclusions and avoid unnecessary de-risking.

- Requires Treasury and the Attorney General to review the CTR and SAR thresholds and determine whether any changes are necessary.

- Requires a formal review of all AML-CFT regulations and guidance with public comment to remove outdated or unnecessary regulations and guidance.

Title III:

- Establishes a path for financial institutions to share de-identified AML-CFT information for purposes of identifying suspicious activity.

While there are several positive aspects of the draft bill, we note at least one that is cause for concern for some small credit unions. In Title III, we support the objective of the provision regarding transaction monitoring software intended to improve the risk-based system of tracking individual transactions. However, regardless of the Rule of Construction, it has been our experience that some examiners will expect the credit unions to comply with such "recommendations." We are concerned that "approved" transactions monitoring software could cause a significant financial burden. Understanding some small credit unions are likely to have examination issues with this provision, we ask the Committee to consider how it might be able to address this concern.

On behalf of America's credit unions and their 115 million members, thank you for holding this important hearing.

Sincerely,

Jim Nussle
President & CEO

**LETTER SUBMITTED BY THE FRATERNAL ORDER OF POLICE**

NATIONAL
FRATERNAL ORDER OF POLICE®

328 MASSACHUSETTS AVENUE, NE
WASHINGTON, DC 20002
PHONE 202-547-8189 • FAX 202-547-8190

CHUCK CANTERBURY
NATIONAL PRESIDENT

JAMES O. PASCO, JR.
EXECUTIVE DIRECTOR

20 May 2019

The Honorable Michael D. Crapo
Chairman
Committee on Banking, Housing and Urban Affairs
United States Senate
Washington, D.C. 20510

The Honorable Sherrod C. Brown
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman and Senator Brown,

I am writing on behalf of the members of the Fraternal Order of Police to advise you of our strong support for the collection of beneficial ownership information to combat illicit finance and corruption. The FOP has supported legislation like H.R. 2513, the "Corporation Transparency Act," for many years, and we are grateful that your committee will be holding a hearing on the issue this week.

Transnational criminal organizations and terrorist operations are using our banks, financial institutions and other means to profit from their illegal activity. This is a well-documented problem for our financial institutions and for law enforcement as we work together to shut down these sophisticated criminal enterprises. Congress and this committee have played a leadership role in identifying the problem and worked with law enforcement to develop legislation like H.R. 2513. In addition, this Administration also agrees with this approach—last July, U.S. Secretary of the Treasury Steven T. Mnuchin testified House Financial Services Committee and stated that there is a real need to "have access to beneficial ownership information for law enforcement and for combating terrorist financing."

The Secretary's remarks made it very clear that this is a pressing issue and the vulnerability of our financial institutions is a genuine threat to public safety and national security. Under current laws, shell corporations may be used as front organizations by criminals conducting illegal activity, such as money laundering, fraud, and tax evasion. We need legislation like "Corporation Transparency Act" to combat this misuse of U.S. corporations by requiring the U.S. Department of the Treasury, specifically the Financial Crimes Enforcement Network (FinCEN), to collect beneficial ownership information from corporations and limited liability companies formed under State laws. It is vital that such information, once collected, be available to law enforcement at every level—local, State, tribal and Federal—using the appropriate protocols. For this reason, the FOP opposes any legislation which would have the Internal Revenue Service (IRS) as the entity collecting the beneficial ownership information.

Once FinCEN has the ability to share this information, law enforcement will be able to investigate possible connections between these corporations and terrorist funding. All too often, investigations hit a dead end when we encounter a company with hidden ownership. Just as robbers or burglars wear masks to hide their faces and make identifying them more difficult; the criminals we are chasing in these cases use shell corporations as masks, concealing themselves while still profiting from their crimes.

When we are able to expose the link between shell companies and drug trafficking, corruption, organized crime and terrorist finance, law enforcement will be able to bring these criminals to justice and make our citizens and our nation safer.

On behalf of the more than 348,000 members of the Fraternal Order of Police, I want to thank this committee for its leadership on this issue and most of all, for its willingness to engage and work with the law enforcement community on the collection of beneficial ownership information. We strongly urge the committee to protect our financial system and our nation from criminal and terrorist organizations by passing legislation to collect this vital data. If I can provide any additional information on this matter, please do not hesitate to contact me or my Executive Director, Jim Pasco, in my Washington office.

Sincerely,

Chuck Canterbury
National President

**LETTER SUBMITTED BY THE INDEPENDENT COMMUNITY BANKERS OF AMERICA**

ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

June 20, 2019

## Community Bank Perspective on Collection of Beneficial Ownership Information

On behalf of the more 52,000 community bank locations across the nation represented by ICBA, we thank Chairman Crapo, Ranking Member Brown, and members of the Banking Committee for convening today's hearing on "Outside Perspectives on the Collection of Beneficial Ownership Information." ICBA is pleased to have the opportunity to submit this statement for the hearing record, which addresses developments since this committee's last hearing on May 21, "Combatting Illicit Financing by Anonymous Shell Companies Through the Collection of Beneficial Ownership Information." The attached ICBA white paper, "Modernizing Anti-Money Laundering and Anti-Terrorist Financing Laws and Regulations," provides a more comprehensive exposition of the community bank perspective on this critical issue.

### Draft Legislation

ICBA is pleased that a bipartisan group of Banking Committee members, Senators Warner, Cotton, Jones, and Rounds, has begun an effort to modernize the BSA and the collection of beneficial ownership information. We thank these Senators for encouraging community bank input. We are currently analyzing the draft Illicit Cash Act and welcome the opportunity to meet with this group to convey the community bank perspective.

### The Corporate Transparency Act Advances

In our May 21 statement, we noted our support for the Corporate Transparency Act (H.R. 2513), sponsored by Representative Carolyn Maloney. We are pleased that H.R. 2513 has advanced with bipartisan support out of the House Financial Services Committee. H.R. 2513 would require corporations and limited liability companies that are not exempt to disclose their "beneficial owners" to FinCEN at the time the company is formed and on an annual basis thereafter. Existing companies that are not exempt would be required to report their beneficial owners to FinCEN two years after regulations are finalized. We believe developing a centralized database, such as the one proposed in H.R. 2513, would increase transparency for all parties involved, including law enforcement, rather than the current Customer Due Diligence rule (which is described below).

Any penalties imposed would apply only to fraudulent activity or willful failure to comply. H.R. 2513 creates limitations and waivers to provide relief for persons who violate the requirements through reasonable cause and not due to willful neglect.

Furthermore, we supported changes in the Manager's Amendment in response to concerns raised about the bill. As a result, H.R. 2513 does not create broad access to beneficial ownership information stored by FinCEN. It provides that this information may only be shared with federal, state, local, or tribal law enforcement agencies for law enforcement, national security, or intelligence purposes. Further, Representative Maloney's Manager's Amendment would create robust protocols for safeguarding beneficial ownership information, including limiting access to this

information within law enforcement agencies to authorized users whose identity is verified through appropriate mechanisms, such as two-factor authentication; audit trails of requests for beneficial ownership information, and annual audits to be conducted by law enforcement agencies that have received information as well as by FinCEN.

Finally, H.R. 2513 requires the Secretary of the Treasury to revise the CDD rule to account for financial institutions' access to comprehensive beneficial ownership information filed by corporations and limited liability companies and reduce any burdens on financial institutions that are, in light of the enactment of this Act unnecessary or duplicative.

## Customer Due Diligence Rule

The purpose of the CDD rule is to create more transparency and thereby deter the abuse of anonymous legal entities for money laundering, corruption, fraud, terrorist financing and sanctions evasion.

ICBA agrees that such transparency is important. We strongly disagree that bank collection of beneficial ownership information is an effective means of creating this transparency. Our recommendation is that beneficial ownership information be collected and verified at the time a legal entity is formed by FinCEN or other appropriate federal or state agency. This solution would provide uniformity and consistency across the United States. Making the formation of an entity contingent on receiving beneficial owner information would create a strong incentive for equity owners and investors to provide such information. Additionally, periodic renewal of an entity's state registration would provide an efficient and effective vehicle for updating beneficial ownership information. ICBA believes this solution must be implemented in a way that safeguards the privacy of business owners and ensures the integrity of data held at FinCEN.

Furthermore, information regarding beneficial owners could be more easily shared between law enforcement and government agencies than between banks and law enforcement. Privacy laws do not permit banks to share personal information with a government agency absent a subpoena or similar directive. Information should be collected by the party that can make the most effective use of it to deter the criminal use of legal entities. This is the government.

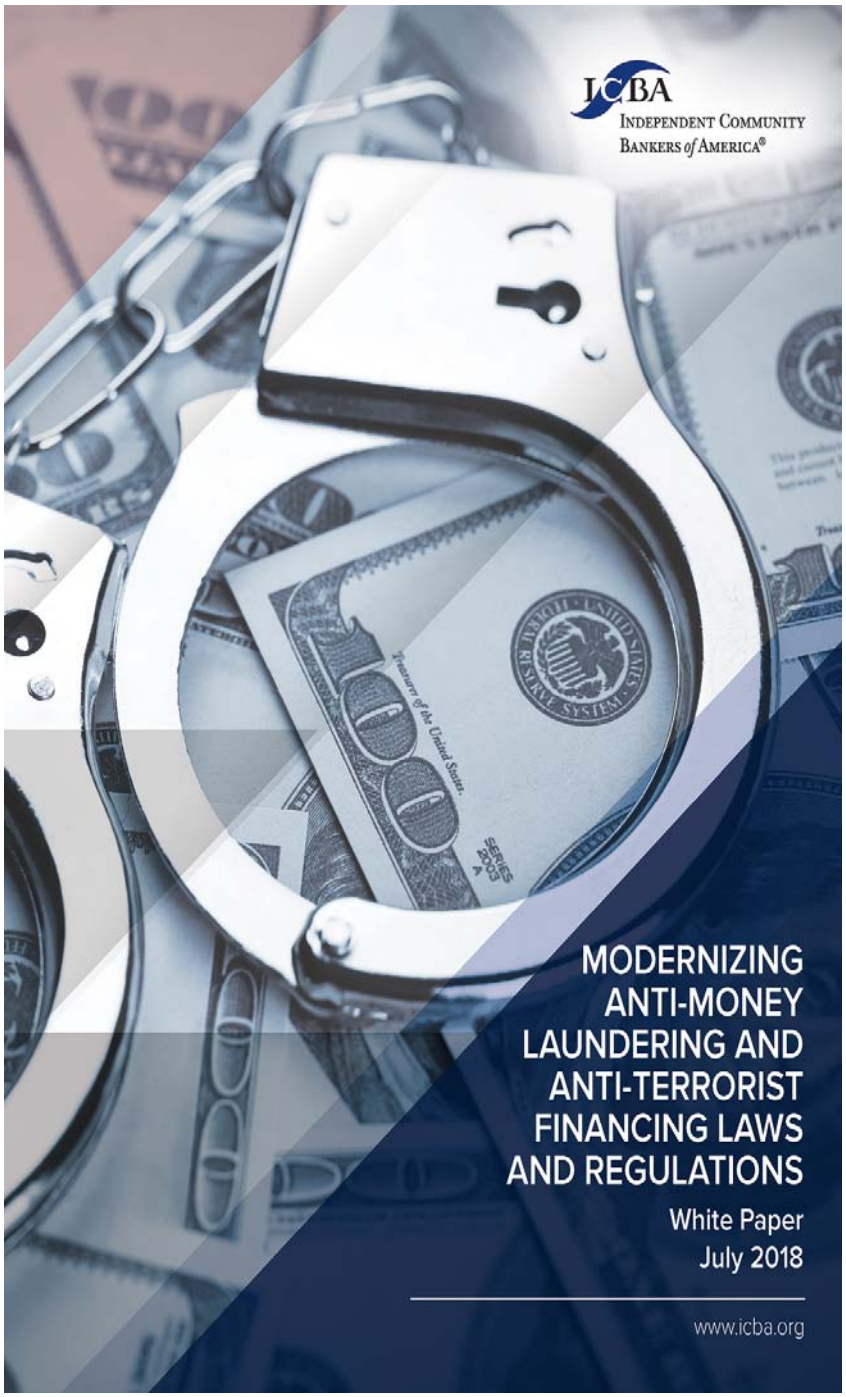
For banks, collection of beneficial ownership information for legal entity customers is difficult to implement and an onerous and inefficient task for both the customer and the employee. While the ownership interest and management responsibility of a business may be straightforward in certain cases and specified in a legal organizational document in other cases, certain legal structures make determining ownership equity extremely difficult, at best. Obtaining this information for legal entities requires a sophisticated understanding of various legal structures and ownership interests that is well beyond the training of a typical community bank loan officer. On the other hand, the provision of this information to FinCEN by business management would create less burden relative to what businesses are required to provide to banks today under the CDD rule.

## Closing

Thank you again for convening today's hearing. ICBA looks forward to working with this committee to reform beneficial ownership information reporting in a way that will strengthen critical law enforcement while rationalizing community bank compliance with this important law.

## Attachment

ICBA White Paper: "Modernizing Anti-Money Laundering and Anti-Terrorist Financing Laws and Regulations"


ICBA
Independent Community
Bankers of America®
MODERNIZING ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING LAWS AND REGULATIONS
White Paper
July 2018
www.icba.org

## TABLE OF CONTENTS

# Introduction

In today's world, it is imperative that financial institutions, law enforcement, and our government work together to combat and prevent financial crime, money laundering, and terrorist financing. Community bankers are committed to supporting balanced, effective measures that will prevent terrorists from using the financial system to fund their operations and prevent money launderers from hiding the proceeds of criminal activities. However, anti-money laundering/combatting the financing of terrorism and Bank Secrecy Act ("BSA") compliance programs (collectively "AML/CFT") consume a growing share of community banks' scarce resources.

Since the inception of the anti-money laundering laws in 1970 and anti-terrorist financing laws in 2001, the burdens placed on banks increasingly create an environment where financial institutions are essentially tasked with identifying, investigating, policing, and reporting potential criminal activity. Each year, community banks must invest more time, money and resources to combat this threat. Yet, community banks report that the current outdated framework is more an exercise of completing forms and strictly adhering to policies and procedures developed from regulatory requirements rather than making an impact in combating financial crime.

A primary challenge facing community banks today is the sharply increasing and disproportionate burden of complying with these growing regulatory requirements.

These regulations also diminish community banks' ability to attract capital, support the financial needs of their customers, serve their communities, and contribute to their local economies. Additionally, many of them do not have dedicated legal and compliance departments and they have a smaller asset base over which to spread compliance costs.

Federal regulators are in the early stages of identifying areas in which burdens can be reduced while maintaining the effectiveness of the AML/CFT regime.

## Modernization will produce more useful information while alleviating compliance burden

Modernization and reform of the BSA will produce more useful information for law enforcement while alleviating one of the most significant and costly sources of community bank compliance burdens. Rather than having banks devote their resources to tasks that are inefficient or redundant, a more efficient and technologically advanced framework would better serve law enforcement and enable community banks to more effectively utilize their resources. BSA modernization will free community bank resources to better serve customers and communities.

ICBA recommends several areas in which the AML/BSA framework can be modernized:

## Update reporting thresholds

As the federal government combats money laundering and terrorist financing, ICBA strongly recommends an emphasis on quality over quantity for all BSA reporting. Reporting thresholds are significantly outdated and capture far more transactions than originally intended. The currency transaction report (CTR) threshold, which was set in 1970, should be raised from $10,000 to $30,000 with future increases linked to inflation.


CTRs are intended to collect information for investigations in tax evasion, money laundering, terrorist financing and other financial crimes. However, the overwhelming percentage of CTRs relate to ordinary business transactions, which create an enormous burden on financial institutions that is not commensurate with financial crime investigations. While the BSA provides banks with the ability to exempt certain customers from CTR reporting, a higher threshold would produce more targeted, useful information for law enforcement.

Suspicious activity reports ("SARs") are the cornerstone of the BSA system and were established as a way for banks to provide leads to law enforcement. Because community banks have a strong incentive to file SARs as a defensive measure to protect themselves from examiner criticism, SARs are filed in increasing and vast numbers without a commensurate

benefit to law enforcement. As the government combats money laundering and terrorist financing, ICBA strongly recommends an emphasis on quality over quantity for SAR filing. ICBA recommends reforming the SAR process by increasing the reporting thresholds, which have not been adjusted since becoming effective in 1992, and by emphasizing those instances in which an institution may rely on risk-based reporting.

### Currently, an institution is required to file a SAR for:

1. criminal violations involving insider abuse in any amount;
2. criminal violations totaling $5,000 or more when a suspect can be identified;
3. criminal violations aggregating $25,000 or more regardless of a potential suspect; and
4. transactions conducted or attempted by, at, or through the bank (or an affiliate) if the bank knows, suspects, or has reason to suspect that the transaction is suspicious.

ICBA recommends the current SARs threshold should be raised from $5,000 to $10,000 which will modernize thresholds by emphasizing quality over quantity in information collection.


In the current regulatory environment, community banks are faced with a cumbersome and overly burdensome process to ensure they are protected and no mistakes are made when reviewed by examiners. They are questioned about the number of SARs filed in relation to the number of accounts and transactions initially identified as suspicious rather than the quality of the bank's monitoring system or investigative process. Additionally, bankers are questioned regarding the total number of SARs filed since the last examination as though a quota is required. As a result, bank employees often file SARs as a defensive measure and to ensure that in hindsight they did not miss or overlook any details and to ensure they filed a requisite number of SARs. The current focus is also a daunting task for banks because it usurps resources by requiring significant time monitoring for thresholds (quantity) and less time focused on actual suspicions (risk).

For each transaction the bank identifies as suspicious, a thorough investigation is conducted that typically includes monitoring and reviewing all documentation and account activity, interviewing appropriate personnel, a review of the investigation by a BSA-trained employee, and sometimes a second review by either a compliance or BSA committee, BSA officer or senior level staff. The investigation is documented, with documents retained on transactions for which a SAR is filed as well as for investigations for which a SAR is not filed. If a SAR is not filed, banks must document and subsequently justify to their examiner why a flagged transaction did not result in a filed SAR. This is done for every suspicious transaction no matter how minor or severe the potential offense. The process is time consuming and labor intensive and community banks are skeptical that the method by which SARs are completed provides commensurate value to law enforcement.

Moreover, the archaic and labor-intensive nature of the SAR process makes the SAR regime ineffective and cumbersome. As stated previously, community banks follow the same SAR procedure for every suspicious transaction no matter how minor the potential offense. This approach leaves community banks skeptical that SARs have real value to law enforcement.

Increasing filing thresholds for both SARs and CTRs would enable community banks to provide more targeted and valuable information to law enforcement.

## Collection of beneficial ownership information by federal or state government

On May 11, 2018, the Financial Crimes Enforcement Network's ("FinCEN") new beneficial ownership rule, which requires banks to collect information on the beneficial owners of legal entity accounts, became effective. FinCEN defines a legal entity customer as a corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction, that opens an account.

FinCEN states that legal entities are at times abused to obfuscate ownership interests and used to engage in illegal activities such as money laundering, corruption, fraud, terrorist financing and sanctions evasion. Criminals have exploited the anonymity that legal entities can provide to engage in a variety of crimes, and often take advantage of shell and front companies to conduct such activity. Making legal entities more transparent by requiring identifying information of natural person owners would likely hinder such

abuses. However, shifting the responsibility and oversight of collecting this information to the private sector—financial institutions—is misguided and ineffective.


Collecting and verifying the identity of all natural-person owners of each entity by either the Internal Revenue Service or other appropriate federal agency and/or state in which the entity is formed would provide uniformity and consistency across the United States. By making the formation of an entity contingent on receiving beneficial owner information, strong incentives would be created for equity owners and investors to provide such information. Additionally, periodic renewal of an entity's state registration would provide an efficient and effective vehicle for updating beneficial ownership information.

The customer due diligence and beneficial ownership rule is a component of Treasury's broader strategy and corresponds with the Administration's and Congress' ongoing work to require the collection of beneficial ownership information at the time that legal entities are formed in the United States. However, requiring both the federal government and financial institutions to collect the same information on the same entities is ineffective, duplicative, unnecessary, and costly. It is important to ensure that any additional requirements maintain a balanced approach that promotes the purposes of BSA with the limited and already strained resources of community banks. This rule does not achieve that balance.

Furthermore, information regarding beneficial owners could be more easily shared between law enforcement and government agencies than between banks and law enforcement. While privacy laws do not permit banks to share personal information with a government agency absent a subpoena or similar directive, inter-agency sharing of personal information is permissible if certain amendments are in place.

Additionally, obtaining beneficial ownership on all legal entity customers, and verifying their identity on certain business accounts, is an onerous task and is difficult to implement. While the ownership interest and management responsibility of a business may be straightforward in certain cases and specified in a legal organizational document in other cases, certain legal structures make determining ownership equity extremely difficult, at best.

Each community bank must have a written customer identification program ("CIP") that enables it to form a reasonable belief that it knows the true identity of each customer. Existing CIP and Enhanced Due Diligence ("EDD") practices apply to natural-person customers as well as legal entity customers. However, incorporating beneficial owners into existing CIP practices and risk assessments creates an implicit requirement for bank employees to understand various legal structures and ownership interests in order to assess risk.

As such, a bank's front-line staff is required to conduct several additional intermediate steps during the account-opening process to ensure they have a reasonable belief they know the true identity of each beneficial owner. This adds significantly more time to each business account opened.

Additionally, the rule requires banks to confirm the beneficial ownership information each time a customer opens an additional account. This is duplicative and extremely burdensome because the bank has already undergone the onerous task of confirming the beneficial ownership information in the first place, and it is on file. To do so each time a new account is opened adds no benefit whatsoever to law enforcement.

Although banks may generally rely on the representations of the customer when answering the financial institution's questions about the natural persons behind the legal entity, bank employees still require some advanced business acumen in order to understand and determine to whom the definition applies.

This rule also requires banks to obtain and verify beneficial ownership information on financial product renewals, such as certificate of deposits and loans, for products established before May 11, 2018. In order to comply with this unreasonable requirement, banks need to stop automatic renewals long enough to obtain a customer's beneficial owner certification (and continue following up with customers who do not respond in a timely manner) because most banks do not require customer interaction for automatic renewals. Not only is this requirement a useless exercise, but there is no reason to believe that a roll over product, loan or certificate of deposit renewal, or automatic renewal is evidence of change in beneficial ownership. These products are scheduled for the customer's convenience and are triggered by maturity or due dates and not changes in ownership. Furthermore, these products are low-risk for financial crimes.

## Enhanced communication among industry, law enforcement and the federal government

Communication and cooperation are critical to an effective working partnership among the government, law enforcement, and financial institutions. Community banks seek more current information from the federal government to better understand what specific methods of terrorist financing and money laundering they are trying to prevent so banks can more readily identify and report truly suspicious transactions.

## Ensuring a balanced approach to combating financial crimes

Assisting law enforcement in its fight against financial crimes is important to community banks. Currently, however, banks are effectively deputized to identify, investigate, report, and police potential financial crimes. While banks are eager to cooperate with law enforcement, they should not act as police. More balance is needed between the responsibilities of the public versus private sectors to detect and prevent financial crime.

For community banks, BSA compliance represents a significant expense in terms of both direct and indirect costs. BSA compliance, whatever the benefit to society at large, is a governmental, law enforcement function. As such, the costs should be borne by the government. ICBA supports the creation of a tax credit to offset the cost of BSA compliance.

Additionally, community banks spend significant resources—in terms of both direct and indirect costs—complying with the BSA and anti-money-laundering laws and regulations. However, the cumulative impact of these regulations places a burden on community banks that is often disproportionate to the benefits of the additional regulatory requirements. As the government continues to combat money laundering and terrorist financing, it is important to focus on quality over quantity for all BSA reporting.

# ABOUT

## ICBA

Independent Community Bankers of America® (ICBA), the nation's voice for nearly 5,700 community banks of all sizes and charter types, is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services.

### CONTINUE THE CONVERSATION

**Lilly Thomas**
Senior Vice President, Senior Regulatory Counsel
Independent Community Bankers of America
Lilly.Thomas@icba.org
www.icba.org/advocacy

**Rhonda Thomas-Whitley**
Independent Community Bankers of America
Assistant Vice President and Regulatory Counsel
Rhonda.Thomas-whitley@icba.org
www.icba.org/advocacy

### PRESS INQUIRIES

**Nicole Swann**
Vice President, Communications
Independent Community Bankers of America
Nicole.Swann@icba.org
202-821-4458

**LETTER SUBMITTED BY THE NATIONAL ASSOCIATION OF MANUFACTURERS**


**Chris Netram**

*Vice President,*
*Tax and Domestic Economic Policy*

June 20, 2019

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, DC 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the National Association of Manufacturers, I thank you for holding today's hearing on *Outside Perspectives on the Collection of Beneficial Ownership Information*.

The NAM is the largest industrial trade association in the United States, representing 14,000 manufacturers small and large in every industrial sector and in all 50 states. Over 90 percent of the NAM's members are small businesses, making them the very companies that could be impacted by a requirement to disclose beneficial ownership information to the Treasury Department's Financial Crimes Enforcement Network (FinCEN).

Manufacturers understand and support the goal of ensuring that law enforcement has the information it needs to combat terrorist financing, money laundering, human trafficking, and other criminal activity. However, we urge the Committee to remain mindful of the fact that the overwhelming majority of American small businesses are law-abiding and, thus, to take steps to avoid overburdening manufacturers or criminalizing paperwork mistakes made in a good faith effort to comply with the law. Moreover, we respectfully request that legislation in this area include robust privacy protections for the investors and managers that are providing the capital necessary to finance economic expansion, R&D, and job creation right here in the United States.

As the Committee considers legislative approaches to require the disclosure of beneficial ownership information to FinCEN, including the recently unveiled discussion draft of the Improving Laundering Laws and Increasing Comprehensive Information Tracking of Criminal Activity in Shell Holdings (ILLICIT CASH) Act, the NAM respectfully urges you to focus on the impact that beneficial ownership disclosures will have on small manufacturers by adhering to the following guiding principles.

**1.) Clarity**

Given the broad applicability of and the civil and criminal liability associated with the proposed disclosure regime, it is vital that its definitions and requirements be exceptionally clear and easily

understandable. A lack of clarity in the law's requirements would significantly increase the burden on small manufacturers and lead to confusion and potential legal liability.

Most critically, specificity is needed within the definition of "beneficial owner." Tests that require small business owners to determine whether an individual has "substantial" control, ownership, and/or economic benefits make it difficult for small manufacturers to identify the information they are required to disclose, as do unclear definitions around those terms. Providing specificity within the definition and limiting the universe of individuals whose information would have to be disclosed because of their control, ownership, and/or economic benefits would provide vital clarity as to what information is required to be reported. A comparable approach has been adopted by FinCEN in a similar context – the Customer Due Diligence (CDD) rule calls for the disclosure of any individual that meets a specific 25 percent ownership threshold, as well as a single individual "with significant responsibility to control, manage, or direct" a business.

**2.) Ease of Compliance**

A commonsense, straightforward compliance regime would ensure that small businesses are not forced to divert capital and hire external experts meet the disclosure requirements. An annual reporting obligation – rather than a requirement to update a beneficial owner's address or passport number each time it changes – would be a strong first step in ensuring easy compliance for law-abiding small businesses. Certainty around periodic reporting, combined with the straightforward disclosure requirements discussed above, would significantly ease the compliance burden on small manufacturers.

**3.) Appropriate Scope**

Members of Congress on both sides of the aisle have been clear that the goal of the drive toward beneficial ownership disclosures is to provide information to FinCEN about the types of corporations and LLCs that are often used for illicit purposes. Accordingly, maintaining a strong exemption for *bona fide* domestic operating companies would help appropriately limit the number of manufacturers swept into the reporting regime.

We urge the Committee to consider other methods to appropriately limit the scope of the regime. For example, requiring subsidiaries of businesses exempt from the disclosure regime to report their beneficial ownership information would be unnecessarily burdensome, as their ownership structure is already clear to FinCEN – so we support a support an effective exemption for these small businesses.

Similarly, requiring a business to "look through" and disclose the beneficial owners of its beneficial owners (and so on) would present a substantial compliance burden for smaller companies and dramatically increase the costs of the disclosure regime. Moreover, requiring federal contractors to submit beneficial ownership information to agencies other than FinCEN would needlessly broaden the scope of the bill, given that FinCEN already has their information to utilize for law enforcement purposes.

**4.) Limited Criminal and Civil Liability**

The vast majority of companies required to comply with the proposed disclosure regime will be legitimate, law-abiding small businesses. As such, overly strict standards that result in fines and enforcement action against a broad range of small businesses that make filing mistakes would unnecessarily waste FinCEN's time, stretch thin critical resources that should be targeted toward detecting illicit activity, and present a significant barrier to business formation in the United States.

The Committee should make clear that mere negligence or *de minimis* noncompliance should not be penalized. Small manufacturers should be encouraged to focus on what they do best – creating jobs and investing in America. They should not face prison time for paperwork errors. Furthermore, we urge Congress to ensure that the *mens rea* standard only penalizes the willful submission of information that an individual knows to be false at the time that they submit the information to FinCEN.

**5.) Strong Privacy Protections**

In complying with the new beneficial ownership disclosure regime, small businesses will be disclosing information to FinCEN that is otherwise not available to the public. Such information will often be sensitive; for the individual beneficial owners, it will include their home address and other personally identifiable information. Protecting this information and preventing its misuse are critical, and we urge the Committee to provide strong standards governing access to and use of the beneficial ownership database. In particular, the Committee should provide clear boundaries around FinCEN's use of the information, set clear rules governing how FinCEN can share data with other agencies, and institute strong penalties for the misuse or unauthorized disclosure of beneficial ownership data.

* * * *

As the Committee crafts its approach to beneficial ownership disclosures, manufacturers urge you to keep in mind the needs of our thriving free enterprise system. An overly broad regime would unduly burden, and potentially criminalize, thousands of small manufacturers across the country. The NAM appreciates the opportunity to comment and looks forward to working with you on this legislation.

On behalf of the more than 12.8 million men and women who make things in America, thank you for your continued attention to these important issues.

Sincerely,

Chris Netram
Vice President, Tax & Domestic Economic Policy

## NATIONAL SECURITY LETTER SUBMITTED BY CHAIRMAN CRAPO

The Honorable Mike Crapo
Chairman
Senate Committee on Banking, Housing, and Urban Affairs
239 Dirksen Senate Building
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Senate Committee on Banking, Housing, and Urban Affairs
503 Hart Senate Office Building
Washington, DC 20510

Wednesday, June 19, 2019

Chairman Crapo and Ranking Member Brown,

We write as former military officers, administration officials, law enforcement agents, and foreign policy experts to affirm our conviction that illicit finance poses a serious threat to U.S. national security. As you work to safeguard the U.S. financial system from abuse, we urge you to act against crime and corruption facilitated by anonymous ownership of U.S. shell companies.

The ability to control U.S. companies without disclosing beneficial ownership information has made them attractive vehicles for money laundering. Rogue regimes, terrorist groups, transnational criminal organizations, arms dealers, kleptocrats, drug cartels, and human traffickers have all used U.S.-registered shell companies to obscure their identities and facilitate illicit activities. Meanwhile, U.S. intelligence and law enforcement agencies often find it difficult to investigate these illicit financial networks without access to information about the beneficial ownership of corporate entities involved.

Adversarial authoritarian regimes have become adept at exploiting financial secrecy to spread malign economic influence globally and undermine American leadership. As General David Petraeus and Senator Sheldon Whitehouse noted recently, "the fight against corruption is more than a legal and moral issue; it has become a strategic one — and a battleground in a great power competition." It is alarming, therefore, that a World Bank study found that U.S. shell companies were used in more grand corruption cases than those of any other country.

The global spread of crime and corruption, often facilitated by anonymous shell companies, has undermined democratization and economic development in many countries, with adverse implications for U.S. and global security. Societies impoverished by kleptocratic rulers breed resentment and instability, providing fertile recruiting ground for terrorist groups — many of whom use anonymous shell companies in their own illicit funding networks. Corporate anonymity can also pose a direct threat to U.S. military operations and troop safety, for example when the Department of Defense spent $3.3 million on a U.S.-Afghan contractor secretly owned by local powerbrokers who also purchased weapons for the Taliban.

Anonymous shell companies are routinely used to circumvent U.S. sanctions relating to Iran, North Korea, Russia, Venezuela, and elsewhere. Indeed, Iranian entities relied on U.S. shell companies to maintain ownership of a skyscraper on New York's Fifth Avenue, which they leased out to Americans for two decades before being detected.

Despite these and numerous other alarming examples, research from the University of Texas and Brigham Young University shows that the U.S. remains one of the easiest places in the world to set up an anonymous shell company. A recent report by Global Financial Integrity demonstrates that, in all 50 U.S. states, more information is currently required to obtain a library card than to register a company.

As the global economy becomes more interconnected and technologically advanced, America's adversaries will turn to innovative methods of laundering the proceeds of crime and spreading malign economic influence. We must ensure that U.S. intelligence and law enforcement agencies possess the resources they need to hunt bad actors through an increasingly complex global financial system, including corporate beneficial ownership information.

By ending anonymous ownership of companies and encouraging other countries to do the same, the United States could turn a vulnerability into an advantage, disrupting illicit financial networks and pushing back against adversaries who seek to undermine the rule of law globally. Many of our democratic allies, including the European Union, have recognized this and mandated the collection of corporate beneficial ownership information to strengthen their own anti-money laundering systems.

We thank you and your Congressional colleagues for your continued leadership and urge you to adopt legislation that would require the collection of information about the beneficial ownership of U.S. companies.

Sincerely,

**Please note that this letter is signed in an individual capacity. Any institutional affiliations are listed for reference only.**

JOHN AGOGLIA, Col. (Ret.), USA
Former Director of the Counterinsurgency Training Center in Afghanistan

NATALIA ARNO
President, Free Russia Foundation

DAVID L. ASHER, PhD
Former Coordinator, North Korea Working Group, Office of the Secretary of State, U.S. Department of State
Former Senior Advisor for East Asian and Pacific Affairs, Office of the Secretary of State, U.S. Department of State
Senior Fellow, Foundation for Defense of Democracies

ANDERS ÅSLUND, PhD
Resident Senior Fellow, Eurasia Center, Atlantic Council

THOMAS P. BALTAZAR, Col. (Ret.), USA
Former Director, Office of Military Affairs, U.S. Agency for International Development

DONNA BARBISCH, Major General (Ret.), USA

ANDREA BARTOLI
Dean of the School of Diplomacy and International Relations, Seton Hall University

RICK BARTON, Amb. (ret.)
Former Assistant Secretary of State, U.S. Department of State
Former Deputy High Commissioner for Refugees, United Nations
Author of *Peace Works* and Lecturer at Princeton University

WILLIAM E. BERRY, JR., Col. (Ret.), USAF

ROB BERSCHINSKI
Former Deputy Assistant Secretary of State for Democracy, Human Rights and Labor, U.S. Department of State
Former Director for Security and Human Rights, National Security Council, The White House

ALINA BLOOM
Former Special Agent, Federal Bureau of Investigation, U.S. Department of Justice

MICHAEL BOSSHART
Former Foreign Service Officer, U.S. Department of State

REBECCA BROCATO
Former Special Assistant to the President, The White House
Former Senior Advisor for Legislative Affairs, U.S. Department of State
Director of Strategy and Government Affairs, National Security Action

BRAD BROOKS-RUBIN
Former Special Advisor for Conflict Diamonds, U.S. Department of State
Managing Director, The Sentry/Enough Project

JOHN J. BYRNE, CAMS, Esq.
Former Executive Vice President, Association of Certified Anti-Money Laundering Specialists
Adjunct Professor, Schar School of Policy and Government, George Mason University

CHARLES T. CALL, PhD
Former Senior Adviser to the Assistant Secretary for Conflict and Stabilization Operations, U.S. Department of State
Associate Professor, American University

GREG E. CALLES
Former Supervisory Senior Resident Agent, Federal Bureau of Investigation

MICHAEL CARPENTER, PhD
Former Deputy Assistant Secretary of Defense for Russia, Ukraine, and Eurasia, U.S. Department of Defense
Senior Director, Biden Center for Diplomacy and Global Engagement, University of Pennsylvania

JOHN A. CASSARA
Former Special Agent, U.S. Department of the Treasury

SARAH CHAYES
Former Special Assistant to the Chairman of the Joint Chiefs of Staff, U.S. Department of Defense
Author, Thieves of State: Why Corruption Threatens Global Security

BETH COLE
Former Director, Office of Civil-Military Cooperation, U.S. Agency for International Development

CHRISTOPHER CORPORA, PhD
Former U.S. National Security Officer
Professor of Practice, Mercyhurst University

THOMAS CREAL, CPA
Former UN Panel Expert for Sanctions
Former Lead Expert for Task Force 2010 in Afghanistan

ARTHUR E. DEWEY
Former Assistant Secretary of State for Population, Refugees, and Migration, U.S. Department of State

LARRY DIAMOND, PhD
Senior Fellow, Freeman Spogli Institute for International Studies, Stanford University
Senior Fellow, Hoover Institution

MICHAEL DZIEDZIC, PhD, Col. (Ret.), USAF
Adjunct Professor, George Mason University

CAMILLE EISS
Former Senior Advisor for Anti-Corruption to the Assistant Secretary for Democracy, Rights and Labor, U.S. Department of State
Chief of Policy and Global Partnerships, Organized Crime and Corruption Reporting Project (OCCRP)

ISRAEL D. ESCABI
Former Unit Chief, Federal Bureau of Investigation

KAREN J. FINKENBINDER, PhD
Rule of Law, Justice & Reconciliation Advisor, Peacekeeping & Stability Operations Institute, U.S. Army War College

JAMIE FLY
Former Counselor for Foreign and National Security Affairs to Senator Marco Rubio
Former Executive Director, Foreign Policy Initiative
Former Director for Counterproliferation Strategy, National Security Council, The White House
Former Assistant for Transnational Threats Policy, Office of the Secretary of Defense, U.S. Department of Defense
Senior Fellow and Director, Future of Geopolitics Program; Director, Asia Program, German Marshall Fund of the United States

JACK H. GAINES
Former Joint Strategic Advisor, U.S. Department of Defense
Chairman, Chronemics

MARY BETH GOODMAN
Former Special Assistant to the President for National Security Affairs and Senior Director for Development, Democracy and Humanitarian Affairs, National Security Council, The White House
Former Director for International Economic Affairs, National Security Council, The White House

KAREN A. GREENAWAY, Esq.
Former Special Agent, Federal Bureau of Investigation, U.S. Department of Justice

MORTON H. HALPERIN
Former Director of Policy Planning, U.S. Department of State

LEONARD R. HAWLEY
Former Deputy Assistant Secretary of State for International Organization Affairs, U.S. Department of State
Former Director for Multilateral Affairs, National Security Council, The White House
Former Policy Team Staff, National 9/11 Commission

CHRISTOPHER HOH
Former Deputy Chief of Mission at the American Embassy in Vienna and Sarajevo
Former Director for South Central European Affairs, U.S. Department of State
Former Director for Response Strategy and Resource Management, Office for Reconstruction and Stabilization, U.S. Department of State

CARYN HOLLIS
Former acting Assistant Secretary of Defense for Special Operations/Low-intensity Conflict, U.S. Department of Defense
Former Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, U.S. Department of Defense

CHRISTOPHER J. HOLSHEK, Col. (Ret.), USA
Senior Fellow, Alliance for Peacebuilding
Senior Civil-Military Advisor, Narrative Strategies

BENJAMIN JUDAH
Research Fellow, Kleptocracy Initiative, Hudson Institute

EDWARD P. JOSEPH
Adjunct Professor & Senior Fellow, Johns Hopkins School of Advanced International Studies

JOSHUA KIRSCHENBAUM
Former Acting Director, Office of Special Measures, Financial Crimes Enforcement Network, U.S. Department of the Treasury
Senior Fellow, Alliance for Securing Democracy, German Marshall Fund

JACQUES PAUL KLEIN, Major General (Ret.), USAF
Former Under-Secretary-General of the United Nations

DAVID J. KRAMER
Former Assistant Secretary of State for Democracy, Human Rights and Labor, U.S. Department of State
Former Deputy Assistant Secretary of State for Europe and Eurasia, U.S. Department of State

MARK A KROEKER
Former Assistant Secretary General *ad interim*, United Nations
Former United Nations Police Commissioner
Former Portland Oregon Police Chief
Former Los Angeles Police Deputy Chief

DEBRA LAPREVOTTE
Former Supervisory Special Agent, International Corruption Unit, Federal Bureau of Investigation, U.S. Department of Justice
Senior Investigator, The Sentry

EDWARD LEMON, PhD
DMGS-Kennan Institute Fellow, Daniel Morgan Graduate School, Wilson Center

ALFONSO E. LENHARDT, Amb. (Ret.), Major General (Ret.), USA
Former Deputy Administrator, U.S. Agency for International Development
Former U.S. Ambassador to Tanzania
Former Sergeant at Arms, U.S. Senate
Former Commanding General, U.S. Army Recruiting Command

DENNIS LORMEL
Former Chief, Terrorist Financing Operations Section, Counterterrorism Division, Federal Bureau of Investigation, U.S. Department of Justice

DAVID M. LUNA
Former Senior Director for National Security & Diplomacy, U.S. Department of State
Former Director for Transnational Threats and Illicit Networks (Anti-Crime Programs), U.S. Department of State
Former Director for Anti-Corruption and Governance Initiatives, Bureau of International Narcotics and Law Enforcement Affairs, U.S. Department of State

JEFFREY W. MADISON
Former Agent, Federal Bureau of Investigation

MAX G. MANWARING, Col. (Ret.), USA
Professor of Military Strategy, Strategic Studies Institute, U.S. Army War College

MICHAEL MCFAUL, Amb. (Ret.), PhD
Former U.S. Ambassador to the Russian Federation
Former Special Assistant to the President and Senior Director of Russian and Eurasian Affairs, National Security Council, The White House
Professor of Political Science, Director and Senior Fellow, Freeman Spogli Institute for International Studies, Stanford University
Senior Fellow, Hoover Institution

THOMAS O. MELIA
Former Assistant Administrator for Europe & Eurasia, U.S. Agency for International Development
Former Deputy Assistant Secretary of State for Democracy, Human Rights, and Labor, U.S. Department of State
Washington Director, PEN America

CHRISTOPHER MOELLER
Former Investigator, Asset Forfeiture and Money Laundering Section, Criminal Division , U.S. Department of Justice

DAVID MURRAY
Former Director, Office of Illicit Finance, U.S. Department of the Treasury
Former Senior Advisor to the Under Secretary, U.S. Department of the Treasury

MATTHEW H. MURRAY
Former Deputy Assistant Secretary of Commerce for Europe, the Middle East and Africa, U.S. Department of Commerce
Former Deputy Assistant Secretary of Commerce for Europe and Eurasia, U.S. Department of Commerce

ANDREW NATSIOS
Former Administrator, U.S. Agency for International Development
Executive Professor at the Bush School, Texas A&M University
Director of the Scowcroft Institute of International Affairs

BRIAN O'TOOLE
Former Senior Adviser to the Director, Office of Foreign Assets Control, U.S. Department of the Treasury
Nonresident Senior Fellow, Global Business and Economics Program, Atlantic Council

JAMES W. PARDEW Amb. (Ret.)
Former Deputy Assistant Secretary General of NATO for Operation and Crisis Management
Former U.S. Ambassador to Bulgaria
Former Deputy Special Adviser to the President and Secretary of State for Democracy in the Balkans

STEWART PATRICK
Senior Fellow, Council on Foreign Relations

CHIP PONCY
Former Director, Office of Strategic Policy for Terrorist Financing and Financial Crimes, U.S. Department of the Treasury
Senior Advisor, Center on Sanctions and Illicit Finance, Foundation for Defense of Democracies

ERIC G. POSTEL
Former Associate Administrator, U.S. Agency for International Development
Former Assistant to the Administrator for Africa, U.S. Agency for International Development
Former Assistant Administrator, E3 Bureau, U.S. Agency for International Development

JOHN PRENDERGAST
Former Director for African Affairs, National Security Council, The White House
Co-founder, The Sentry

NED PRICE
Former Special Assistant to the President, The White House
Former Spokesperson, National Security Council, The White House
Former Senior Analyst, Central Intelligence Agency
Director of Policy and Communications, National Security Action

ELIZABETH ROSENBERG
Former Senior Advisor to the Assistant Secretary for Terrorist Financing and Financial Crimes, and then to the Under Secretary for Terrorism and Financial Intelligence, U.S. Department of the Treasury
Senior Fellow and Director of the Energy, Economics, and Security Program, Center for a New American Security

LAURA ROSENBERGER
Former Chief of Staff to Deputy Secretary of State, U.S. Department of State
Former Senior Advisor to Deputy National Security Advisor, National Security Council, The White House
Former Director for China and Korea, National Security Council, The White House
Director of the Alliance for Securing Democracy and Senior Fellow at the German Marshall Fund of the United States

TOMMY ROSS
Former Deputy Assistant Secretary of Defense for Security Cooperation, U.S. Department of Defense
Senior Associate, Center for Strategic and International Studies

JOSH RUDOLPH
Former Director for International Economics, National Security Council, The White House
Former Deputy Director, Markets Room, U.S. Department of the Treasury
Former Advisor to the U.S. Executive Director, International Monetary Fund
Senior Fellow, Alliance for Securing Democracy, German Marshall Fund

ROBERT SAALE
Former Director, Hostage Recovery Fusion Cell, Federal Bureau of Investigation, U.S. Department of Justice

DONALD L. "LARRY" SAMPLER, JR.
Former Assistant Administrator, U.S. Agency for International Development
Vice President for Administration & Finance/COO, Metropolitan State University, Denver

MARC SCHNEIDER
Former Assistant Administrator for Latin America, U.S. Agency for International Development
Former Principal Deputy Assistant Secretary of State for Human Rights, U.S. Department of State
Former Senior Vice-president, International Crisis Group

DONALD SEMESKY
Former Chief of Financial Operations, Drug Enforcement Administration, U.S. Department of Justice
Former Anti-Money-Laundering Policy Adviser and IRS-Criminal Investigation (IRS-CI) Liaison Officer, Office of National Drug Control Policy, The White House

DANIEL SERWER
Professor, Johns Hopkins School of Advanced International Studies

LOUISE SHELLEY, PhD
Omer L. and Nancy Hirst Endowed Chair, George Mason University
Director, Terrorism, Transnational Crime and Corruption Center, George Mason University
University Professor, Schar School of Policy and Government, George Mason University

NATE SIBLEY
Research Fellow, Kleptocracy Initiative, Hudson Institute

BARBARA SMITH
Former Deputy Assistant Administrator for Policy, Planning and Learning, U.S. Agency for International Development
Former Director for Afghanistan and Pakistan, National Security Council, The White House
Senior Associate (Non-resident), Center for Strategic and International Studies
Adjunct Professor, Korbel School of International Studies

GAYLE E. SMITH
Former Administrator, U.S. Agency for International Development
Former Senior Director for Development and Democracy, National Security Council, The White House
President and CEO, The ONE Campaign

TYLER STAPLETON
Former Senior Legislative Assistant for National Security, U.S. House of Representatives
Deputy Director of Congressional Relations, Foundation for Defense of Democracies

STEPHEN JOHN STEDMAN
Senior Fellow, Freeman Spogli Institute for International Studies, Stanford University

THOMAS STRENTZ, PhD
Former Supervisory Special Agent, Federal Bureau of Investigation, U.S. Department of Justice

ADAM SZUBIN
Former Acting Secretary of the Treasury, U.S. Department of the Treasury
Former acting Under Secretary, Office of Terrorism and Financial Intelligence, Department of the Treasury

CHARLES E. TUCKER, Major General (Ret.), USAF
Former Director of Doctrine, Training, and Force Development (J-7) for the U.S. National Guard, Washington D.C.
Executive Director of the World Engagement Institute, Chicago, IL

ROBERT ULMER
Former Special Agent, Federal Bureau of Investigation, U.S. Department of Justice

ROBERT W. VERICKER
Former Agent, Federal Bureau of Investigation
Associate Professor, Administration of Justice Department, University of Hawaii
JODI VITTORI, Lt Col. (Ret.), USAF
Former ISAF Task Force Shafafiyat Contracting, Economic Development, and Rule of Law Team Chief

WILLIAM F. WECHSLER
Former Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism, U.S. Department of Defense
Former Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, U.S. Department of Defense

LAURA WILLIAMS
Former Supervisory Special Agent, Financial Crimes Section, Federal Bureau of Investigation

CLINT WILLIAMSON
Former Ambassador-at-Large for War Crimes Issues, Department of State
Former Special Assistant to the President, The White House
Former Senior Director for Relief, Stabilization and Development, National Security Council, The White House
Senior Director for Rule of Law, Governance and Security, McCain Institute

JONATHAN WINER
Former Deputy Assistant Secretary of State for International Law Enforcement, U.S. Department of State

BEVERLY S. WRIGHT
Former Supervisory Special Agent, Federal Bureau of Investigation, U.S. Department of Justice

JAMES M. WRIGHT
Former Senior Advisor, Office of Technical Assistance, U.S. Department of the Treasury
Board Member, U.S. Capital Chapter, Association of Certified Anti-money Laundering Specialists

CC:

The Honorable Mike Pompeo, Secretary of State

The Honorable Steve Mnuchin, Secretary of the Treasury

The Honorable Patrick Shanahan, Acting Secretary of Defense

The Honorable William Barr, Attorney General

The Honorable Wilbur Ross, Secretary of Commerce

The Honorable Kevin McAleenan, Acting Secretary of Homeland Security

The Honorable John Bolton, Assistant to the President for National Security Affairs

The Honorable Mark Green, Administrator, U.S. Agency for International Development

**LETTER SUBMITTED BY THE NATIONAL DISTRICT ATTORNEYS ASSOCIATION**

**National District Attorneys Association**
Staff Contact: Frank Russo
703-519-1655 or frusso@ndaajustice.org
www.ndaa.org

June 19th, 2019

The Honorable Michael D. Crapo
Chairman, Committee on Banking
United States Senate
Washington, D.C. 20510

The Honorable Sherrod C. Brown
Ranking Member, Committee on Banking
United States Senate
Washington, D.C. 20510

Dear Chairman Crapo & Ranking Member Brown,

On behalf of the National District Attorneys Association (NDAA), the largest prosecutor organization representing 2,500 elected and appointed District Attorneys across the United States as well as 40,000 Assistant District Attorneys, I write regarding beneficial ownership legislation.

NDAA continues to support legislative efforts that provide beneficial ownership information to state and local law enforcement agencies. The need for the collection of this ownership information is critical to law enforcement investigations into organized transnational criminal operations, terrorism financing and other unlawful activity. On July 12, 2018, the U.S. Secretary of the Treasury, Steven T. Mnuchin, called on Congress to find a way to facilitate the collection of this information "in the next six months," and stated further, "I don't want to be coming back here next year and [not] have this solved."

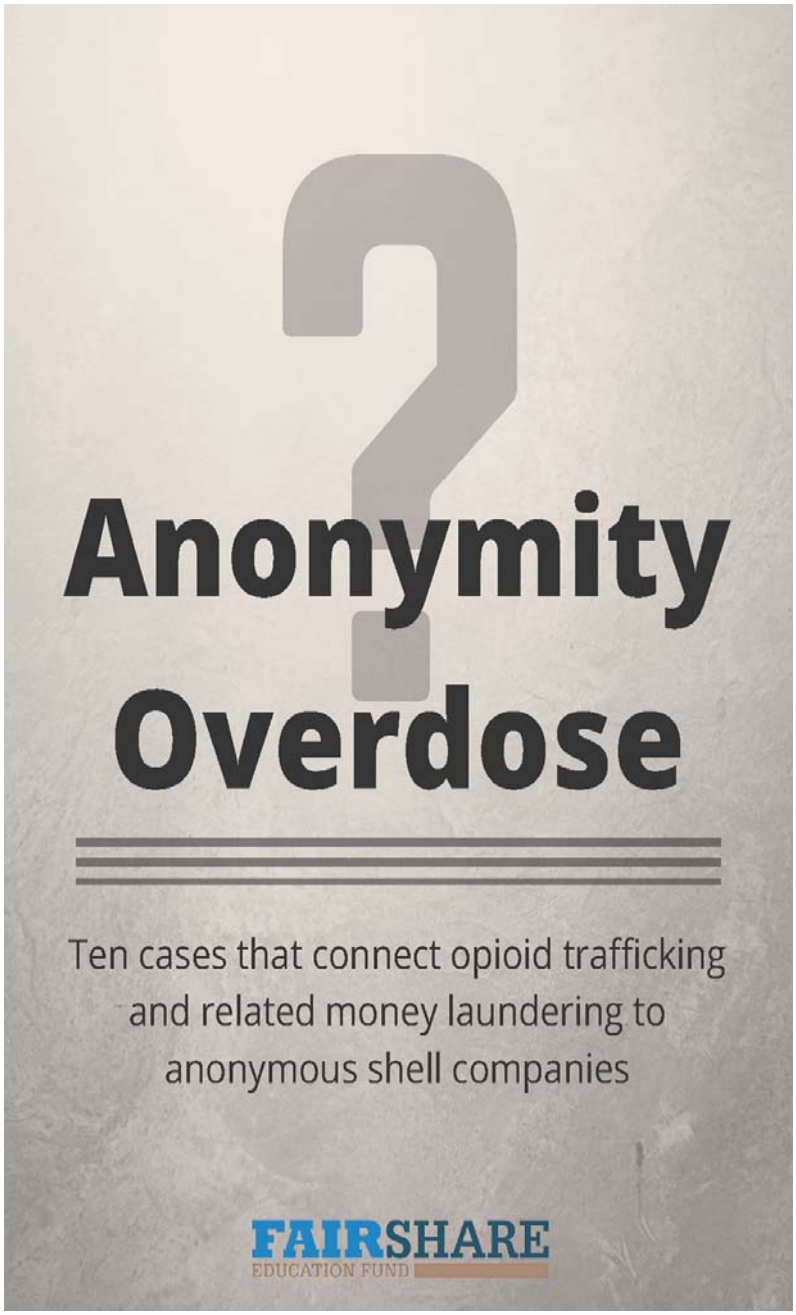
As end users of evidence collected throughout the investigative process, it is imperative that prosecutors have as much information as possible in order to determine the best course of action for prosecuting an individual or entity that has committed a crime. Beneficial ownership data collection is vital to this effort, and law enforcement and prosecutors must have lawful access to that information. Any approach to beneficial ownership that limits law enforcement's access to this data is inadequate to address the threats caused by criminal organizations operating in the United States through shell corporations.

We appreciate your willingness to hold a hearing on this landmark issue and look forward to working with your staff to move beneficial ownership legislation forward.

Sincerely,

Jonathan Blodgett
President

**"ANONYMITY OVERDOSE", BY NATHAN PROCTOR AND JULIA LADICS, FAIR SHARE EDUCATION FUND**



# Anonymity Overdose;

Ten cases that connect opioid trafficking and related money laundering to anonymous shell companies

FAIRSHARE
EDUCATION FUND

Written by:
Nathan Proctor and Julia Ladics
Fair Share Education Fund

Special thanks to Mark Hays, Gideon Weissman, John Cassara and the FACT Coalition

**August 2016**

## Executive Summary

*"[W]e have become convinced that we cannot stop the drug trade without first cutting off the money that flows to drug trafficking organizations."* – The Bipartisan United States Senate Caucus on International Narcotics Control.[1]

Over the last 15 years, opioid overdose deaths have quadrupled, and opioid abuse has become a full-blown crisis.[2] As lawmakers, law enforcement and other public officials struggle to address this problem, we can make it easier to go after the money used in drug trafficking by ending the gaps in our laws that allow companies to be incorporated anonymously.

***Drug money is laundered with astonishing effectiveness.*** The Office of National Drug Control Policy estimates that $65 billion is spent by Americans every year on illegal drugs, but only $1 billion, or roughly 1.5%, of that money is seized per year domestically by all federal agencies combined.[3] In other words, it is likely that 98.5% of the proceeds derived from drug trafficking remain in the hands of traffickers.

One of the tools that criminals use to launder their money so successfully are shell companies, especially anonymous shell companies. These companies only exist on paper and, in most cases, law enforcement does not have access to information about who owns and controls them. Indeed, in most cases such information isn't even collected when companies are formed. As such, many promising investigations are abandoned when law enforcement runs into an anonymous shell company. Authorities may have good reason to suspect someone of being involved in criminal activity. However, without the basic information necessary to show that a suspect is directly linked to a shell company used to facilitate illegal activity, they are unable to make their case, or run out of the time and resources needed to do so.

In this report we found ten case studies that connect opioid trafficking and shell companies, where law enforcement did succeed in untangling the web of secrecy and anonymity. However, these cases represent a minority.

In some of the cases that we've found, profits made by the perpetrators were spent fairly brazenly on items such as luxury real estate, diamond encrusted watches or race horses. Often little of that was recovered by investigators. For example, the biggest of Mexico's drug gangs, the Los Zetas cartel, used anonymous shell companies to launder millions, in part by purchasing race horses with drug proceeds – they even named one horse "Number One Cartel." In one of the largest oxycodone busts in Oregon history, Kingsley Iyare Osemwengie and his associates were found to use call girls and couriers to transport oxycodone, and then move profits through an anonymous shell company aptly named High Profit Investments LLC. Similarly, even after he was officially designated under the Foreign Narcotics Kingpin Designation Act as a drug lord, Fernando Melciades Zevallos Gonzalez was able to sell his Miami properties and escape with the proceeds through anonymous companies. His empire continues to operate. You can read more about these and other examples on pages 10-15.

***Our recommendation: Require the collection of beneficial ownership information and provide that information to law enforcement.***

We need to equip our law enforcement officers with tools they can use to put an end to drug cartels. Simply requiring that all companies formed in the U.S. disclose their beneficial owners would enable law enforcement to more effectively follow the money trail and make it harder for criminals to hide their money. We should use every tool at our disposal to tackle the opioid crisis, and going after the money is just such a critical tool.

## "One of the Worst Public Health Epidemics" in U.S. History

Opioid addiction is growing across the United States, and is a public health crisis – 78 Americans die every day from an opioid overdose.[4] As of last year, opioid overdoses accounted for more deaths than motor vehicle crashes.[5]

Roughly 75% of opioid users say they started with prescription pain killers.[6] Then, because it is easier to abuse and significantly cheaper, heroin often becomes the next stage in their addiction.[7]

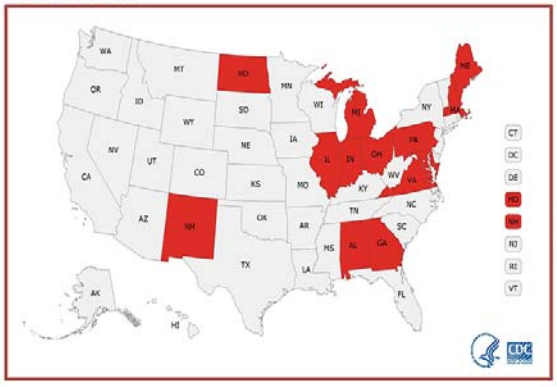
**Common Opioids**

- Oxycodone
- Codeine
- Fentanyl
- Hydrocodone
- Morphine
- Opium
- Heroin

Drug cartels are competing on price with prescription opioids, and they are winning. In most states heroin costs less than a packet of cigarettes[8] which range from $4.38 in Missouri to $10.45 in New York. Meanwhile, OxyContin can sell for over $80 a pill.[9]

Overdose deaths from prescription pain killers and heroin have quadrupled since 1999[10] while the number of heroin users nearly doubled between 2005 and 2012.[11] The White House and others have labeled this as one of the worst public health epidemics in U.S. history.[12]

**Worst Hit States**




Statistically significant drug overdose death rate increase from 2013 to 2014, US states CDC Injury Center, http://www.cdc.gov/drugoverdose/data/statedeaths.html

## A Price Tag North of $193 Billion

The opioid epidemic has had an immeasurable impact on families, congregations, communities, local law enforcement and medical providers. And while the largest costs have been human, there are also significant public financial costs to both local governments and others working on the front lines of the issue.

A 2007 estimate, the most recent one available, put the economic cost of opioid addiction at $193 billion.[13] Given how much the crisis has grown since 2007, the price tag is likely many times this level. The $193 billion estimate includes:

- $120 billion in lost productivity, mainly due to labor participation costs, participation in drug abuse treatment, incarceration and premature death;
- $11 billion in healthcare costs – for drug treatment and drug-related medical consequences; and
- $61 billion in criminal justice costs, primarily due to criminal investigation, prosecution and incarceration, and victim costs.

*"In order to have the biggest impact on its mission as the nation's drug enforcement agency, DEA has identified and targeted those illegal proceeds that flow back to sources of supply as the top priority of its financial enforcement program; since this is the very money that is destined to finance the next cycle of illegal drugs that will be marketed to our consumer markets."*

**- Drug Enforcement Agency**

https://www.dea.gov/ops/money.shtml

## Going After the Money is a Key Strategy

As communities struggle to respond to the growing opioid crisis, we must use all the tools available to help those efforts. As such, we need to consider better tools for law enforcement to go after the proceeds of drug trafficking.

Clearly, one of the largest motivations behind drug trafficking is the huge amount of profit that comes from engaging in such activity.[14] If authorities could seize those profits or make it more difficult for profits to move from the street-level trafficking to the bank accounts of kingpins, they could lower this incentive.

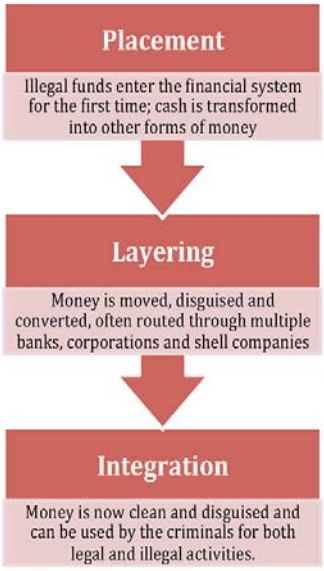
Currently law enforcement says that drug profits are most vulnerable and easiest to tie back to the traffickers when they are in cash form.[15] However, even in its most vulnerable state, law enforcement officials estimate we are seizing less than one percent of illicit outbound cash flows on the southwest border and even less of the money laundered through the international financial system.[16]

John Cassara, a former special agent for the Department of the Treasury agrees that going after the money is key, yet difficult. In an article from 2013 he wrote: "Today's complex financial fraud cases sometimes take years to complete. From a management point of view, it is a tremendous investment. They can't afford to waste scarce resources that lead to investigative dead-ends. What most outsiders do not realize is that a very large percentage of investigations are unsuccessful.

"Although commentators argue the point, the bottom-line metric that quantifies success for law enforcement is the number of investigations that result in successful prosecutions and convictions. Another key metric for certain crimes is criminal assets forfeited...Within law enforcement, there is a subtle and sometimes selective weeding of cases that are chosen to be pursued."[17]

## The Basics of Money Laundering

Money laundering refers to activities that are undertaken specifically to hide the true source of the money. This source is usually a criminal enterprise or activity, and laundering is done to make the income seem legitimate to allow it to be used in the normal economy.[18]




There are three stages to money laundering: placement, layering and integration. Placement is how the illegal money enters the financial system. This usually involves turning cash into something easier to transfer, such as a bank account deposit, a wire transfer, a pre-paid stored value card, travelers check, etc.

The next step, layering, refers to how this money is disguised. Typically, this is done through multiple wire transfers through many banks and shell companies and corporations in order to make the money trail very hard to trace. These are also often done through multiple jurisdictions, for example from the U.S. to the Cayman Islands, to the Bahamas and then back to the U.S. The final stage, integration, is when the money is clean enough (or far enough removed from the criminal activity) to be useable for legal and legitimate transactions.[19]

### Anonymous, LLC: How a company ends up with no owner

In the U.S., companies are formed at the state level. However, in most states, very little information is required from the people forming companies – generally less than it takes to get a library card.[20] Typically, a new company must list a company name, the name of an 'agent' authorized to accept legal service on behalf of the company, and a contact address for that agent. A few states require a bit more information – say, the name of at least one 'manager' of the company being created. But not a single U.S. state requires people forming companies to disclose the real, living person or persons that

own, control and ultimately 'benefit' from the company's existence – the so-called 'beneficial' owners of a company.

### What is a Shell Company?

When you think of a company, you imagine a business with employees, operations, products and sales. But unlike a regular company, a shell company is a hollow structure, set up for the purposes of performing financial manoeuvres. Essentially, it only exists on paper.

One of the key features of companies is that they can set up bank accounts – hence shell companies, especially anonymous ones, are often used simply for monetary and other bank transactions.

http://www.economist.com/blogs/graphicdetail/2016/04/using-and-abusing-offshore-accounts

This state of affairs means that there are many easy ways in which someone who wants to set up a shell company and hide the fact that they own it, can do so. For example, anonymous shell companies often have nominee owners or directors, people who are unrelated to the activities of the company. Their role is to be the public face of the company on paper, while the real owners remain hidden. Sometimes, the nominee owners or directors aren't even people but companies, law firms or other entities. In egregious cases, the nominee owners or directors can sometimes simply be made-up names.

All this allows the true beneficiaries, the people who benefit from the activities of the company, to remain hidden. It is often difficult and sometimes impossible to link the nominee owners or directors back to the real beneficiary.

### Financial Getaway Cars

While a shell company might sometimes serve a purpose in law-abiding business operations, keeping information about the real owner of a business from law enforcement is harder to defend. Saying "I can't think of a reason not to do that," Patrick Fallon, Jr., head of the FBI's financial crimes section, said he believes all shell companies should be required to disclose their true owners.[21]

According to a 2012 academic study, out of 60 countries examined, the United States was found to be the easiest place in the world for criminals to incorporate an anonymous shell company for illegal activities.[22] And since there is no process in place to keep track of the beneficial owners of companies formed in the U.S.,[23] there is no way to trace criminals' identities let alone hold them responsible for their actions.

That makes anonymous shell companies formed in the U.S. a favorite tool for moving illicit money. As Story County Iowa Sherriff Paul Fitzgerald wrote, "Think of them as financial getaway cars — companies set up to move ill-gotten money without leaving anyone to be held accountable." [24]

**Anonymous shell companies are also used in:**

- Terrorist financing
- Human trafficking
- Tax avoidance and evasion
- Fraud (e.g. insurance)
- Ponzi schemes
- Arms dealing

## Law Enforcement Struggles to Go After Drug Money

Most arrests for drug trafficking involve low level distributors[25] whose ranks can easily be replenished.[26] These arrests resemble a large game of whack-a-mole, where distributors substitute one another very quickly. Many law enforcement experts believe that in order to disrupt the drug trade more substantially, we need to arrest the kingpins and cartel bosses.

The DEA and other law enforcement and public policy organizations have determined that the biggest impact they can have on drug trafficking is to intercept their illegal profits and interrupt their monetary flows.[27] This would help dethrone those in the highest seats of authority in drug operations and stop the demand-fueled regeneration of street level operations.

As long as these easy money laundering mechanisms are in place, there will always be people willing to traffic drugs.

We need to fix the system to close the loopholes that allow any criminal with the inclination to traffic drugs to do so.

However this can often be difficult if not impossible. Law enforcement frequently runs up against a brick wall when they encounter an anonymous shell company; many investigations need to be abandoned when they run into one because law enforcement loses the money trail.[28] "On a near-daily basis we encounter a company or network of companies involved in suspicious activity, but we are unable to glean who is actually controlling and benefiting from those entities, and from their illicit activity. In other words, we can't identify the criminal," said Cyrus Vance Jr., District Attorney for New York County, NY.[29] Not only do they have trouble accessing paperwork about the beneficial owners of a company, if they succeed, they often see documentation that lists no owners or other anonymous companies as owners.

*"Our statement of national transparency standards should be something more than: 'U.S. financial transparency: Better than Lichtenstein and trying to catch up to Panama.' Simply put, we lag behind many other countries in the world in this regard, and it makes our statements concerning transparency and tax evasion ring hollow and hypocritical."*

**- Robert M. Morgenthau, District Attorney**
New York County, NY, in testimony before the Committee on Homeland Security and Government Affairs, June 18, 2009.

Because of the challenges of tracing money beyond the placement stage, there is little chance of connecting cash deposited in a bank to the eventual use by those higher up in the drug-trafficking enterprise. Once drug traffickers manage to get beyond the placement stage, and layer their money into the financial system, it is effectively lost to law enforcement.

According to Adam Szubin, the acting under secretary for terrorism and financial intelligence at the U.S. Treasury, "with every threat that we track, be it foreign terrorists, narcotics cartels, sanctioned regimes or cyber hackers, our investigators encounter American shell companies used to hide and move money." [30]

***Ending the use of anonymous shell companies would assist law enforcement in making it more difficult for drug traffickers to hide and launder their money.[31]***

## The Insider Perspective

All too often investigations are stymied when we encounter a company with hidden ownership. These nameless, faceless companies can do business just like any other, but it is difficult, if not impossible, to identify the real people behind them.

"Follow the money" is a standard investigative strategy. Law enforcement agents start at the street level — the drug dealer or low-level lackey — and try to follow the paper trail to the ringleader. When we can identify the owners of anonymous shell companies, we can track down those kingpins and bring them to justice.

An anonymous company in Nevada may be owned by another in Delaware, which is owned by a trust in the Cayman Islands, and so on. Criminals use layers of shell companies to frustrate investigators and protect themselves from prosecution. Sometimes we find alternate routes to bring evidence against the kingpins, but more regularly our investigations are thwarted at the low end of the criminal food chain. We may arrest low-level lackeys, who get easily replaced. So we go after them and fail to prosecute the top-level crooks.

This is a problem wherever anonymous companies can be incorporated. That includes virtually every U.S. state, for very few collect any information about the real owner of a company. For all the grumbling about offshore shell companies, many U.S. states are no better. Secrecy has become a big business in places like Delaware, Nevada and Wyoming, where even the people named on a company's board of directors are often little more than a fiction. For a small fee an incorporation agent can provide your company with a set of "nominees," or random individuals, to stand in as representatives for your board of directors and shareholders. It's a practice perfectly legal in most states. In fact, the only two states that require information identifying corporate owners – a standard practice in most countries – are Maine and Alaska.

Once a company has the legitimacy afforded by incorporation in the United States, opening bank accounts to access the global financial system is easy. You or I have to show proof of identity to put a few hundred dollars into a checking account, but a corporation can instantly move millions of dollars to distant points on the globe without so much as a real person's name — someone who can be held accountable if the corporation violates a law — associated with the transaction.

It is almost a certainty that, at this very moment, a terrorist cell, drug cartel or corrupt government official is using an anonymous U.S. shell corporation to finance illicit activities. We should provide law enforcement with the tools necessary to thwart these activities and set a standard for the rest of the world.

**Cyrus Vance Jr., District Attorney for New York County, State of New York**
Op-Ed published by Reuters
October 2012

"In order to succeed, terrorists, organized crime, drug cartels and major fraudsters must have the ability to raise, move, store and spend money. Anonymous shell companies, that shield beneficial ownership, are one of the primary tools used by bad guys to openly acquire and access nefarious funds."

**Former Chief of the FBI's Terrorist Financing Operations Section**, Dennis M. Lormel, op-ed in the Cleveland Plain Dealer, August 16, 2013.

"Years of research and law enforcement investigations have conclusively demonstrated the link between the abuse of legal entities, on the one hand, and, on the other hand, WMD proliferation, terrorist financing, sanctions evasion, tax evasion, corruption and money laundering for virtually all forms of serious criminal activity. As these reports and investigations indicate, this abuse is particularly prevalent with respect to legal entities created in the United States."

**Assistant Secretary for Terrorist Financing, U.S. Department of the Treasury**, David S. Cohen, Testimony before the Committee on Homeland Security and Government Affairs, June 18, 2009.

"While [some] notorious drug trafficking famil[ies] may be beyond our reach, the proceeds from their decade's long money laundering scheme are not."

**Manhattan U.S. Attorney**, Preet Bharara, DEA Press release, October 10th 2012

"The lack of corporate transparency has allowed criminal entities a gateway into the financial system and further veils their illicit activity. Investigations can be significantly hampered in cases where criminal targets utilize shell corporations."

**Deputy Assistant Director, Office of Investigations, U.S. Immigration and Customs Enforcement**, Janice Ayala, Testimony before the Committee on Homeland Security and Government Affairs, June 18, 2009.

"DEA realizes that there are not enough time or law enforcement resources to adequately address all illegal drug proceeds. Therefore, in order to have the biggest impact on its mission as the nation's drug enforcement agency, DEA has identified and targeted those illegal proceeds that flow back to sources of supply as the top priority of its financial enforcement program."

**Drug Enforcement Administration**, Programs: Money Laundering, https://www.dea.gov/ops/money.shtml

"TCOs [Transnational Criminal Organizations] continue to exploit the banking industry to give illicit drug proceeds the appearance of legitimate profits. Money launderers often open bank accounts with fraudulent names or businesses and structure deposits to avoid reporting requirements."

**2015 National Drug Threat Assessment Summary**, 96-97

## Case Studies

### Drug Traffickers Use Call Girls to Transport Oxycodone All Across the U.S.

**Kingsley Iyare Osemwengie** and his associates used call girls and curriers to transport oxycodone and the money made from selling it across the United States. He disguised his income through an anonymous shell company, aptly named High Profit Investments LLC.

Kingsley Iyare Osemwengie of Las Vegas, Nevada, was part of a sophisticated drug trafficking organization that diverted legitimate medicine such as oxycodone into the black market. The ring involved drug trafficking and money laundering activity in Massachusetts, Nevada, Texas, Florida, Georgia, Utah, Colorado, New York, Washington, Alaska, Pennsylvania and Oregon. This was the largest oxycodone trafficking case in the history of the District of Oregon based on the sheer volume of oxycodone distributed, the geographic scope of the conspiracy, and the enormous profits generated. A single 80 milligram oxycodone pill sold for a range of $30 wholesale to $80 retail. Osemwengie invested in luxury real estate and flashy jewelry including a watch decorated with over 1,000 diamonds.[32]

The traffickers used call girls to transport the drugs across the country, and Osemwengie even used one of them as the nominee for an anonymous shell company used to launder proceeds from his drug trafficking scheme. The company was aptly named High Profit Investments LLC[33] and was incorporated in Nevada.

### Fraudulent Online Pharmacy Diverts Prescription Drugs

**Mihran and Artur Stepanyan** operated at least four anonymous shell companies which they allegedly used to hide a wide-ranging criminal enterprise engaged in racketeering. Their biggest business consisted of diverting prescription drugs such as oxycodone from unlicensed sources to unknowing customers through a website pharmacy.

Mihran and Artur Stepanyan, along with at least 19 other people, are considered to be part of a nationwide drug diversion, money laundering and fraud enterprise, an online pharmacy. So much of the pharmacy's business was criminal that it qualified as a racketeering enterprise. The Stepanyans diverted legitimate prescription drugs and obtained other prescription drugs from unlicensed sources. **They used several anonymous shell companies, such as GC National Wholesale Inc.,[34] Nationwide Payment Solutions Inc.,[35] FM Distributors Inc.[36] and more to sell the drugs and launder the money.** During their operations over $393 million worth of drugs was distributed and over $5 million was stolen in financial crimes.[37] The operation was just beginning to experiment

with a murder-for-hire scheme when they got caught. The majority of their enterprises were based in Northern California, but also included Puerto Rico, New Mexico and others.

## Drug Money Laundering Disguised As "International Tax Planning, Asset Protection and Other Wealth Preservation Techniques"

**Martin Tremblay** ran a complex criminal operation centred around his use of multiple anonymous shell companies and training as an investment banker to launder drug money. His company fittingly claimed to be a leader in, amongst other things, "wealth preservation techniques."

Tremblay was the president and managing director of the Bahamas based **anonymous shell company, Dominion Investments Ltd.,[38] which he used to launder over $1 billion** from the firm's clients. The money he laundered came from all sorts of illegal activity including drug trafficking involving cocaine, GHB and other drugs. His money laundering scheme ran from 1998 to roughly 2005, and his company owned bank accounts all over the U.S. To further conceal the source and nature of these funds, Tremblay and his co-conspirators created shell companies and fictitious entities all over the world, including the U.S, using the same false nominees, addresses, and telephone numbers, to launder these illegal proceeds.[39]

## Money Launderers 'Teach' Undercover IRS How to Hide Drug Money

**Pavel Sosa Medina and Amado Vazquez Jr.** laundered money for others for profit using shell companies based in Kentucky and Florida. In a secret IRS sting operation, the pair laid out step by step instructions to undercover IRS agents on how to launder and hide their purported drug profits using anonymous shell companies.

Vazquez and Sosa Medina conspired to launder money for profit. The two were suspected money launderers from previous cases involving laundered drug profits through a Miami-Dade check-cashing company.[40] Using their history as a stepping stone, in an undercover operation, IRS agents approached the pair asking them to help launder around half a million dollars in supposed drug money. The pair, saying they were willing to help as their business was already involved in criminal activity,[41] laid out a step-by-step money laundering plan to the IRS that included shell companies, blank checks and multiple wire transfers.[42] **The anonymous shell companies they used were incorporated in Florida and Kentucky, and they included ZAN Providers LLC[43] and R.C. & Son Enterprise LLC.[44]** Both are in prison in Florida.

## Peruvian Airline Owner and Drug Kingpin Continues Criminal Activity From Prison

Notorious and violent drug trafficker **Fernando Zevallos**, founder of the airline Aero Continente, used two anonymous shell companies, La Hacienda (USA) LLC and Running Brooks LLC, to funnel his drug money into real estate in Florida.

Although in prison in Peru, Fernando Melciades Zevallos Gonzalez's criminal network continues to operate. Since the 1980s, **Zevallos has operated a drug trafficking organization and used two anonymous shell companies based in Miami, La Hacienda (USA) LLC**[45] **and Running Brook LLC,** [46] **both incorporated in Florida, to hide his drug profits.** After being designated a "significant foreign narcotics trafficker" under the Kingpin Act which froze his U.S. assets, Zevallos still managed to use the shell companies to move $1.4 million of his $1.7 million out of the United States. It is likely that to achieve this, Zevallos transferred the shell companies to be under his wife's name,[47] which is how the authorities tracked him. Key members of his associates and family continue to operate his drug network,[48] and the rest of his finances are still out of reach of the U.S. and Peruvian authorities.

## Fake Gold Miners Produce and Traffic Drugs

The elusive **Sanchez-Paredes family** have been operating a drug trafficking organization based in Peru for decades. They use Florida based anonymous shell companies such as Comarsa, a gold mining company, to produce cocaine and launder their profits.

Since the early 1980s Peruvian authorities have investigating the Sanchez-Paredes family who allegedly operate the Sanchez-Paredes Drug Trafficking Organization (DTO). There is a criminal complaint pending against the family in Peru, whilst in the U.S. investigations continue. Peruvian law enforcement believe that the Sanchez-Paredes DTO has financed various businesses including mining companies, farms, real estate investments, transportation companies and more, for the purpose of laundering many millions of dollars in narcotics trafficking proceeds. For example, **the Sanchez-Paredes DTO owns two anonymous mining companies, CIA Minera Aurifera Santa Rosa SA ("Comarsa") and CIA Minera San Simon ("San Simon"). Both of these firms claim to be mining gold but are believed to be manufacturing cocaine**; calcium oxide is used for both gold mining and cocaine production, and the amount seized by Peruvian authorities in 2007 was significantly more than the amount necessary to mine gold.

More generally, the Sanchez-Paredes DTO uses many shell companies[49] and bank accounts linked to them to hide and launder their drug profits. They used various distant family members as the nominal owners of the company while the names of the real owners remained hidden. Followed by a seizure of 12 bank accounts containing over $31 million from the family, Manhattan U.S. Attorney Preet Bharara said: "While this allegedly notorious drug trafficking family may be beyond our reach, the proceeds from their decade's long money laundering scheme are not."[50] Successful cases such as

this show how following the money can be an effective way of cracking down on drug trafficking, however this case is the exception to the rule due to lack of incorporation transparency.

## Former USC Athlete Leads Massive International Drug Trafficking and Money Laundering Organization

**Owen Hanson** allegedly the lead a violent international narcotics trafficking and gambling ring based in San Diego, California. His activities reached as far as Australia, and he used a U.S. based anonymous shell company called Big Dog Memorabilia Inc., to disguise his activities.

22 people were indicted in relation to the racketeering enterprise they allegedly named "ODOG", an international drug trafficking, illegal sports gambling and money laundering organization. The organization used runners to both collect gambling debts and deliver drugs such as heroin to customers. Along with many others, a Certified Public Accountant (CPA), Luke Fairfield, assisted the enterprise by setting up anonymous shell companies and advised them on how to structure their bank transfers to remain inconspicuous. **One of these anonymous shell companies' real name was Big Dog Sports Memorabilia Inc.,[51] which was a front company used to manage the money behind the organization's operations.** The enterprise employed violence and threats of extreme violence to ensure people paid their drug or gambling debts, and their reach extended as far as Peru and Australia. The case against Hanson and his associates is still ongoing in California.[52]

## Over 50 Luxury Vehicles Used to Launder Heroin Trafficking Money

**Addonise Wells and Mario Freeman** used anonymous shell companies to invest their heroin trafficking profits in luxury vehicles. They also employed **Jimmie Goodgame,** who also bought luxury vehicles and was involved in the money laundering aspect of the enterprise.

Addonnise Wells and Mario Freeman are accused of leading a large scale heroin trafficking ring in Ohio. The pair used an anonymous front company, Moe's Tire Company, to deliver the drugs and launder the profits. They also employed Jimmie Goodgame and his wife Stacey to **launder money for them through more anonymous shell companies. One of these companies was called J&G Enterprises I LLC,**[53] which was anonymous until 2008, when the agent's name was changed to that of Jimmie Goodgame.[54] It is unclear why this change occurred.

While the Goodgames bought luxury vehicles to protect and hide the money, Wells and Freeman bought real estate in the names of their relatives for the same purpose. These luxury vehicles were also used by Wells and his associates to transport drugs.[55]

Authorities had suspected the Goodgames' involvement in drug trafficking for years. At a coincidental traffic stop outside Chicago, police found over $500,000 in cash hidden in containers in one of the cars registered to Goodgame. With this evidence, they were able to build a strong enough case to go after the operation. Goodgame alone controlled at least $1.5 million in profits.[56]

## Los Zetas Drug Cartel Launders Money Using Race Horses

The leader of the infamous Los Zetas cartel, **Miguel Angel Trevino**, used anonymous shell companies to launder money. The cartel and its leader purchased race horses in Oklahoma, which they gave names such as 'Number One Cartel' both to keep their money safe and profit off horseracing.

The biggest of Mexico's drug gangs is the Los Zetas cartel, whose former leader...[is] Miguel Ángel Treviño...From 2008, **the Zetas used [anonymous] shell companies, in a scheme to launder millions of dollars of drug money into the United States, with the true ownership hidden behind front men.**[57] The money was hidden behind the purchase of race horses, some of whom were given names such as 'Number One Cartel' and 'Morning Cartel'. The horses were incredibly successful and reported to win the cartel several million dollars.

Fourteen people, including Treviño, were indicted on money laundering charges by the U.S. in 2012.[58] Treviño was captured in Mexico in July 2013.[59] As of September 2013, four co-defendants from the original indictment have yet to be caught. Nine people have been sentenced for their role in the scheme. [60] [61]

*This case study was excerpted from "The Great Rip Off" by Global Witness.*

## 'Boss of Bosses' Crime Lord and Drug Trafficker Still Free in Moscow

Known as the 'boss of bosses', the Russian **Semion Mogilevich** uses anonymous shell companies all around the world, including the U.S., to launder money for his vast criminal enterprise. Mogilevich traffics drugs, cheats on the stock market, facilitates prostitution, and more. Although several arrest warrants have been issued against him, he still lives freely in Moscow.

The FBI has described Semion Mogilevich as "the most dangerous mobster in the world," allegedly "involved in weapons trafficking, contract murders, extortion, drug trafficking, and prostitution on an international scale." [62]According to an indictment, that reputation did not stop the Russian from setting up a **vast network of anonymous companies, stretching from Eastern Pennsylvania to the United Kingdom[63], which allowed him to cheat the stock market and steal over $150 million from investors**

**in the United States and overseas**[64]...By inflating the price of his companies through manipulating securities and false reporting, including reportedly lying to the Securities and Exchange Commission, Mogilevich convinced investors to purchase millions in stocks in a company that allegedly did no real business. Those involved lost millions.

In spite of several arrest warrants issued against him, Mogilevich still lives freely in Moscow, according to the FBI. He has not been convicted for these crimes.[65] This case is a clear demonstration of how some drug trafficking organizations are part of a larger criminal enterprise involved in many different criminal activities. This it illustrates how money laundering tools such as anonymous companies can be used to hide and finance all kinds of illicit activities and layers of complexity that make it even more difficult for law enforcement to monitor, track and seize the proceeds derived from drug trafficking.

*This case study was excerpted from The Great Rip Off by Global Witness.*

## Recommendations

This report recommends that federal law makers end the use of anonymous shell companies by mandating the collection of true beneficial ownership information from all companies. This information then needs to be easily and efficiently accessible by law enforcement, who can then act on it to help curb drug trafficking and hence the ongoing opioid crisis.

*"U.S. shell companies [have] the dubious distinction of being the only money laundering method where secrecy is provided by a government entity...This is simply unacceptable."*

**- Adam Szubin,** Acting Under Secretary for Terrorism and Financial Intelligence of the U.S. Treasury

Quote from column published in the Hill, quoted in the Daily Sabah, July 12th 2016, http://www.dailysabah.com/americas/2016/07/12/us-shell-companies-cover-money-transfers-of-terrorists-traffickers-rough-states-treasury-official-warns

## Citations


[1] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. 3

[2] Health and Human Services, http://hhs.gov/sites/default/files/Factsheet-opioids-061516.pdf

[3] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. 11

[4] Centers for Disease Control and Prevention, *Injury Prevention & Control: Opioid Overdose*, http://www.cdc.gov/drugoverdose/epidemic/index.html

[5] The White House, *FACT SHEET: Obama Administration Announces Public and Private Sector Efforts to Address Prescription Drug Abuse and Heroin Use* (2015), https://www.whitehouse.gov/the-press-office/2015/10/21/fact-sheet-obama-administration-announces-public-and-private-sector

[6] National Institute on Drug Abuse, *What is the Federal Government Doing to Combat the Opioid Abuse Epidemic?* (2015), Presented by Nora D. Volkow, Director, National Institute on Drug Abuse, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations https://www.drugabuse.gov/about-nida/legislative-activities/testimony-to-congress/2016/what-federal-government-doing-to-combat-opioid-abuse-epidemic

[7] National Institute on Drug Abuse, *America's Addiction to Opioids: Heroin and Prescription Drug Abuse* (2014), Presented by Nora D. Volkow, M.D., Senate Caucus on International Narcotics Control, https://www.drugabuse.gov/about-nida/legislative-activities/testimony-to-congress/2016/americas-addiction-to-opioids-heroin-prescription-drug-abuse , figure 3

[8] Lenny Bernstein, "Why a bag of heroin costs less than a pack of cigarettes", *Washington Post*, August 27, 2015, https://www.washingtonpost.com/news/to-your-health/wp/2015/08/27/why-a-bag-of-heroin-costs-less-than-a-pack-of-cigarettes-2/

[9] Sergeant Stephen Opferman of the Los Angeles County Sheriff's Department, quoted by CNN (2011) http://money.cnn.com/2011/06/01/news/economy/prescription_drug_abuse/

[10] Centers for Disease Control and Prevention. Morbidity and Mortality Weekly Report, (2011), http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6043a4.htm?s_cid=mm6043a4_w#fig2

[11] National Institute on Drug Abuse, *America's Addiction to Opioids: Heroin and Prescription Drug Abuse* (2014), Presented by Nora D. Volkow, M.D., Senate Caucus on International Narcotics Control, https://www.drugabuse.gov/about-nida/legislative-activities/testimony-to-congress/2016/americas-addiction-to-opioids-heroin-prescription-drug-abuse

[12] Michael Botticelli, Director of the National Drug Control Policy, White House quoted in WNYT (2016) http://wnyt.com/news/white-house-drug-policy-director-albany-heroin-epidemic-public-health-epidemic/4158338/

[13] The White House, *How Illicit Drug Use Affects Business and the Economy*, https://www.whitehouse.gov/ondcp/ondcp-fact-sheets/how-illicit-drug-use-affects-business-and-the-economy

[14] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. 23

[15] Drug Enforcement Administration, *Programs: Money Laundering*, https://www.dea.gov/ops/money.shtml

[16] ibid pg. 3

[17] John Cassara, "Predictive Analytics: The Future of Successful Law Enforcement?", *Government Computer News* (2013), accessed from: http://www.johncassara.com/articles.html

[18] Internal Revenue Service, *Overview – Money Laundering*, https://www.irs.gov/uac/overview-money-laundering

[19] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. -19

[20] Raymond Baker, "Incorporation Transparency Laws", *Huffington Post* November 4th, 2009, Accessed from: http://www.gfintegrity.org/press-release/updating-incorporation-transparency-laws/
[21] Kevin G. Hall and Marisa Taylor, "The Crux Over Shell Companies: Who are the True Owners?", *McClatchy DC*, April 7th 2016, http://www.mcclatchydc.com/news/nation-world/national/article70602352.html
[22] Global Financial Integrity, *Anonymous Companies*, http://www.gfintegrity.org/issue/anonymous-companies/
[23] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. 24
[24] Paul Fitzgerald, "It's Time for Congress to Stop 'Financial Getaway Cars'", *The Des Moines Register*, May 12th, 2016 http://www.desmoinesregister.com/story/opinion/abetteriowa/2016/05/12/s-time-congress-stop-financial-getaway-cars/84250750/
[25] Federal Bureau of Investigation, *Crime in the United States: 2014*, https://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2014/crime-in-the-u.s.-2014/persons-arrested/main
[26] Cyrus Vance Jr., District Attorney for New York County, State of New York, op-ed published by Reuters, October 9, 2012.
[27] Drug Enforcement Administration, *Programs: Money Laundering*, https://www.dea.gov/ops/money.shtml
[28] Janice Ayala, Deputy Assistant Director, Office of Investigations, U.S. Immigration and Customs Enforcement, Testimony before the Committee on Homeland Security and Government Affairs, June 18, 2009
[29] Cyrus Vance Jr., District Attorney for New York County, State of New York, included in his testimony before the U.S. House of Representatives Task Force to Investigate Terrorism Finance, June 24, 2015.
[30] "U.S. Shell Companies Cover Money Transfers of Terrorists, Traffickers, Rough States; Treasury Official Warns", *Daily Sabah Americas*, July 12th 2016
[31] Daniel Glaser, Asst. Secretary for Terrorist Financing, U.S. Department of the Treasury, Testimony before the Senate Committee on the Judiciary, November 1, 2011
[32] Drug Enforcement Administration, "Nationwide Oxycodone Trafficking Ring Dismantled", April 29th, 2013 https://www.dea.gov/divisions/sea/2013/sea042913.shtml
[33] "High Profit Investments, LLC.", https://opencorporates.com/companies/us_nv/E0845552006-6
[34] "GC National Wholesale INC", https://opencorporates.com/companies/us_ca/C3441251
[35] "Nationwide Payment Solutions, INC." https://opencorporates.com/companies/us_ca/C3698786
[36] "FMC Distributors, INC." https://opencorporates.com/companies/pr/90905-111
[37] The Department of Justice, "Thirty-Three Defendants Charged in Massive Criminal Conspiracies Including Allegations of Fraud, Prescription Drug Diversion, and Money Laundering" May 7th, 2015 https://www.justice.gov/opa/pr/thirty-three-defendants-charged-massive-criminal-conspiracies-including-allegations-fraud
[38] "Dominion Investments Limited" https://opencorporates.com/companies/bs/19800B
[39] Drug Enforcement Administration, "International Money Manager Pleads Guilty to Laundering Drug Proceeds in Government Sting", November 21st 2006, https://www.dea.gov/pubs/states/newsrel/nyc112106.html
[40] Alfonso Chardy, "2 South Florida Men are Arrested on Money Laundering Charges", *Miami Herald*, December 19th, 2014, http://www.miamiherald.com/news/local/crime/article4677768.html
[41] ibid
[42] The United States Attorney's Office, Southern District of Florida, "Second Defendant Sentenced for Laundering over $400,000 in Currency from Purported Narcotics Transactions",

January 28th 2015 https://www.justice.gov/usao-sdfl/pr/second-defendant-sentenced-laundering-over-400000-currency-purported-narcotics

[43] "ZAN Providers, LLC" https://opencorporates.com/companies/us_ky/0851952

[44] "R.C. & Son Enterprise, LLC" https://opencorporates.com/companies/us_fl/L10000064587

[45] "La Hacienda (USA), LLC" https://opencorporates.com/companies/us_fl/L99000003231

[46] "Running Brook, LLC" https://opencorporates.com/companies/us_fl/L00000010931

[47] "La Hacienda (USA), LLC" http://www.companies-florida.com/la-hacienda-usa-llc-1ao9h/

[48] Drug Enforcement Administration, "Peruvian Kingpin and his Wife Indicted", July 27th 2007 https://www.dea.gov/pubs/states/newsrel/mia072707.html

[49] "Pacific Gateway Corp." https://opencorporates.com/companies/us_fl/P07000054235
"Advancer Logistics, LLC" https://opencorporates.com/companies/us_fl/L11000100906
"Exim Logistics Corp" https://opencorporates.com/companies/us_fl/P10000010063

[50] Drug Enforcement Administration, "Manhattan U.S. Attorney Announces Seizure of Over $31 Million in Connection with an International Drug Trafficking and Money Laundering Scheme", October 10, 2012 https://www.dea.gov/divisions/nyc/2012/nyc101012.shtml

[51] "Big Dog Sports Memorabilia Inc." https://opencorporates.com/companies/us_wy/2014-000663606

[52] The Department of Justice, "Twenty-Two Charged with Racketeering Conspiracy and Related Crimes Involving Drug Trafficking, Illegal Gambling and Money Laundering", January 27th, 2016 https://www.justice.gov/usao-sdca/pr/twenty-two-charged-racketeering-conspiracy-and-related-crimes-involving-drug

[53] "J&G Enterprises I, LLC." https://opencorporates.com/companies/us_oh/1549532

[54] Ohio Secretary of State's Office, Business filing portal, business search for 'J&G Enterprises I LLC' http://www5.sos.state.oh.us/ords/f?p=100:7:0::NO:7:P7_CHARTER_NUM:1549532

[55]Federal Bureau of Investigation, Cleveland Division, "Eight people indicted for roles in large-scale heroin trafficking and money laundering ring", May 12th 2011, https://www.fbi.gov/cleveland/press-releases/2011/eight-people-indicted-for-roles-in-large-scale-heroin-trafficking-and-money-laundering-ring

[56] Peter Krouse, "Heroin ring laundered drug money through luxury cars and real estate", *Cleveland.com*, May 13th 2011, http://blog.cleveland.com/metro/2011/05/post_459.html

[57] New York Times, A drug family in the winner's circle, 12 June 2012, http://www.nytimes.com/2012/06/13/us/drug-money-from-mexico-makes-its-way-to-the-racetrack.html?_r=0

[58] FBI, Federal grand jury indicts Los Zetas leader in money laundering scheme, http://www.fbi.gov/sanantonio/press-releases/2012/federal-grand-jury-in-texas-indicts-los-zetas-leader-in-money-laundering-scheme

[59] The Guardian, Mexico captures Zetas leader Miguel Angel Treviño Morales, known as Z-40, http://www.theguardian.com/world/2013/jul/16/mexico-drugs-trade

[60] U.S. Attorney's Office Western District of Texas, "Austin Horse Trainer Sentenced To Federal Prison In Multi-Million Dollar Money Laundering Conspiracy Involving Los Zetas Drug Trafficking Proceeds, Extortion, And Bribery", http://www.justice.gov/usao/txw/news/2013/Zetas_sentencings_2nd.html; Borderl and Beat, Carlos Nayen Borbolla sentenced to 15 years in zetas money laundering case, http://www.borderlandbeat.com/2013/12/carlos-nayen-borbolla-sentenced-to-15.html

[61] The Great Rip Off Map, "Los Zetas Drug Trafficking in Racehorse Scandal" http://greatripoffmap.globalwitness.org/#!/case/58010

[62] FBI, Top ten fugitives, http://www.fbi.gov/news/stories/2009/october/mogilevich_102109

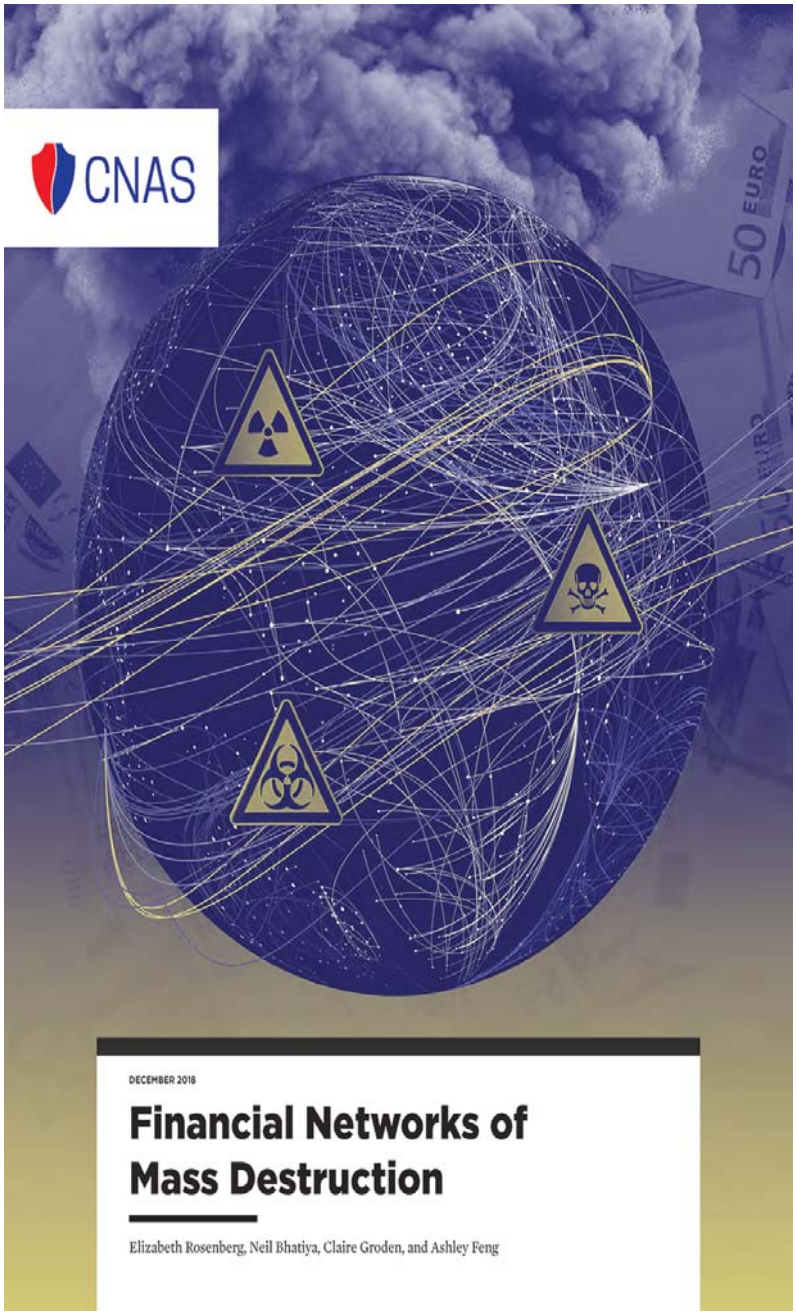
[63] U.S. District Court for the Eastern District of Pennsylvania, USA vs. Semion Mogilevich, Superseding Indictment, pages 14-15, https://www.documentcloud.org/documents/1278690-indictment-%20mogilevich.html#annotation/a175321 and https://www.documentcloud.org/documents/1278690-indictment-mogilevich.html#annotation/a175322

and https://www.documentcloud.org/documents/1278690-indictment-mogilevich.html#annotation/a175322

[64] U.S. District Court for the Eastern District of Pennsylvania, USA vs. Semion Mogilevich, Superseding Indictment, https://www.documentcloud.org/documents/1278690-indictment-mogilevich.html#annotation/a175320

[65] The Great Rip Off Map, "Russian Crime Boss Conned Investors out of Millions" http://greatripoffmap.globalwitness.org/#!/case/57957

**"FINANCIAL NETWORKS OF MASS DESTRUCTION", BY ELIZABETH ROSENBERG, NEIL BHATIYA, CLAIRE GRODEN, AND ASHLEY FENG**



## About the Authors


**ELIZABETH ROSENBERG** is a Senior Fellow and Director of the Energy, Economics, and Security Program at CNAS. Previously, she served as a Senior Advisor at the U.S. Department of the Treasury on international illicit finance issues, helping senior officials develop financial sanctions and formulate anti-money laundering and counterterrorist financing policy.

**NEIL BHATIYA** is the Research Associate for the Energy, Economics, and Security Program at CNAS. His work focuses on the geopolitics of energy, climate change, and tools of economic statecraft. Prior to joining CNAS, he was the Climate and Diplomacy Fellow at the Center for Climate and Security. He was previously a Fellow at the Century Foundation.

**CLAIRE GRODEN** is a JD candidate at NYU School of Law and former Program Associate at the Center on Law and Security at the law school. Previously she worked as a reporter at *Fortune* and *The New Republic* magazines. She holds a bachelor's degree from Dartmouth College in government and Asian studies, and a master's of law (Chinese studies) from Peking University, where she was a Yenching Scholar.

**ASHLEY FENG** is a Research Assistant in the Energy, Economics, and Security Program at CNAS, focusing on East Asia and China. Previously she was a Research Associate for China Studies at the Council on Foreign Relations, where she researched U.S. policy toward China and Chinese foreign policy.



**Cover Photo**
Images: Getty Images; Design: Melody Cook/CNAS


## Acknowledgements


The authors would like to thank Loren DeJonge Schulman for her review of this report. They also thank Zachary Goldman, Sue Eckert, Jonathan Brewer, and Frederick Reynolds for their valuable ideas and feedback during the drafting of the report. Finally, they would like to acknowledge Melody Cook, Tristan Campos, and Maura McCarthy for their assistance with the production of this report.

This report was made possible by the generous funding of the John D. and Catherine T. MacArthur Foundation.


## About the Energy, Economics & Security Program

The Energy, Economics, and Security Program analyzes the changing global energy and economic landscape and its national security implications. From the shifting geopolitics of energy to tools of economic statecraft, such as trade policy and sanctions, to security concerns tied to a changing natural environment, the program develops strategies to help policymakers understand, anticipate, and respond. The program draws from the diverse expertise and backgrounds of its team and leverages other CNAS experts' strengths in regional knowledge, defense, and foreign policy to inform conversations in the nexus of energy markets, industry, and U.S. national security and economic policy.

# FINANCIAL NETWORKS OF MASS DESTRUCTION

## Executive Summary

### Key Takeaways

- The lack of effective and universal financial controls to prevent weapons of mass destruction (WMD) proliferation is a gaping security vulnerability for the international community.
- Illicit actors, including those acting on behalf of countries such as Iran and North Korea, have exploited, are exploiting, and will continue to exploit these vulnerabilities.
- The United States has unique power and responsibility to combine domestic legislative and regulatory reforms with international leadership in order to strengthen the countering proliferation finance regime. Doing so will require overcoming significant political will obstacles.

The international community has long prioritized reducing the risk of weapons of mass destruction proliferation, whether from state actors such as North Korea and Iran, or from non-state actors, particularly criminals and transnational terrorist networks. Despite this concern, however, there remains a significant blind spot: the efforts to prevent the financing of WMD proliferation are only in their infancy. The legal framework to prevent the financing of proliferation is weak, and implementation across the world is spotty. These weaknesses derive from one overwhelming fact: The international community has not prioritized financial controls to fight proliferation. Very few countries have demonstrated the political will to put further emphasis on this threat to international peace and security.

The role of the United States is essential in building a stronger regime to counter proliferation finance. As the world's largest economy, with a sophisticated financial sector, well-resourced law enforcement and intelligence capabilities, and the ability to restrict access to the U.S. dollar, the United States has a great deal of leverage in helping those countries that wish to do more, and in compelling laggard countries to focus more intensively on the issue.

This is a crucial national security concern for the United States, even though to date it has not been approached as such. These networks are quite sophisticated at evading detection and know how to exploit weak regulations and enforcement in jurisdictions around the world. North Korea and Iran in particular have operated (and North Korea continues to operate) egregious, publicly documented, sophisticated global networks of trusted agents. These networks have contributed significantly to what had been an active uranium-enrichment program (in the case of Iran), and a substantial nuclear weapons capability (in the case of North Korea). These states are creative and diligent in developing new ways to continually disguise their activities, pioneering new technology and networks to sustain themselves and grow. The United States has prioritized dealing with North Korea and Iran as high-level security threats, but the proliferation finance aspect of that strategy has been woefully underdeveloped.

Stepping up action to combat the financing of proliferation will take legal change at home, including financial transparency measures and new methodologies to facilitate information sharing between banks and between banks and national authorities. It will also require intensive leadership in international forums such as the Financial Action Task Force (FATF) and at the United Nations (U.N.) to elevate due diligence and compliance around preventing the financing of proliferation. This will include revising FATF's recommendations to incorporate more proactive risk-based measures so that countries are judged on more than just compliance with screening against a list of proliferators subject to sanctions. The latter should focus on strengthening the work of the United Nations Security Council

**The weaknesses in the regime derive from one overwhelming fact: The international community has not prioritized financial controls to fight proliferation.**

Resolution (UNSCR) 1540 nonproliferation committee, improving the guidance that FATF provides on proliferation finance, and encouraging dozens of countries to improve their legal frameworks and dedicate the required level of attention and resourcing to fulfill their international obligations.

The risk of inadequately responding to the risk of proliferation finance is stark. The use of a weapon of mass destruction by a malign state actor or a non-state actor, especially a nuclear one, would be a generation-defining catastrophe. In the aftermath, the international community would ask what went wrong. What such a retrospective would discover is that such capabilities may have been facilitated through ordinary commercial channels. The response to such a discovery may have broad macroeconomic consequences. Avoiding that disaster, and the growth of threats emanating from WMD stockpiles in the hands of rogue actors, is the goal of this report.

**Strong measures to counter proliferation finance must be a key piece of a holistic approach to national security policy.**

This report explores the weaknesses of the current countering proliferation finance regime. Using case studies, it highlights how a lack of political will allows proliferation networks to obtain goods and move money in violation of international controls. It offers a survey of the current legal framework for approaching countering proliferation finance. This framework provides some important tools to U.S. and international authorities, but is alarmingly weak in many areas. The report then discusses how even a solid legal framework may flounder because of fundamental problems with political will at the national and international levels. It then offers recommendations for the United States and its international partners to build a much stronger countering proliferation finance regime. The report is designed to help security and foreign policy leaders understand the gravity of the issue and the necessity of elevating countering proliferation finance work in broader nonproliferation activities and analysis of transnational threats, especially North Korea and Iran policy. It argues that strong measures to counter proliferation finance must be a key piece of a holistic approach to national security policy, and it outlines a roadmap for how to get there.

## Introduction

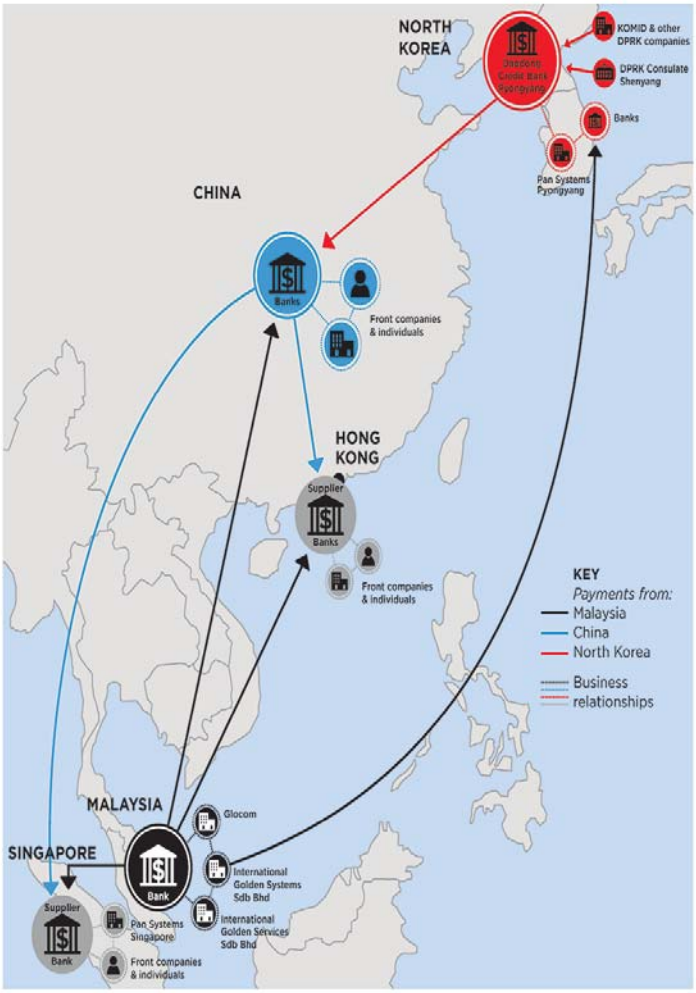
In December 2012, the Republic of Korea salvaged the debris of an Unha-3 rocket, which the Democratic People's Republic of Korea (DPRK) had used to launch a satellite into orbit. The launch was particularly alarming given the potential for the rocket to carry a nuclear warhead. Pyongyang's sophisticated nuclear program has for decades been a prominent national security concern for the United States, its allies South Korea and Japan, North Korea's ally China, and the wider international community.

After an exhaustive review, nonproliferation and illicit finance experts from the United Nations Panel of Experts on North Korea discovered the origins of many of the components the North Koreans used to build the rocket. Despite U.N. sanctions and the international consensus that Pyongyang obtaining sophisticated missile capabilities is a critical threat to international peace and security, the Unha-3 contained materials that had been manufactured in China, the former Soviet Union, the United Kingdom, Switzerland, and the United States, almost certainly transacting in currencies from major Western economies.[1]

As concerning as it was that North Korea was able to procure materials from advanced democracies and the world's leaders on nonproliferation policy, just as alarming is that many of the components were off-the-shelf items that were not included on export control lists designed to prevent goods from falling into the hands of proliferating states. The fact that North Korea was able to obtain commercial goods with such ease is a stark

*The wreckage of North Korea's Unha-3 sits at the 2nd Fleet Command's naval base on December 14, 2012. The U.N. Panel of Experts concluded that materials in Unha-3 had been manufactured in China, the former Soviet Union, the United Kingdom, Switzerland, and the United States. (Yeong-Wook/DongA Daily/Getty Images)*

**Figure 1: North Korea's Procurement Networks**[130]




*A simplified illustration of North Korea's sophisticated procurement networks, based in multiple countries. In this case, Pan Systems Pyongyang and its front companies carry out financial activity in multiple jurisdictions, which benefits, among others, the Korea Mining and Development Trading Corporation (KOMID), which is widely considered to be North Korea's primary arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons. Pan Systems Pyongyang's involvement in Middle East business is referenced without details (not shown).*

demonstration of the extent to which its proliferation networks have penetrated the international financial system. The ability of these networks to use shell companies to exploit globalized supply chains, penetrate financial networks to obtain goods not on export control lists, and obtain know-how threaten North Korea's neighbors and the world. This underscores the challenges facing financial institutions in trying to discover illicit activity.

The construction of the Unha-3 with internationally sourced components, procured using international financial channels, is but one example of what the financing of weapons of mass destruction proliferation looks like in practice. Figure 1 offers an illustrative example of how complex these networks are. North Korea, as well as Iran – especially before the implementation of the Joint Comprehensive Plan of Action (JCPOA) – Syria, India, and Pakistan, have all been at the forefront of global security concerns about how illicit and covert weapons of mass destruction programs are financed and supplied with materials.

### What Is Proliferation Finance?

In contrast to the nuclear weapons programs of advanced industrial states, many U.S. adversaries do not have the indigenous research, development, and deployment capacity to constitute weapons of mass destruction programs entirely on their own. As a result, they have to seek financial resources, goods, and know-how elsewhere, including from reputable industrial firms throughout the world, especially from the United States and Europe. The illicit networks that procure these goods and the revenue to sustain illicit WMD programs represent a serious national security threat: financing of proliferation is a critical backbone, the essential money trail, that enables rogue states, and non-state actors, to threaten peace and security.[3] These networks dupe and abuse public and private sector institutions alike, and cultivate complicit insiders. The stakes for this dirty money movement are high, and the response to date has been woefully and alarmingly lacking.

It is possible to detect and track the financing of proliferation. By going outside their own national borders to find support for illicit weapons programs, proliferating states leave themselves open to discovery by the international community. If moving money in exchange for goods is essential to building a weapons of mass destruction program, then it becomes possible for financial regulators, law enforcement, and intelligence agencies to track and disrupt it, and, where possible, to apprehend


*North Korea fired an intercontinental ballistic missile for the first time in four months in November 2017. Components of many North Korean rockets are procured from companies in advanced democracies, many of whom are considered world leaders on nonproliferation policies. (Chung Sung-Jun/Getty Images)*

members of the proliferation networks. Shutting down the money trail for proliferators can be a powerful and effective tool to check the devastating threat posed by rogue states with nuclear weapons. Ultimately, cracking down on the financing of illicit activities is an effective way to stop the illicit activity itself.

This is easier said than done. The issue facing the international community is that these networks are quite sophisticated at evading detection and know how to exploit weak enforcement in jurisdictions around the world. North Korea and Iran, in particular, have operated (and, in the case of North Korea, continues to operate) egregious, publicly documented, sophisticated global networks of trusted agents. These networks have contributed significantly to what had been an active uranium-enrichment program (in the case of Iran), and a substantial nuclear weapons capability (in the case of North Korea). These states are creative and diligent in developing new ways to continually disguise their activities, pioneering new technology and networks to sustain themselves and grow.[3]

In the wake of the U.S. withdrawal from the Iran nuclear deal, known as the Joint Comprehensive Plan of Action (JCPOA), it is possible that Iran may try to restart a nuclear-enrichment program, including potential steps to weaponization. Prior to the JCPOA, Iranian-affiliated actors had been implicated in a number of proliferation finance cases. In one case, Iran procured components for its nuclear and ballistic missile program through

**North Korea's evasion of international controls stands in stark contrast to its purported interest in assuring the international community that it is committed to normalization.**

a complex structure of payments channeled through banks in France, the United Arab Emirates, and Turkey to obtain materials from a Spanish manufacturer. The Iranian company in question was able to get around a denial of an export license by Spanish authorities for electrical discharge machines by using two different countries of transshipment.[4] Examples like this are important because they emphasize the truly global reach of these networks.

In the case of North Korea, despite the ongoing diplomatic process between the Kim Jong-un regime and the Trump administration, it is far from clear that Pyongyang

*Members of President Trump's cabinet and closest advisors have articulated concerns that Iran may try to restart its nuclear-enrichment program. (Chip Somodevilla/Getty Images)*

is on a path to denuclearization. In fact, attempts to procure proliferation-related goods appear to continue unabated, as evidenced by recent United Nations Panel of Experts reports. North Korea's evasion of international controls stands in stark contrast to its purported interest in assuring the international community that it is committed to normalization of relations.[5]

In the face of this persistent, even potentially expanding threat, the international community is willfully blind to the notion that policy and financial leaders, ideally together, can do much more to prevent the growth of illicit nuclear weapons. Foreign policy, security, and nonproliferation experts around the world unquestioningly accept a doctrine that extraordinary financial pressure and controls have tried and failed to constrain rogue proliferators. This assumption is wrong – the controls and pressure have never been, and still are not, as comprehensive as they should be. The potential cost of failing to fix this weakness is stark: a confrontation with a nuclear-armed state or terrorist group able to build an arsenal with the help of reputable Western companies would be a catastrophic global governance failure.

### The Role for the United States

The United States is well placed to correct this misperception and make a meaningful difference to check the global nuclear threat. Indeed, because the dollar is the global currency of choice for trade, investment, and as a reserve currency, and because the U.S. financial sector is the largest globally, the role of the United States to halt the financing of proliferation is vital. The current administration deserves credit for attempting to address this situation, but must do much more to focus maximum effort on constraining rogue countries' ability to pursue

an illicit weapons capability. This includes specific enforcement actions domestically, such as strengthening rules around financial transparency, extending safe harbor provisions for banks working creatively on finding proliferation finance typologies internally, and increasing resources for national law enforcement, and regulatory and intelligence agencies. It also means making countering proliferation finance the first priority for its presidency of FATF, the global standard setter for financial crimes regulation.[6] This will furthermore strengthen the control regime to the point that it can prevent proliferation threats from other countries and non-state actors much sooner. Financial network analysis is a key part of threat detection and evaluation for that effort, and the United States and the international community must use levers within the financial system to identify and deter the proliferation threat. The United States and certain jurisdictions in Western Europe, for example the United Kingdom, have built very powerful legal and regulatory powers to investigate, disrupt, and prosecute a wide variety of financial crimes risks, including money laundering and corruption. This is the base for attacking dirty money.

**Because the U.S. financial sector is the largest globally, the role of the United States to halt the financing of proliferation is vital.**

What is needed now is political will to fill in the gaps for the countering proliferation finance regime. The historic current lack of will stands in bewildering contrast to the clear and intensive concern that international policymakers have about the threats of weapons of mass destruction, particularly the use of nuclear weapons. The United States in particular has gone to great lengths to counter proliferation threats. The Trump administration has spent an enormous amount of political and diplomatic capital ensuring that North Korea and Iran cannot threaten their neighbors with nuclear weapons. With this base and the leverage that it has created, the U.S. administration must put in place the legal regime and policy guidance to better prevent the financing of nuclear-weapons proliferation.

Accomplishing this will take legal change at home, including with financial transparency measures and new methodologies to facilitate information sharing between banks and between banks and national authorities. It will also require intensive leadership in international forums such as FATF and at the United Nations to elevate due diligence and compliance around preventing the financing of proliferation, including revising FATF's recommendations to incorporate more proactive risk-based measures so that countries are judged on more than just compliance with sanctions. The latter should focus on strengthening the work of the United Nations Security Council Resolution 1540 nonproliferation committee, improving the guidance that FATF provides on proliferation finance, and encouraging dozens of countries to improve their legal frameworks and dedicate the required level of attention and resourcing to fulfill their international obligations.

Other jurisdictions look to the United States as an example because of the centrality of the U.S. dollar to international commerce. The size of its financial sector means that U.S. regulations directly and indirectly affect firms worldwide. U.S. intelligence and law enforcement capabilities are also unparalleled in finding and stopping these activities. The unique scale of these capabilities also gives the United States diplomatic heft in bilateral interactions with partners and allies facing risk because of proliferation financing, as well as in multilateral institutions where these issues are addressed, for example the U.N. and FATF.

The legal and administrative solutions are not hard to articulate. They include fixing gaps in national legislation, financial regulations, export controls, and other oversight mechanisms for global commerce. The truly difficult work for the United States will be urging, or compelling, the political will to fight the financing of proliferation, and reducing institutional resistance to sharing information with the private sector. Even though all U.N. member states are obligated under Chapter VII

*In November 2017, the United Nations Security Council held an emergency meeting concerning North Korea's nuclear ambitions after that nation test-fired an advanced intercontinental ballistic missile days earlier. (Drew Angerer/Getty Images)*

authority of the United Nations Charter to comply with Security Council resolutions aimed at combating WMD proliferation and its financing – and indeed many profess the will to do so – many sophisticated and well-resourced states do not.

An open secret of an enormous array of countries is that they are unwilling, or see themselves as unable, to sacrifice the economic advantages of looking the other way. They may even knowingly facilitate proliferation. For some countries, allowing North Korea to penetrate their financial system is lucrative, or affords political and diplomatic dividends, as discussed in the case studies in this report. These examples, which are notorious and in some cases date back decades, underscore the complex political calculations that serve as roadblocks for necessary action.

### The Peril of Willful Blindness and Failure to Prioritize

The weaknesses of the regime to counter proliferation finance contrasts markedly with how the international community handles efforts to counter terrorist financing. Two decades ago, the U.S. Treasury Department and relevant agencies in the U.S. intelligence community had tried to track al Qaeda's finances following the 1998 embassy bombings in Kenya and Tanzania, though it was not a high-priority effort, either within the United States government or internationally. Richard Clarke, President Clinton's top terrorism advisor, cited U.S. intelligence officials who downplayed targeting financing by saying that terrorist groups like al Qaeda "didn't need a lot of money."[7] However, over time the effort to counter terrorist financing was buttressed by a strong international framework: the United Nations had adopted a counterterrorist financing convention in 1999, and it was aided by specific U.N. Security Council resolutions, such as 1267 (1999). Enormous international political will to implement a holistic regime to counter the financing of terrorism coalesced after the disaster of 9/11. Global policy leaders realized after these attacks that following the money trails could be a blueprint to mapping the network and understanding – perhaps even anticipating – its moves.

In order to ultimately track Osama bin Laden to his Pakistani safe house, the U.S. intelligence community was able to use knowledge about the channels he used to circulate information and money. Bin Laden relied on couriers to convey messages and financial resources between him and his network of agents elsewhere in Pakistan, Afghanistan, and around the world. The documents seized in the raid on his headquarters offered extensive insight into al Qaeda's operations and plans.[8] During the past decade and a half, individual states and the international community built a sophisticated regime for countering the terrorist financing threat.[9]

But now the threat is evolving. Terrorist plots are overwhelmingly homegrown in the West (73 percent of attacks in Europe and North America from 2014 to 2017 were homegrown), and there is an uptick in incidents in Europe, with attacks increasing 7 percent from 2016 to 2017.[10] As a result, the regulation and practices to track and impede terrorist financing are becoming increasingly sophisticated and nuanced, taking a strong system and adapting it to present-day circumstances in a way that should serve as a model for other examples of countering threat finance.[11]

The risk now is that the international community will wake up to proliferation finance only after a similar paradigm-shifting event. The stakes are high and, based on expanding proliferation threats, it is certainly possible that we will learn a bitter lesson about the significance of countering proliferation finance efforts only after a major nuclear event has occurred. One of the gravest challenges for security leaders today is to avoid repeating an underestimation of the contemporary terrorist threat. In this case, this means realizing too late how blind and complicit we have been in allowing banks, businesses, and national governments to help grow rogue nuclear weapons arsenals.

This report offers a survey of the current legal framework for countering proliferation finance. As it now stands, this framework provides some important tools to U.S. and international authorities but is weak in many areas. The report then discusses how even a solid legal design may be inadequate because of fundamental problems with political will at the national and international levels. It then offers recommendations for the United States and its international partners to build a much stronger countering proliferation finance regime. This report is designed to help security and foreign policy leaders understand the gravity of the issue and the necessity of elevating work in countering proliferation finance to broader nonproliferation activities and analysis of transnational threats, especially with regard to policy for North Korea and Iran. Arguing that strong measures to counter proliferation finance must be key in a holistic approach to national security policy, this report outlines a roadmap for how to get there.

## The Current Legal Framework: Strong Initial Steps with Many Gaps to Fill

Frameworks to combat proliferation rely on three interlinked layers: international legal obligations put into place by the United Nations; the soft law framework, exemplified by FATF's recommendations; and domestic law. All three of these layers impact the risk management practices of global banks. In 1946, the United Nations General Assembly's very first resolution created a commission "to investigate the problems raised by the discovery of atomic energy." More than 70 years later, countering the proliferation of weapons of mass destruction remains a foundational goal of the international community.

The Security Council Committee established pursuant to Resolution 1540 (2004) (1540 Committee) monitors the implementation of Resolution 1540 (2004), which obligates states to have and enforce measures against the proliferation of nuclear, chemical, and biological weapons by non-state actors. The Security Council Committee established pursuant to resolution 1718 Committee (2006) (1718 Committee) is specific to North Korea's proliferation threat. It designates individuals and entities engaged in or providing support for North Korea's WMD programs, and individuals or entities who act at their behest. The 1718 Committee also monitors other restrictions on North Korean economic activity, such as its procurement and sale of energy resources, among other measures. But one tool in the counter-proliferation arsenal – countering the financing of proliferation – remains poorly understood and figures minimally in U.N. nonproliferation obligations, even as the international community increasingly seeks to use financial methods to rein in the nuclear programs of Iran and North Korea.

*U.S. Secretary of State Mike Pompeo chairs a United Nations Security Council meeting on North Korea. Since the beginning of the Trump administration, the U.N. Security Council has passed four resolutions establishing tighter economic restrictions on North Korea. (Spencer Platt/Getty Images)*

The global push to specifically counter the financing of proliferation had a promising start in 2004, when the U.N. Security Council passed Resolution 1540, a remarkably sweeping resolution that demanded member states enact comprehensive frameworks to prevent WMD proliferation and its financing by non-state actors. Unlike nearly all Security Council resolutions, which react to specific conflicts, this resolution sought to counter proliferation broadly, and it required member states to overhaul their sovereign laws in specific ways in order to do so.

Unfortunately, however, the drafters of Resolution 1540 (2004) concentrated primarily on controls on goods and materials, and it contains only two narrow references to financing: under operational paragraph 2, all member states are required to implement legislation to prohibit financing of manufacture, acquisition, possession, development, transport, transfer, or use of WMD, and their means of delivery, by non-state actors. Under operational paragraph 3(d), all states are required to implement controls on financing the export or transshipment of WMD and their means of delivery, and related materials.

Under operational paragraph 12 of a subsequent resolution, 2325 (2016), the 1540 Committee is required to continue to intensify efforts to promote full implementation of Resolution 1540 (2004). In particular, the need for more attention to proliferation finance measures, *inter alia*, is noted. Resolution 2325 (2016) is the first use of the term "proliferation financing" in a Security Council resolution, but, except insofar as Resolution 2325 (2016) is a successor resolution, the term is not defined.

Resolution 1540 (2004) on nonproliferation was unanimously approved by the Security Council in the aftermath of the discovery of Abdul Qadeer (A. Q.) Khan's WMD proliferation network (thus the primary focus of the resolution is on non-state actors: the businessmen, fixers, commercial traders, factory owners, etc., whom the network comprised, and also the terrorists seeking the capabilities). As of October 2018, 12 U.N. member states had yet to submit a report on implementation, as called for by the Security Council.[12]

A relevant U.N. resolution for comparing approaches to targeting the financing of a transnational security threat, Resolution 1373, was enacted weeks after the 9/11 attacks to establish similarly comprehensive frameworks to counter terrorism and its financing. The notably rapid and thorough implementation of Resolution 1373 was as


*In 2002, when border tensions were running high in South Asia, Pakistan test-fired a medium-range surface-to-surface missile. Pakistan has been at the forefront of global security concerns related to proliferation finance. (Handout/Getty Images)*

unprecedented as the resolution itself, with all members submitting a first report, as called for by the council within a year and a half of the resolution's adoption.[13] Member states widely criminalized acts of terrorism in their domestic laws, and the financing of terrorism was added to FATF's portfolio the same year it was enacted.[14]

The U.N. does require member states to counter state-led proliferation, with attention to financial channels, through a series of Iran- and North Korea–related resolutions. Targeted financial sanctions are at the core of such measures, but the provisions extend more widely to include activity-based sanctions, requirements for vigilance, and other prohibitions, for example on dealings with North Korean financial institutions and on financial services that could contribute to North Korea's WMD programs.

**Gaps in International Focus and Implementation**

U.N. member states have not pursued implementation of Resolution 1540 with the same level of political dedication as counterterrorism financing obligations. Some of these gaps are for legal reasons, which are addressed is this section. Due to a complex set of political, diplomatic, and economic circumstances, which are unique to each member state, violations of international obligations, many of which are brazen and well-documented, are allowed to occur.

Legally, one of the major challenges to states wishing to formulate domestic countering proliferation finance measures is that, unlike countering terrorist financing, working against proliferation finance measures is not linked to a specific international convention.[15] Additionally, member states are not prioritizing the clarification of how much effort 1540 requires to fight the financing of proliferation by states, as opposed to non-state actors. This misses the point that state proliferators such as North Korea, Iran, Syria, Pakistan, India, and others usually rely at least in part on overseas procurement networks made up of non-state actors – the primary target of Resolution 1540 (2004).

But significant problems also surround implementation of country-specific U.N. sanctions. As testified by numerous U.N. Panel of Export reports, as well as by independent analysts using open-source information, the vast majority of U.N. member states do not heed the requirements of U.N. sanctions and provide financial resources to the regime in North Korea, or they allow companies operating in their jurisdictions to facilitate transactions in violation of sanctions. Many sub-Saharan African states have had North Korean military personnel on their soil to provide training in exchange for cash that can be used by the regime to sustain and expand its proliferation programs, to cite one prominent set of violations.[16]

In other instances, some U.N. member states, including members of the Security Council, block more aggressive action for political or diplomatic reasons. Russia and China weakened U.N. Security Resolution 2375 (2017),

*Chinese President Xi Jinping delivers remarks at the United Nations General Assembly. Behind the scenes at the United Nations, China, along with Russia, weakened U.N. Security Resolution 2375, a nonproliferation resolution targeting North Korea. (Lintao Zhang/ Getty Images)*

*The lack of transparency in the shipping industry provides support to the illicit networks looking to evade U.N. sanctions. To date it has been difficult to build an international coalition to interdict ships bound for North Korean ports because of international legal concerns. (Spencer Platt/Getty Images)*

a nonproliferation resolution targeting North Korea, from its original draft that would have blacklisted Kim Jong-un, removed exceptions for all transshipments of Russia coal, and completely banned the hiring and payment of North Korean laborers abroad.[17] Similar to China, Russia also fears a collapse of the North Korean regime, which would result in a sudden influx of refugees to both China and Russia. A collapse could also result in possible conflict on the Korean Peninsula, as different powers try to seize control of North Korea's nuclear weapons.

To date, it has been very difficult to build an international coalition to interdict shipping bound for North Korean ports because of concerns that international law does not allow the forcible boarding of ships in international waters. Indeed, the ability of warships to legally board merchant vessels is quite limited: "A warship may only stop a merchant vessel if there is reasonable ground to believe (a) that the ship is engaged in piracy; (b) that the ship is engaged in the slave trade; or (c) that [though] flying a foreign flag or refusing to show its flag the ship is, in reality, of the same nationality as the warship."[18]

As the next section, "The Roadblocks Political Inaction and Inadequate Rules," will demonstrate, such activities are not solely a function of weaknesses around the legal regime, but rather have to do with much more fundamental questions of political will.

### Gaps at the Financial Action Task Force

The United Nations is not the only multilateral institution that is struggling, or stumbling, with a response to proliferation finance. While proliferation financing was added to FATF's portfolio in 2008, differing member opinions about the role financial institutions could or should play in detecting financing of proliferation ensured that the effort remained a relatively low priority element of FATF's work. FATF's current standards, guidance, and ongoing attention, for example, are not nearly as comprehensive for proliferation finance as they are for countering terrorist financing or anti-money laundering. This is true even while the proliferation risk is recognized by FATF's members, and indeed the international community, as a prominent security threat on par with these other challenges. The FATF recommendations that emphasize the importance of a risk-based approach for anti-money laundering and countering terrorist financing measures do not extend the principle to proliferation finance. Specifically, FATF's one

recommendation solely related to proliferation finance, Recommendation 7, is quite limited in what it requires of FATF member states:

> Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.[19]

As FATF's own non-binding guidance on proliferation finance makes clear, however, targeted financial sanctions alone are an incomplete strategy to really counter proliferation networks. Most sophisticated actors know how to structure their activities to avoid the scrutiny of sanctions screening:

> However, the [sanctions] screening would not be sufficient on its own, as targeted financial sanctions are also applicable to persons/entities acting on behalf of or at the direction of designated persons/entities. This adds additional complexities for public and private sector entities in identifying and detecting the persons, entities, and transactions related to proliferation financing.[20]

The latest version from FATF expands on 2013 guidance related to non-targeted financial sanctions elements of the requirements of U.N. sanctions resolutions. Unfortunately, it says little about the financial requirements of UNSCR 1540, the fundamental building block of the U.N. framework to combat proliferation. This is a significant gap that FATF should address quickly. The effort to do this needs to be led, or at least strongly encouraged, by the United States, which is in a unique position to do so while it holds the FATF presidency.


*Rick McDonell was the executive secretary of the Financial Action Task Force between 2007 and 2015, during which time FATF released a major typologies report on proliferation financing. FATF is the global standard setter for financial crimes regulation. (Aurelien Meunier/Getty Images)*

Besides comprehensive reviews by the 1540 Committee, there are few tools that precisely measure the degree to which states have implemented proliferation financing measures. In 2016, a comprehensive review on the status of implementation of Resolution 1540 (2004) shows that few states have dedicated proliferation financing legislation in place.[21] However, in comparison with previous reviews, the 2016 report noted significant progress between 2008 and 2016, as described in Table 1. While the numbers of measures to prohibit and enforce the prohibition of financing of proliferation activities and measures on the financing of illicit WMD-related transactions had increased, most states had not addressed the need to prohibit the financing of means of delivery, especially for nuclear weapons.

The comprehensive review also highlighted that most states rely on counterterrorism financing measures to address problems with proliferation financing. Although there was an improvement in measures on the financing of illicit WMD-related trade transactions, this was largely due to increased and improved legislation on counterterrorism financing, money laundering, and the establishment of financial intelligence units.

TABLE 1
**Financial Measures to Control WMD Proliferation under Resolution 1540 (2004)**

| | | NUMBER OF STATES | | |
|---|---|---|---|---|
| | | 2008 | 2011 | 2016 |
| **LEGISLATION IN PLACE** (obligations under operative paragraph 2) | **NUCLEAR WEAPONS** | 66 | 124 | 158 |
| | **CHEMICAL WEAPONS** | 71 | 129 | 166 |
| | **BIOLOGICAL WEAPONS** | 64 | 122 | 161 |
| **ENFORCEMENT MEASURES IN PLACE** (obligations under operative paragraph 2) | **NUCLEAR WEAPONS** | 78 | 119 | 155 |
| | **CHEMICAL WEAPONS** | 87 | 121 | 161 |
| | **BIOLOGICAL WEAPONS** | 75 | 114 | 156 |
| **MEASURES TO CONTROL FINANCING OF ILLICIT WMD-RELATED TRADE** (obligations under Operative Paragraph 3(c) and Operative Paragraph 3(d)) | **NUCLEAR WEAPONS** | - | 33 | 109 |
| | **CHEMICAL WEAPONS** | - | 37 | 110 |
| | **BIOLOGICAL WEAPONS** | - | 35 | 109 |

*Source: United Nations Security Council, Letter from the Chair of the Security Council Committee Established Pursuant to Resolution 1540 (2004), S/2016/1038 (December 9, 2016), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/1038.*

FATF statistics provide further evidence of inadequate implementation, despite the fact that the organization only focuses on U.N. financial sanctions on North Korea and Iran. FATF standards are assessed on a five-part scale:

- C: compliant
- LC: largely compliant; only minor shortcomings
- PC: partially compliant; moderate shortcomings
- NC: non-compliant; major shortcomings
- NA: not applicable. A requirement does not apply, due to the structural, legal, or institutional features of the country.

The effectiveness of implementation on these standards is measured by "immediate outcomes" on a four-part scale:

- HE: high level of effectiveness; the immediate outcome is achieved to a very large extent; minor improvements needed.
- SE: substantial level of effectiveness; achievement to a large extent, with moderate improvements needed.
- ME: moderate level of effectiveness; the outcome is achieved to some extent, but major improvements are needed.
- LE: low level of effectiveness; the immediate outcome is not achieved or only to a negligible extent, with fundamental improvements needed.

To date, 65 states have been evaluated against the 2012 FATF standards, which include Recommendation 7 (the North Korea and Iran targeted financial sanctions) and Immediate Outcome 11 (which demonstrate whether or not the implemented targeted financial sanctions were effective). These scores are shown in Table 2.

These data show that even against FATF's limited requirements on proliferation financing, states are inadequately meeting these standards both in terms of technical compliance and effectiveness.

The next two sections will outline the prevailing legal regimes in key national jurisdictions: the United States and a few other states. A survey of these legal regimes reveals a number of important factors. To begin with, countering proliferation finance sits at the intersection of several different legal and regulatory approaches, with different departments responsible for understanding and combating different aspects. This fact often leads to no single agency taking leadership and ultimate responsibility for a coordinated and comprehensive national approach to the issue.

On the one hand, a multi-agency involvement in the issue can be an advantage for building a stronger regime, as it increases the tools and resources that can be brought to bear on the problem. On the other hand, it also means that there are interagency "stovepiping" obstacles to closer cooperation. For example, both the Department of Defense and Department of State operate technical assistance programs run by the Defense Threat Reduction Agency for Defense and by the Export Control and

TABLE 2

**Cumulative Scoring of States against the 2012 FATF Standards**

| TECHNICAL COMPLIANCE | COMPLIANT | LARGELY COMPLIANT | PARTIALLY COMPLIANT | NOT COMPLIANT |
|---|---|---|---|---|
| NO. OF COUNTRIES | 10 | 14 | 21 | 20 |
| EFFECTIVENESS | HIGHLY EFFECTIVE | SUBSTANTIAL LEVEL OF EFFECTIVENESS | MODERATE LEVEL OF EFFECTIVENESS | LOW LEVEL OF EFFECTIVENESS |
| NO. OF COUNTRIES | 2 | 14 | 17 | 32 |

*Source: Financial Action Task Force, "Consolidated assessment ratings," (November 26, 2018), http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf.*

Related Border Security (EXBS) for State. U.S. partners who have worked with both programs rate the level of assistance as high quality. However, the two programs, according to experts, do not often communicate on proliferation finance priorities.

Beyond the national coordination issue, there are distinct groups of leaders and laggard states with regard to efforts to counter proliferation financing. The distinctions between the two – what makes one state capable and eager to fight the threat and another not – are important if the international community is to build an effective consensus and competency around fighting proliferation threats.

### The Legal Regime in the United States

The United States is a leader on countering proliferation finance due to its relatively strong existing statutory prohibitions and authorities, and the model it offers to other jurisdictions on how to address the issue. The United States is rare in having been rated highly effective in implementation of United Nations targeted financial sanctions on DPRK and Iran by FATF. However, the U.S. system features serious vulnerabilities as well that have allowed proliferators to take advantage of the system. These include challenges in banking regulations and the problem of anonymous companies, especially the extent to which the United States does not mandate the collection of beneficial ownership information, which refers to the individual who actually controls a corporate entity, even though the entity may not legally be in that person's name.

Broadly, the United States has one of the most well-developed legal and regulatory frameworks when dealing with financial crimes compliance issues. However, even these impressive capabilities do not fully incorporate proliferation finance as explicitly as the threat requires. In the United States as in the United Kingdom – two of the leading jurisdictions in countering proliferation finance efforts – efforts against proliferation finance have failed to come into their own as a distinct area of law. The financing of proliferation is not explicitly criminalized. Rather, countering proliferation finance is largely governed indirectly via three regulatory regimes: export control, sanctions, and anti–money laundering. This deficiency lowers its profile as a risk compared with countering terrorist financing. By comparison, while financing terrorism is a specific criminal offense, proliferation finance can be addressed only sideways using these three regulatory frameworks – none of which captures the full scope of proliferation finance alone, thereby contributing to the problem of willful blindness.

Before outlining what changes would be needed to more fully address the financing of proliferation, it is worth explaining how the existing U.S. legal framework, particularly export control, sanctions compliance, and anti–money laundering measures, treat the money-making and movement of proliferation networks. By sketching this legal framework, this section provides a snapshot of the current national patchwork of countering proliferation finance law. At the center of these three regulatory structures sit financial institutions, which have the potential to act as the first line of detection and denial when proliferators engage with the financial system. This is a necessary aspect of their work, as well as being a potential chokepoint to disrupt their activities, which

*The Trump administration, concerned that Iran will return to a nuclear-enrichment path that may include a weaponization component, has used diplomatic and economic tools to constrain Iran's abilities to do so. Iran's Army Day parade showcases examples of Iran's sophisticated missile capabilities. (Majid/Getty Images)*

underscores why proliferation finance is important and distinct from larger countering proliferation efforts. Banks can uniquely contribute through their knowledge of customer transactions. They must extend the work they already do to meet regulatory and legal requirements – and their regulators must better incentivize such activity. Like proliferation finance networks, financial institutions are transnational, with asymmetric influence, by comparison with national governments, to stem financial flows. However, that influence does not translate automatically into effectiveness. Too often financial institutions, even when aware of the proliferation threat, remain enablers of proliferation finance by acting as unwitting gatekeepers into the formal financial system. Awareness-raising, capacity-building, and technical assistance can ameliorate this situation, along with greater requirements for the sellers and shippers of proliferation goods. But political will, as this report emphasizes in a later chapter, must also be present for the entire system to work properly.

**Facilitating the countering of proliferation finance presents a significant regulatory compliance risk for banks.**

As a number of bank representatives emphasized in interviews with the authors of this report, financial institutions' obligations in the countering proliferation finance space are not black and white, particularly because the issue cuts across regulatory frameworks but lacks its own. For example, many banks approach proliferation finance efforts using the same perspective they take with sanctions screening. That is an incomplete foundation, however, as proliferation networks continuously create new entities to conduct illicit activity. These firms would be designated only after they had been caught conducting proliferation activity.

Other banks use strategies for dealing with money laundering threats to combat proliferation finance. While such strategies may help in thinking about how to collect data from commercial account holders involved in deceptive trading practices, money laundering and proliferation finance are distinct threats. Money launderers are trying to clean dirty money; proliferators want to move clean money in order to obtain goods illegally. More advanced banks recognize the need to build on their detection and investigation methods from anti-money laundering to tackle proliferation finance.[22]

For banks, facilitating the countering of proliferation finance presents a significant regulatory compliance risk. Their approach to detecting and reporting proliferators in their networks is informed by limited formal, as well as informal guidance from governments; the legal and regulatory frameworks outlined below; and their own appetite for risk. Many banks interviewed by this research team expressed a desire for clearer regulations and guidance (both public and, to avoid adaptation by the networks themselves, private) outlining their obligations regarding countering proliferation finance. More expansive regulations can offer a much stronger proliferation control regime, in which export controls, sanctions, and anti-money laundering work can be more aggressively targeted to better discover and disrupt proliferation networks.


*In May 2017, a U.S. federal judge approved "damming" seizure warrants for North Korean money in some of the United States' and the world's biggest banks, which included Deutsche Bank. (Thomas Lohnes/Getty Images)*

An additional weakness of the U.S. approach is the idea that expanding the legal regime around proliferation finance in the United States will be costly and have a negative impact on companies. It is true that the compliance divisions of international banks represent a significant cost center to their broader enterprises. However, focusing solely on the costs of additional regulatory scrutiny, not its benefits, is shortsighted. Companies are already paying costs of compliance by trying to do due diligence without having proper guidance about what the right flag posts and standards should be. It is in banks' interest to have a stronger and more efficient regulatory posture. Otherwise, the risks and costs are uneven and spread around banks and companies. Indeed, some of the biggest banks who are keenly aware of their vulnerabilities articulate this perspective themselves.

Many bankers, public officials, and analysts think the current system is deeply flawed and the United States is vulnerable. Former Deputy Assistant Attorney General and current Financial Crimes Enforcement Network (FinCEN) Director Kenneth Blanco has emphasized the ease with which sanctioned entities in North Korea were able to pass money through the U.S. financial system, for the direct benefit of North Korea's weapons of mass destruction program.[23] In one example from May 2017, a federal judge approved "damming" seizure warrants—which are used to block outgoing funds transfers—for North Korean money in some of the United States' (and the world's) biggest banks: Bank of America, Bank of New York Mellon, Citigroup, Deutsche Bank, HSBC, J. P. Morgan Chase, Standard Chartered, and Wells Fargo.[24]

*U.S. Secretary Wilbur Ross's Department of Commerce houses the Bureau of Industry and Security (BIS), which modifies the Controlled Commodities List of items whose export and re-export is controlled by BIS. (Win McNamee/Getty Images)*

### EXPORT CONTROLS

The U.S. export control system is a highly sophisticated web of authorities and statutes that play a key role in preventing the export of goods and technology related to weapons of mass destruction. Included in its purview are dual-use goods, which are primarily commercial and industrial items that could be used for either benign civilian purposes or military activities, including WMD program development. For example, in the 2015 case of *U.S. v. Hsien Tai Tsai*, the Department of Justice sentenced the defendant to 24 months in jail for exporting, without a license, rotary surface grinders from the United States to Taiwan with the ultimate destination of North Korea; these devices can be used to produce rings and gaskets, as well as rocket parts. Tsai had previously been designated for assisting North Korea's weapons of mass destruction program.[25]

The export control system integrates international export control regimes of which the United States is a member. These include the Nuclear Suppliers Group, Missile Technology Control Regime, Wassenaar Arrangement, Australia Group, and Zangger Committee. Within the United States, the implementation of the mandates of these regimes is split among several federal agencies: the Department of Commerce, Department of State, Nuclear Regulatory Commission, Department of Energy, Department of Treasury, and Department of Defense. The Department of State implements the International Trade in Arms Regulations, which controls non-nuclear defense technologies; the Nuclear Regulatory Commission implements nuclear product-specific export controls. The focus of these export control regimes is on exporters rather than banks, but there are legal implications for banks within the regulatory structure.

**The U.S. export control system is a highly sophisticated web of authorities and statutes that play a key role in preventing the export of goods and technology related to weapons of mass destruction.**

The export control regime of particular relevance in the counterproliferation context is the Export Administration Regulations (EAR), which is administered by the Commerce Department's Bureau of Industry and Security (BIS). The regulations' statutory authority originally derived from the now-expired Export Administration Act, which has been continued under the International Emergency Economic Powers Act. The EAR focuses on dual-use goods with predominantly commercial applications included on the Controlled Commodities List (CCL), a sprawling inventory of specific items whose export and re-export is controlled by BIS. Nuclear materials and chemical and biological weapons are all categories of these controlled items, but the list also covers industrial technology and components that could be repurposed for nuclear proliferation.[26]

Items not specifically listed on the CCL are still subject to the EAR: any item that is in the United States or originates in the United States (among other, more technical, specifications) is considered subject to the regulations. Exporters can determine whether a license is required for their item by identifying it on the CCL and comparing the classification number to a country chart that specifies the receiving countries for which that class of good

requires a license. A dual-use good with nuclear proliferation uses, for example, may be exported to Canada without a license, but not to Pakistan. In this way, the U.S. dual-use export control system monitors goods across two axes, taking into account both the risks of a particular item and its final destination.

The EAR includes general "catch-all" provisions (called EPCI, the Enhanced Proliferation Control Initiative) that significantly expand controls over proliferation-supporting activities. EPCI broadens U.S. export controls based on exports' end use, expanding EAR beyond simple list-based control. In Part 744.2, entities are prohibited from exporting, re-exporting, or transferring any item subject to EAR without a license that the exporter has knowledge (defined as to "know or have reason to know") will be used for nuclear explosive purposes or other illicit nuclear ends.[27] This provision expands the Commerce Department's authority to include any item – as long as it originated or exists in the United States – that is known to be destined for proliferation. Part 744.6 is of particular relevance to proliferation financing: it prohibits any U.S. person from knowingly supporting an export, re-export, or transfer of an item that has a proliferation-related end use. Support is defined to include financing.[28]

Banks are obligated to conduct due diligence and keep records of transactions concerning dual-use goods in their trade finance businesses. However, it does not appear that the Commerce Department has ever brought an enforcement action against a bank for failing to do so, and many bankers told this report's research team about the difficultly in keeping up with additions to export control lists. For banks, finding these listed goods among documents related to their purchase, sale, or transfer requires a granular knowledge of what is being shipped that is not available to banks handling the trade finance aspect of the transaction. This is true in large part because the way in which goods are labeled (on payment invoices, for example) does not often provide sufficiently detailed information to allow checking against what would appear on an export control list. Additionally, many banks have said they lack the expertise to vet export control lists.[29]

Another challenge is that many jurisdictions do not digitize trade finance documents. This makes it difficult for banks to quickly verify information about commercial transactions. As trade is increasingly conducted via "open account" terms – in which the buyer and seller do not rely on the bank for any crediting – banks are losing the visibility into transactions that trade finance traditionally provided.[30] A bank can still conduct standard sanctions screening against the parties involved in an open-account deal, but their ability to see the underlying reasons for the transaction, because of limitations in the amount of information a Society for Worldwide Interbank Financial Telecommunication (SWIFT) message can convey, is sharply curtailed.

**The lack of visibility into transactions is a serious vulnerability for broader counterproliferation efforts.**

This is a serious vulnerability for broader counterproliferation efforts: it is hard for banks to see the full spectrum of trade data, and it is difficult for customs, shipping agents, freight forwarders, and the wider shipping community to spot a suspicious money trail in the movement of goods. Currently, financial payment information available to banks generally offers extremely limited information about the details of a financial transaction. This is especially true in the trade space, where the payments are for goods, but banks cannot verify a lot of the information about what the goods are or their ultimate end use. Only 20 percent of global trade is conducted with trade finance, which requires greater disclosure of information about the transaction for the banks processing it.[31] The rise of the alternative open-account transfer is more prevalent, and ultimately features less transparency for the banks that are trying to scan transactions for proliferation-related goods. Expanding required information in financial payments would facilitate the collection of information that may help banks identify proliferation networks.[32]

#### U.S. SANCTIONS REGIME

The United States layers its own domestic sanctions authorities on the international nonproliferation sanctions regime of the United Nations, deepening the compliance obligations that national authorities place on banks beyond U.N. requirements. U.S. sanctions prohibit a broader range of activities and entities than do U.N. sanctions (for a comprehensive list, see Table 3: Executive and Legislative Actions That Form the U.S. Sanctions Framework Related to Proliferation). Domestic sanctions authorities can be developed by the executive or legislative branches, with executive orders primarily deriving their authority from the International Emergency Economics Powers Act. Legislative sanctions often address country-specific risks, for example

the North Korea Sanctions and Policy Enhancement Act of 2016. Most sanctions are implemented and administered by the Office of Foreign Assets Control (OFAC), which is within the Treasury Department and has the authority to designate entities, issue regulations, and conduct enforcement actions. The State Department also has the authority to designate entities and coordinate with OFAC in issuing sanctions guidance.

In addition to screening clients against sanctions lists, U.S. banks are advised to take risk-mitigation measures that ensure they do not inadvertently finance (1) designated entities hiding behind shell or front companies or (2) any proliferation activity by designated entities pursuant to WMD authorities.[33] Due diligence is required to make sure that banks freeze the assets of not only persons on the Specially Designated Nationals and Blocked Persons list, the U.S. sanctions blacklist, but also, generally, of entities owned or controlled by them. This poses a dilemma, though, when financial institutions do not have access to accurate or up-to-date details on who owns or controls a company (i.e., beneficial ownership information), because the jurisdiction in which they operate does not require its collection and disclosure in the corporation formation process.

This is embarrassingly the case in the United States, which FATF has graded as non-compliant for its failure to mandate beneficial ownership disclosure.[34] Despite entreaties to legislators from law enforcement and the banks themselves to patch this hole, congressional efforts to do so have consistently stalled. As long as that remains the case, it is almost certain that North Korean money is making its way through the U.S. financial system, obscured from the gaze of sanctions screening, as in the previously cited "damming" seizure warrants for banks processing more than $700 million in transactions on behalf of entities tied to North Korea.

Banks are also accountable for the broader activity-based sanctions embedded in international and domestic frameworks (including UNSCRs such as 2397, which restrict certain types of energy trade with Pyongyang, and Executive Order 13810) banning, for example, transactions that raise hard currency for North Korea via natural resource sales.[35] Despite the broad mandate of these sanctions, their enforcement on financial institutions so far has been limited, mostly to banks that were found to be transacting with entities already designated by sanctions. So far, Commerzbank AG, HSBC, and BNP Paribas are among the financial institutions that have been prosecuted and/or subject to civil enforcement under sanctions law for intentionally creating payment systems that omitted or obscured information to evade U.S. sanctions on proliferators.[36]

#### ANTI-MONEY LAUNDERING REQUIREMENTS

While proliferation financing is an area of lesser focus for many regulators and banks, money laundering is a familiar crime already subject to sophisticated legal frameworks. U.S. law does include financing of proliferation as a subset of the crime of money laundering, so many banks and regulators may believe that anti–money laundering compliance will also minimize banks' involvement in proliferation finance.[37] Consequently, components of countering proliferation financing practices at banks – such as flagging, investigating, and filing suspicious activity reports (SARs) on transactions of concern – originate in anti–money laundering programs.

However, effective anti–money laundering controls are not sufficient to combat proliferation finance: unlike money laundering, which tries to hide the origins of dirty money, proliferation financing involves raising money that is likely to support a weapons of mass destruction program, and that hides the purpose of the goods being purchased with often legitimate money. The typologies of proliferation finance differ from money laundering in a number of ways, including that the former often involves legitimate transactions at the front end.[38] Despite the shortcomings of anti–money laundering programs in the context of countering proliferation finance, they remain one of the most robust legal frameworks that apply to this nascent compliance space.

In the United States, the most important anti–money laundering statutes that create obligations for banks are the Bank Secrecy Act (BSA) of 1970 and Title III of the

**Effective anti–money laundering controls are not sufficient to combat proliferation finance.**

USA Patriot (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001, which significantly amends the BSA. Certain obligations and protections created by these statutes – such as filing SARs and safe harbors for companies to share information without legal liability for allowing past illicit conduct by customers – play a key role in banks' countering proliferation finance compliance work as well.

Under the Bank Secrecy Act, banks are required to undertake risk-based procedures for conducting customer due diligence and ongoing monitoring of accounts in order to report suspicious transactions. Banks are required to verify customers' identity before opening an account.[39] Banks must also submit SARs for any activity that might violate the law, or for any

TABLE 3

**Executive and Legislative Actions That Form the U.S. Sanctions Framework Related to Proliferation**

**EXECUTIVE ORDERS**

***General nonproliferation actions***

E.O. 12938 (1994): Underpins the general nonproliferation sanctions regime not specifically tied to a particular state. Prohibits the importation of goods or services provided by anyone found to be supporting proliferation activity.

E.O. 13094 (1998): Amends E.O. 12938 to include additional measures that should be taken against a foreign person determined by the Secretary of State to be contributing to any entity's WMD proliferation program. Those measures include a ban on federal government procurement from or assistance for the designated person, as well as a ban on importing any goods or services produced by the person.

E.O. 13382 (2005): Provides for the blocking of persons who have been designated as engaging in or supporting proliferation, and gives the Treasury Department the discretion to also block any persons financially supporting those listed.

***North Korea nonproliferation actions***

E.O. 13466 (2008): Declares a national emergency due to the threat of proliferation of WMD on the Korean Peninsula and transfers existing sanctions from the authorization of the Trading with the Enemies Act to the International Emergency Economic Powers Act, which authorizes the majority of contemporary sanctions.

E.O. 13551 (2010): Expands the scope of the national emergency related to North Korea declared by E.O. 13466, creating authority to block property and assets of listed persons pursuant to U.N. Security Council Resolutions 1718 and 1874.

E.O. 13570 (2011): Expands the scope of the national emergency related to North Korea in the previous executive orders, strengthening the Treasury Department's authority to implement U.N. Security Resolutions 1718 and 1874. Prohibits the importation of any goods from North Korea.

E.O. 13687 (2015): Implements U.N. Security Resolutions 2087 and 2094 by expanding the list of U.S.-blocked persons related to North Korea.

E.O. 13722 (2016): Implements U.N. Security Resolution 2270 and the North Korea Sanctions and Policy Enhancement Act. The order grants Treasury broad authority to designate persons involved in the North Korean economy whose revenue may indirectly contribute to the North Korean government, as well as those providing financial services to them. This order, in tandem with E.O. 13382, underpins the Treasury's imposition of secondary sanctions on Chinese and Russian firms in August, October, and November 2017 and August 2018.

E.O. 13810 (2017): Implements U.N. Security Resolutions 2321, 2356, 2371, and 2375 by giving Treasury the discretion to block any person operating in a range of commercial sectors in North Korea, among other activities, and those who provide financial services to them. The Treasury Department is also given the authority to impose sanctions on a foreign financial institution that knowingly violates sanctions, vastly expanding U.S. authority to impose secondary penalties. This order underpinned the imposition of such secondary measures on two Chinese firms in January 2018.[38]

***Principal Iran nonproliferation actions***

*Note: A broad set of executive and legislative authorities target Iran's threatening and destabilizing activity; these are not listed here. This table lists authorities tied specifically to Iran's illicit proliferation activities.*[39]

E.O. 13599 (2012): Implements secondary U.S. sanctions on Iran's Central Bank for concealing transactions between sanctioned parties. This blocks any U.S.-based assets of entities owned or controlled by the Iranian government, in part because of "the threat to government and financial institutions resulting from the illicit activities of the Government of Iran, including its pursuit of nuclear weapons."

E.O. 13716 (2016): Revokes E.O. 13574, 13590, 13622, and 13645; amends E.O. 13628; and provides for implementation authorities of sanctions outside the scope of the JCPOA.

E.O. 13846 (2018): Reimposes Certain Sanctions With Respect to Iran: Reintroduces measures that had been lifted by the JCPOA, with specific reference to countering a range of Iranian threats, including "Iran's proliferation and development of missiles."

**ACTS OF CONGRESS**

Chemical and Biological Weapons Control and Warfare Elimination Act (1991): Gives the president the authority to use the U.S. export control system to prevent the export of goods and technologies that would assist a country in developing the capability to produce or use chemical or biological weapons. Amends the Arms Export Control Act to establish a list of goods and technologies that would assist a foreign government in acquiring chemical or biological weapons.

Iran Sanctions Act (1996): Enacts sanctions authorities to target firms that sell to Iran any technology useful for its nuclear program or certain types of conventional weapons. The act also sanctions firms that invest in Iran's energy sector.

Iran, North Korea, and Syria Nonproliferation Act (2006): Authorizes the United States to impose trade sanctions on individuals and entities – not just governments – that engage in proliferation.

Comprehensive Iran Sanctions, Accountability, and Divestment Act (2010): Amends the Iran Sanctions Act to expand the energy-related activities relevant to Iran that are sanctionable and to add measures that can be imposed. The act also mandates the imposition of sanctions on foreign financial institutions that facilitate WMD transactions related to Iran, among other activities.

Iran Threat Reduction and Syria Human Rights Act (2012): Broadens the Iran Sanctions Act by requiring sanctions to be imposed on non-U.S. firms directly or indirectly involved in specified activities, particularly in relation to the provision of vessels and shipping services to transport certain goods related to proliferation or terrorism activities. U.S. firms can also be liable for the actions of their foreign subsidiaries that violate sanctions against Iran.

Iran Freedom and Counter-Proliferation Act (2012): Imposes sanctions on persons connected to Iran's energy, shipping, and shipbuilding sectors, as well as on those transacting in precious metals or materials that could be used in Iran's WMD or ballistic missile program. Financing any of these activities is also prohibited.

North Korea Sanctions and Policy Enhancement Act (2016): Requires the president to impose sanctions on anyone supporting or engaging in proliferation activities. Previously this was at the discretion of the president, in tandem with the Treasury and State Departments. This act also widens U.S. authority to impose secondary measures.

Countering America's Adversaries through Sanctions Act (2017): Imposes sanctions on Iran, Russia, and North Korea pursuant to an array of threats, including, in the case of North Korea, proliferation activity. It updates the North Korea Sanctions and Policy Enhancement Act to include subsequent U.N. Security Council sanctions; prohibits indirect correspondent accounts; and enhances inspection authorities to enforce North Korea–related sanctions.

customer activity that is abnormal for that person's profile and has no clear business or lawful purpose. In addition to flagging potential instances of money laundering, these SARs can be used to flag proliferation-related activity – even though banks interviewed by this research team expressed difficulty in differentiating suspicious activity linked to proliferation from other suspicious activity and difficulty in identifying proliferation financing at all. Indeed, U.S. government officials interviewed for this report said that the utility of specifically flagging proliferation finance as the reason for a SAR was of dubious value, although that may be a function of the sophistication of the U.S. jurisdiction. It may be valuable for national authorities in other, less mature jurisdictions to have their financial institutions flag proliferation-linked transactions, in order to raise awareness within the compliance community as to the importance of looking for these red flags.[40] What matters is that the SAR is filed in the first place, and that as much descriptive information as possible about the transactions and account holders is included.

Current and former members of the law enforcement community told the authors of this report that knowledge of a possible proliferation transaction is not usually what initiates a broader investigation, but it is an important piece of data for mapping a network and has figured in previous proliferation cases.[41] Such reports may initiate a probe and can certainly have value in ongoing investigations that have been launched with a predicate offense of money laundering or violation of trade controls.

The Patriot Act amended and strengthened the BSA to require U.S. financial institutions to apply enhanced due diligence to correspondent banking accounts, which are any account established for conducting transactions with a foreign financial institution. The Patriot Act also required banks to apply enhanced scrutiny to accounts held by senior foreign political officials, known as politically exposed persons. Because of their role in cross-border payments, correspondent accounts virtually always factor into proliferation finance pathways:

North Korea, for example, is known to commonly use correspondent accounts with Chinese banks to facilitate international transactions.[43] The amended BSA made anti–money laundering measures even more applicable to countering proliferation finance efforts by placing them under greater scrutiny.

The Patriot Act includes provisions under Sections 314(a) and 314(b) to encourage and allow information sharing between banks and the federal government regarding potential money laundering and terrorist financing activities. Under these provisions, the U.S. government is able to query banks for specific information, through FinCEN (and receive other information from banks), and banks are given certain liability protections to share information with one another regarding money laundering and terrorist financing. The sharing of proliferation finance information is broadly, though not universally, considered to be swept into the authorities for money laundering information exchange. A more explicit legal reference about its inclusion could enhance information exchange on this topic, encouraging banks to focus more on it because their regulators would be given a more explicit focus on it.

Recently, the Treasury Department has taken increased advantage of Section 311 of the Patriot Act to counter proliferation finance. Section 311 allows the Treasury Secretary to designate a foreign jurisdiction, account, or financial institution as being of primary money laundering concern. This designation allows the Treasury to require domestic financial institutions to take special measures in relation to the designated entity, such as additional due diligence or limitations on the opening of correspondent accounts. In practice, given the salience for all major international institutions of abiding by U.S. law, this means a 311 designation can have a crippling effect on a target.


*Former U.S. President George W. Bush speaks about the Patriot Act at the National Counterterrorism Center. The act significantly amended the Bank Secrecy Act of 1970, creating certain obligations and protections that play a key role in banks' countering proliferation finance compliance work. (Mark Wilson/Getty Images)*

The first, and most prominent use of the 311 authority against a proliferator was in 2005, when the United States designated Banco Delta Asia as an institution of primary money laundering concern, acting specifically on behalf of North Korea.[43] In 2016, the United States designated North Korea as a jurisdiction of primary money laundering concern and prohibited U.S. financial institutions from opening correspondent banking accounts on behalf of North Korean banks. U.S. financial institutions are required to conduct enhanced due diligence to make sure North Korean entities are not gaining access – even indirectly – to U.S. correspondent accounts.[44] The Treasury Department also used the 311 authority to designate the Bank of Dandong as of primary money laundering concern for violating U.S. and U.N. sanctions on North Korea in November 2017, effectively cutting the Chinese bank off from the U.S. financial system.[45] In early 2018, FinCEN pursued a 311 action against ABLV, a Latvian bank that had facilitated North Korean financial transactions in violation of U.S. and U.N. sanctions.

**A Section 311 designation allows the Treasury Department to require domestic financial institutions to take special measures in relation to designated entities.**

#### FOREIGN LEGAL REGIME: LEADERS AND LAGGARDS

While the United States has been an effective standard setter, it is not the only major international player that has implemented a powerful legal and regulatory framework for countering proliferation finance. However strong or weak the international frameworks established by the United Nations or FATF are, they are translated into laws, regulations, and procedures at the national level, which includes the risk management practices of global banks. The capacity, resources, and will that any one country can bring to bear on this issue vary widely. Strong national-level legal frameworks have some particular themes in common. First, they allow for the fast and efficient imposition of United Nations sanctions, particularly those targeting specific state actors such as North Korea.

Second, like the United States, nations in the top ranks have laws in place to cover export control frameworks, sanctions, anti–money laundering, and other financial transparency measures. FATF has underlined the intertwined nature of countering proliferation finance and export controls in its own reports: "Many of the policy options for countering proliferation finance draw on resources already available through the export control system, or are dependent on information or legal authorities which is available only from export control authorities."[46]

The United Kingdom and Australia are good examples of countries with effective political leadership and technical expertise on proliferation issues that could serve as models for other jurisdictions. They are both major international trading nations and active members of international regimes for the control of illicit goods, including the Australia Group, Nuclear Suppliers Group, Wassenaar Arrangement, and Missile Technology Control Regime.

Australia, in particular, has been recognized for leading legislation on countering proliferation finance. Australia's Charter of the United Nations Act of 1945 provides a legal framework to implement Security Council Resolutions, including those related to proliferation finance. These regulations are then made by the executive branch, but do not have to be passed by parliament, allowing for speedy amendments that can "ensure timely compliance with Security Council Resolutions."[47] Besides an overarching framework for implementing UNSCRs, Australia's parliament also passed related "Regulations on Dealing with Assets, Democratic People's Republic of Korea, Iran, and Customs (Prohibited Exports)." Australia has a profound advantage over the United States, in that its Australian Transaction Reports and Analysis Centre has access to all cross-border transactions, on which they can immediately run analysis. U.S. rules, by contrast, require the collection of data only for transactions exceeding $3,000, and have to request the data directly from banks.

*The United Kingdom has a leading framework on proliferation finance. Unlike other jurisdictions, the U.K. criminalizes activities that constitute proliferation finance. (Jack Taylor/Getty Images)*

The United Kingdom currently operates under European Union (EU) rules for countering proliferation, though it does have its own regulatory framework for trade controls, and is currently involved in "onshoring" much of the regulatory framework to U.K. law in response to its decision to leave the European Union (for example, by passing legislation granting it the authority to impose sanctions). Much like the U.S. export control system, however, the EU regulation governing dual-use goods includes a catch-all clause (Article 4) requiring exporters and firms providing brokering services to notify and seek approval from national authorities if they are aware that a dual-use good is destined for a WMD-related end use. This clause allows the regulation to include items that are not on the EU dual-use list.[48] In this regulation, "brokering services" excludes financial businesses, differentiating the EU regime from that of the United States by omitting financial service providers from the catch-all provision.

Another important benchmark enshrined in U.K. law is the set of regulations that update previous compliance requirements for banks in detecting and preventing money laundering and terrorist financing. Banks are required to carry out ongoing monitoring and customer due diligence practices, as well as enhanced due diligence in certain high-risk circumstances.[49] Banks must also create anti–money laundering policy statements and keep records of customer due diligence practices. And banks are required to try to identify money laundering or terrorist financing being carried out by their customers, and to alert the National Crime Agency (NCA) with a SAR. Though the regulations were enacted to fulfill the

**The United Kingdom and Australia are good examples of countries with effective political leadership and technical expertise on proliferation issues that could serve as models for other jurisdictions.**

U.K.'s obligations to implement the EU Anti-Money Laundering Directive, it is unlikely that Brexit will result in any rollback of the regulations due to the U.K.'s independently aggressive stance toward money laundering.

The Proceeds of Crime Act 2002 is the U.K.'s other primary legislation governing anti-money laundering programs, which makes it a crime to fail to disclose information when banks "know or suspect" that money laundering is taking place, an important diligence standard.[50] This statute makes it possible for banks to be held criminally liable for failing to file SARs to the NCA. In 2017, the Proceeds of Crime Act was updated by Section 11 of the Criminal Finances Act, enabling banks to share information among themselves about money laundering activities in order to jointly file reports to the NCA.[51]

Importantly, the United Kingdom, through the Anti-Terrorism Crime and Security Act of 2001, pointedly criminalizes activities that constitute proliferation finance, given domestic law enforcement a powerful legal tool.[52] The United Kingdom also emphasizes the importance of interagency coordination. Sanctions are enforced by the Office of Financial Sanctions Implementation in the Treasury, with assistance from the National Crime Agency (to investigate sanctions breaches), Her Majesty's Revenue and Customs and the Export Control Organization (to enforce trade sanctions), and the Foreign and Commonwealth Office (to negotiate sanctions).[53] Unlike the United States, the United Kingdom also recognized that financial transparency can enable it to meet national security goals. The U.K. government has proposed a public beneficial ownership registry for corporate entities that own or control property in the United Kingdom.[54]

#### STATE OF THE REGIME IN HIGH-RISK JURISDICTIONS

A number of jurisdictions at a high risk for facilitating proliferation finance, particularly in East Asia, stand out for trying to pioneer solutions, notwithstanding different resource bases and risk profiles. Broadly speaking, they are reasonably well resourced, with technical competency and sophistication as regards tracking illicit financial activity and proliferation activities. Several have shown prominent recent efforts to implement legal authorities and controls around the financing of proliferation. As highlighted by researchers Andrea Berger and Anagha Joshi, Malaysia's Strategic Trade Act imposes severe criminal penalties for export control violations of "strategic items and technology." This act specifically targets individuals and entities involved in financing the acquisition of weapons of mass destruction.[55] The implementing authority in Malaysia, the Ministry of International Trade and Industry, offers continuous guidance and training on the obligations for the Strategic Trade Act for businesses operating in the country.[56] FATF has recognized these efforts, complementing Malaysia for its strong legal and regulatory framework and good interagency coordination, but also encouraging it to improve its framework for using targeted financial sanctions against WMD proliferation.[57]

Thailand is another jurisdiction that has been exploited by proliferation networks – including by entities and individuals who have acted on behalf of North Korea's Ocean Maritime Management (OMM), a North Korean shipping firm known to be involved in arms trafficking.[58] Thailand's Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act of 2016 includes specific and detailed legislation targeting proliferation financing. Notably, the act provides for the immediate listing of persons and entities sanctioned by the United Nations, and specifies criminal liability for a broad range of illicit activity, including:

> providing or collecting funds or conducting a financial or asset transaction or acts in any way to commit a terrorist act or proliferate weapons of mass destruction; acting with the knowledge that the beneficial person of that financial or asset transaction is a designated person; or acting with the intention that the funds or asset are to be used in support of any activity of a designated person or persons, a group or an entity involved in terrorism or the proliferation of weapons of mass destruction.[59]

Conversely, laggard countries that do very little to identify and impede proliferation financing are each weak in their own way. For some countries, there are scant legal prohibitions to fight proliferation finance. This is a foundational problem for many of the least well-resourced jurisdictions. Other countries lack the legal, monetary, and subject matter expertise resources, and need significant technical assistance. FATF, as part of its global review processes, issues public statements about deficient jurisdictions that the body is monitoring, highlighting specific gaps in national laws or implementation. States can graduate from such close and critical scrutiny, exiting monitoring by creating and implementing comprehensive plans to improve anti-money laundering and countering the financing of terrorism (AML/CFT) measures. This can have a beneficial impact on combating proliferation finance as well. However, given the previously described limitations on

the requirements and guidance that FATF and the U.N. set out for countries, a plan for greater national financial transparency and monitoring may yet leave countries inadequately equipped to combat the threat.

Among these "high-risk and other monitored jurisdictions" identified by FATF in its review as of October 2018 are North Korea, Ethiopia, Iran, Pakistan, Serbia, Sri Lanka, Trinidad and Tobago, Tunisia, and Yemen.[60] Not surprisingly, many of these countries are high on the list of jurisdictions about which the international community is concerned for countering terrorist financing, or are active combat zones involving foreign terrorist organizations (Syria, Pakistan, and Yemen). North Korea is an extreme proliferation risk, which unsurprisingly

**For some countries, there are scant legal prohibitions to fight proliferation finance.**

has failed the test for adequate international financial standards. Iran is under enormous scrutiny from the United States for proliferation activity (though FATF's most recent statement on Iran focused on its AML/CFT deficiencies, reflecting the current focus of FATF standards).[61] Pakistan, too, is an extreme proliferation risk because of both its rapidly developing nuclear weapons program and the proliferation activities of A. Q. Khan and his international network, uncovered only in 2003.

For other states with moderate deficiencies, such as China, which was last rated as non- or partially compliant with 25 out of the 40 FATF recommendations, FATF has identified specific legal measures that need to be taken to assure the international community that the countries are improving their frameworks for combating illicit and criminal financial activity (including potential financing of proliferation).[62]

By way of example, in its June 2018 compliance report on global AML/CFT, FATF highlighted the following needed changes to improve financial sector transparency, among a variety of issues: implementing targeted financial sanctions (Ethiopia); improving interagency and federal-provincial cooperation (Pakistan, a noted proliferation risk); ensuring that national authorities have timely access to beneficial ownership information (Serbia); enhancing even the most basic risk-based supervision of financial institutions (Sri Lanka); and encouraging national authorities to pursue prosecutions when criminal cases are made (Trinidad and Tobago).[63]

The cases of India and Pakistan are worth further discussion, and Pakistan is covered in a later case study. There is a clear distinction in how the international community and the United States approach proliferation risk from countries that are under sanctions regimes (Iran, North Korea, and Syria) versus those that are not (India and Pakistan). As will be discussed in the Pakistan case study, sanctions on India and Pakistan were removed for political reasons – the underlying proliferation and acquisition of goods in violation of export control regimes never stopped. The international community simply decided its limited bandwidth was better used against other proliferation threats. It is worth questioning whether that acquiescence has permitted the sustainment of dangerous networks and contributed to an arms race in South Asia that is extremely destabilizing.

#### POLICY CHANGE: SEIZING THE OPPORTUNITY

Highlighting these specific deficiencies provides a roadmap for the international community to tailor properly its technical assistance work. To be sure, this work is challenging for governments and banks alike as a practical matter, given the breadth of regulatory requirements and resource constraints. That difficulty is only exacerbated, however, by a lack of high-level political prioritization, and by the fact that the international community has not reached consensus on building a true, institutionalized, practical commitment to more information gathering, disclosure, and sharing.

If the U.S. administration wishes to challenge adversaries on nonproliferation priorities, it has no choice but to keep pushing on international standards and national-level compliance related to countering proliferation finance, prioritizing opportunities to advance a more ambitious policy framework. There is a strong possibility that countering proliferation work may be possible even while other nonproliferation issues remain highly controversial, including how to approach Iran's ambitions. The United States has significant ability to shape the issue from Washington, especially by focusing on congressional legislation, and with Treasury officials making the most of leadership opportunities during the U.S. presidency of FATF from 2018 to 2019. Some U.S. officials have embraced this perspective, as evidenced in their agenda document for the FATF presidency, but bandwidth issues, exacerbated by the short duration (one year) of the FATF presidency are significant challenges.[64] This is compounded by the fact that China, which is a drag on leadership on these issues, will assume the FATF presidency in mid-2019.

In its most recent plenary, FATF announced that it was starting a project to gauge the degree of support among

member states for expanding the FATF recommendations for countering proliferation finance and for enhancing the implementation of existing obligations. The project will also consider developing best practices on combating proliferation finance. These may address such issues as criminalization, international cooperation, and how to conduct risk assessments. Unfortunately, it is unlikely that the U.S. delegation will serve as a co-chair for that effort, which reduces the chances of pushing meaningful changes the project team recommends at a future plenary. It is certainly unlikely to happen quickly, while the United States holds the FATF presidency.[65]

### The Influence of International Rules on the Private Sector

The private sector must match major steps taken by the government sector if the countering proliferation regime is to work effectively. The private sector responds to the requirements and incentives put in place by their regulators, and to the information that government shares with them to identify and track proliferators. This means that the information and signaling from governments is a crucial function of how effective banks can be at impeding proliferation finance. Regulators in the United States and elsewhere need to signal with concrete legal and regulatory steps that banks must specifically look for proliferation finance, not merely maintain adequate controls against illicit finance. And national governments must lean much further forward in supporting this work by sharing lead information to better identify proliferation finance. Only by adopting this posture will regulators properly balance the costs of economy-wide rules and regulations with the benefits to U.S. national security and actually enable a change in counterproliferation efforts within the private sector.

As governments engage with their banking sectors, they must realize that this is often difficult work for even the most sophisticated financial organizations to carry out correctly and thoroughly on a constant basis. Governments must be prepared to create legal and regulatory frameworks for the greater sharing of information and provision of guidance; otherwise banks will continue to struggle to differentiate proliferation-linked transactions from the much larger volume of legitimate commercial trade they resemble. It is very difficult for global banks to conduct proper due diligence on the customers who are account holders with their correspondent banking partners in high-risk jurisdictions. Ensuring that banks that self-report are not exposed to legal jeopardy is also a crucial step. These positive incentives should exist alongside the threat of fines and legal action.

## The Roadblocks: Political Inaction and Inadequate Rules

The most prominent obstacles to a strong countering proliferation finance regime originate in a fundamental lack of political will. This is clearly demonstrated by the very weak, nascent global regime to counter proliferation finance. It may be more accurate to say there are numerous uncoordinated national efforts that attempt to work together, but the whole is far less than the sum of its parts. There is no good public policy reason, aside from a lack of political will to prioritize the issue, to explain inaction on laws and regulation, or why the United States cannot build stronger domestic financial transparency, or has not been more forceful in setting the tone at the U.N. and FATF.

Despite the fact that some legal regimes – in the United States and in some more sophisticated jurisdictions – have developed significant tools to combat the financing of proliferation, the problem persists, with numerous examples of networks operating with ease. The next section analyzes why these problems persist despite clear-cut rules. There are obvious economic reasons for which such activity continues: some states find it lucrative to continue to trade with proliferating states like North Korea. There are also political reasons for why some jurisdictions do not pass sufficiently strong laws (or do not enforce them). Some jurisdictions believe stronger rules hurt business interests, or cracking down on specific bad state actors will have diplomatic consequences. Certain

**The most prominent obstacles to a strong countering proliferation finance regime originate in a fundamental lack of political will.**

governments have interagency coordination challenges that the highest-level political authorities are not invested in solving. Also, some countries may believe that proliferation finance is a low priority threat, or that proliferation is better addressed through controls on equipment and materials, rather than on related financial transactions. Only stronger political will can overcome the obstacles to a stronger regime.

Proliferation finance experts, as well as representatives of banks and even regulators themselves, have spoken about the need to change legal and regulatory mindsets from a largely rules-based approach to a risk-based one. The hallmark of a rules-based approach is compliance with the letter of the law regarding measures such as the

*Cities and provinces in Northeast China create a strong economic conduit between China and North Korea. In Dandong, pictured here, a single company transacted more than $500 million worth of business with North Korea. This situation is replicated throughout the city and neighboring provinces. (Kevin Frayer/Getty Images)*

implementation and enforcement of targeted financial sanctions on designated entities. Conversely, a risk-based approach takes a much wider aperture to scrutiny of, in the case of proliferation finance, financial activities undertaken by corporate entities or individuals. A risk-based approach also includes greater surveillance of activity, focused on how account holders conduct their business and structure their transactions, and on who their counterparties are and where they operate.

For a risk-based approach to be implemented, the political and policy community must embrace a much more aggressive posture. The current limited attitude to the issue is an obstacle to better rules, coordinated agency action, measures within and across jurisdictions, and resourcing. It is also an obstacle to basic acknowledgment and coordination among the many constituencies that touch this issue, including nonproliferation, security and defense, financial oversight, and global trade communities. The academic and think tank community has researched the nature of these problems intensely, with numerous studies prominent in the field.[66] Experts have outlined gaps in the regime. It is now up to leaders in national and international forums to translate those ideas into policy. The next two subsections address these political will questions, first within the context of policy decision-making in the United States, and then in the wider international context.

Among the initial challenges for countering proliferation finance regimes in many countries is the overall lack of knowledge about what proliferation finance is and how the specific networks operate in various regions. Often, both the financial institutions and their government regulators lack relevant knowledge of typologies and red flags. More than one representative from a global bank told this report's research team that they felt they were safe from illicit finance originating from North Korea because their customers did not trade with North Korean companies.[67] This is a dangerously restrictive conception of the risk of exposure for financial institutions, because it misses activity that is illegal but would not be captured by sanctions screening alone.

**Often, both financial institutions and their government regulators lack relevant knowledge of typologies and red flags.**

Just as often, financial institutions know that proliferation finance is a risk, but they lack guidance from regulators about their national and international legal obligations to combat it, how national laws can empower banks to address the threat, and how they can coordinate efforts with other banks in their jurisdiction.[68] Often such an approach exists because national governments and international bodies do not provide adequate guidance themselves. National authorities have often failed to

convey the seriousness of countering proliferation finance as a policy objective, at either the political or the regulatory level. Many banks have uncovered proliferation networks thanks to information about typologies and red flags provided by national governments – however, not every government is proactive or shares enough to clarify the scope of more than one node in a network.

Why do such obstacles exist? Certainly size is not an obstacle: Jersey (in 2011) and the Bahamas (in 2018) have published very respectable guidance on proliferation finance.[69] Many national governments fear that regulatory scrutiny would scare away large classes of customers, and thus do not want to sacrifice their lucrative financial services sectors.[70] Others believe privacy regulations bar them from sharing the kind of information that makes a strong countering proliferation finance regime work.[71]

Virtually all banks in all jurisdictions told this research team that they understood well their legal obligation to file suspicious activity reports. If a U.S. bank believes an account holder is conducting a transaction that is unusual or indicates possible fraud, money laundering, or other illegal activity, it must file a SAR with the U.S. Department of the Treasury's FinCEN, as mandated by the Bank Secrecy Act. Banks in other jurisdictions report SARs to their national authorities, often the financial intelligence units. However, those bankers told this research team that they received neither feedback on whether their reports had been useful to law enforcement, nor guidance on what kind of reporting to regulators would align with highest national priorities for combating financial crime or security threats. As a recent Clearing House report argued:

> As financial institutions have been incentivized by regulatory enforcement actions to file increasing numbers of suspicious activity reports (SARs), a declining percentage provide value to law enforcement. Yet those regulators examining banks for AML compliance continue to emphasize the importance of financial institutions developing carefully crafted, highly detailed SARs, with little to no feedback provide on such submissions, either from themselves or those government authorities who utilize the data.[72]

A much more systemic problem is the extent to which different legal regimes create regulatory islands where information-sharing mechanisms are restrictive. Because individual banks are subject to the laws of the country in which they operate, they often cannot share relevant information about customers with other offices in other jurisdictions but within the same bank. These restrictions make it difficult for large multinational banks to track customer behavior and accounts across multiple nodes in a global supply chain. Realistically, and as extensively documented by open-source investigators such as the Center for Advanced Defense Studies (C4ADS), proliferation networks are global and span multiple institutions and countries, and they involve multiple people.[73]

A culture of restrictions on data sharing out of fear of losing a competitive edge, or of exposure to legal risk, or because of privacy concerns, is an obstacle to the countering proliferation finance regime. Numerous bank compliance officers cited strict privacy regulations as an obstacle to better information sharing on proliferation finance red flags and typologies. This trend is continuing with the European Union's introduction of the Global Data Protection Regulation, which makes it much more difficult for banks to share information.[74] While privacy protections are of course important, they must not become an insuperable obstacle to keep malign actors out of the global financial system. There is a real tension between privacy and the economic interests of the global trade and financial services sector on the one hand, and on the other the interests of the international community in preventing a catastrophic use of a weapon of mass destruction. Proliferation networks count on those gaps to procure dangerous capabilities without having to worry about strict scrutiny or aggressive law enforcement action until they have acquired what they need.

Improving these political will problems becomes more urgent as the nature of global financial systems changes in response to technological changes. The United States and its partners must be well positioned to anticipate changes in financial technology that can impact the utility of crimes investigation and sanctions compliance. While some financial technology innovations, such as distributed ledger technology, may make it easier to increase transparency in payments, others, for example virtual currencies, can make anonymity easier. The rise of peer-to-peer payments in particular presents obstacles to transparency and to the reach of U.S. jurisdiction. To the extent that the United States sits in the loop of global payments that take place in dollars, it can wield its legal jurisdiction to enforce sanctions or other currency-linked controls on proliferation finance.

### Political Challenges to Countering Proliferation Finance in the United States

In the United States, even as executive agencies may acknowledge the proliferation finance threat, this theme is broadly absent from the foreign policy approach to the most significant illicit nuclear challenges. The Departments of State, Commerce, Homeland Security, and Justice, and the 17 members of the intelligence community touch on issues involved in tracking proliferation finance. However, they all see different pieces, which makes coordination difficult. As a result, highest-level analytical work to identify and fill gaps and set related policy priorities for national attention is a challenge.

The government role is important because financial institutions ultimately build their crimes compliance strengths around what national authorities incentivize through legal requirements and formal and informal guidance. Proliferation finance is distinct from money laundering or terrorist financing because its indicators – how the money trail winds its way through global banks, what kind of account holders are involved – are different, leaving banks at a decisive disadvantage. Often the transactions underlying a proliferation finance effort look extremely similar to legitimate commerce undertaken by respectable trading firms. Financial criminals often hide behind constantly changing aliases and move money between jurisdictions and currencies, taking advantage of anonymous companies. In practice, a focus on checking a sanctions list for named proliferators only turns up nodes, including long-defunct nodes of proliferation networks rather than current activity.

To robustly track proliferation activities, banks and firms of all sizes must augment sanctions compliance with customer due diligence, transaction monitoring, and network and pattern analysis strategies to ensure that account holders comply with national and international laws. Many of the largest, most well-resourced banks are already doing this, but even they struggle, which is why banks must also collaborate closely with national regulators to share, with appropriate safeguards, information on proliferation networks. The biggest banks actively engage in these activities already, but they may struggle to work collaboratively with other banks, and smaller banks do not have the resources to implement broad programs for countering proliferation finance. Many of these shortcomings can best be addressed by policymakers setting the correct legal and regulatory framework, which is ultimately a function of exercising political will.

#### *Case Study: The Anonymous Company Problem in the United States*

There are several significant technical impediments to building out the legal framework for countering proliferation finance efforts in the United States. The legislative changes to do so are not complicated, but they have foundered amidst political differences. For example, the United States has very minimal standards for disclosure of beneficial ownership in the corporate formation process, which means that the country has a major problem with anonymous companies. Among these it is extremely difficult to trace who ultimately controls and benefits from corporate entities. While incorporation is a legitimate business practice, it is also often used to avoid income tax, park overseas money inside the United States, and launder dirty money.

In this legal framework, proliferation networks can create a string of limited liability corporations conducting legitimate business, only to turn around and use that business track record as a cover for procuring sensitive proliferation-related goods. Know Your Customer procedures and customer due diligence practices, which are vital tools to uncover illicit financial activities and networks, and on which there has been important policy advancement during the past few years, are nevertheless impaired if regulators and law enforcement do not have strong transparency around beneficial ownership.[75]

The lack of progress in ending the problem of anonymous companies in the United States is an important case study that illustrates weak U.S. political will to address illicit finance problems, including proliferation finance. There are several reasons for this. First, the existing situation underscores that while the United States is in many regards a leader on countering proliferation finance, including through its legal framework, technical capacity, and willingness to push an aggressive policy agenda in international fora, the nation still has significant vulnerabilities of its own. It is notable that despite the damage and risk that FATF can deliver to jurisdictions when it discloses their deficiencies, a finding of "non-compliant" in its most recent review of the U.S. approach to transparency and beneficial ownership did not motivate the United States to embrace policy change.[76] Nor does it seem to weigh on the minds of U.S. policymakers that close allies such as Australia and the European Union, have established requirements in pursuit of clear financial crimes compliance priorities.[77] The EU, for example, is intent on building upon its strong beneficial ownership requirements through its Fifth Money Laundering Directive, which requires members to make beneficial ownership registers public.[78]

Arguments advanced by business interests about the overburdensome cost of compliance with beneficial ownership reform are the primary impediment to advancing new laws in this area and stamping out corporate anonymity.[79] These include concern that the penalties for incorrect or incomplete disclosure would be onerous, especially when other government agencies, for instance the IRS and the Securities and Exchange Commission (SEC), collect information on corporations already. Unfortunately for U.S. national security or efforts to effectively combat criminal financial activity, these cost concerns appear to be more salient to policymakers. Both law enforcement and banking communities have spoken out about the need for remedial action on financial transparency. M. Kendall Day, when he was Acting Deputy Assistant Attorney General for the U.S. Department of Justice's Criminal Division, testified to the U.S. Senate that "the pervasive use of front companies, shell companies, nominees, or other means to conceal the true beneficial owners of assets is one of the greatest loopholes in this country's AML regime."[80]

**The lack of progress in ending the problem of anonymous companies in the United States is an important case study that illustrates weak U.S. political will to address illicit finance problems.**

The problem is not restricted to the anti–money laundering space. The same typologies appear in proliferation finance cases. Foreign-based front companies, either started entirely from scratch or repurposed from already existing entities, where the nature of the business activity switches from legitimate to illegitimate, figured in proliferation cases from North Korea, Syria, Iran, and Pakistan.[81] In one of the most infamous recent "serial proliferator" cases, Chinese national Li Fang Wei (also known as Karl Lee) repeatedly created companies to conduct procurement activity, even as his entities were sanctioned by the United States.[82]

Similar activity has been high-profile news with entities located and operating in the United States. Despite the fact that Iran has for decades been the subject of U.S. primary and secondary sanctions, Iranian entities have been successful in penetrating the U.S. financial system. From 2008 to 2013, U.S. authorities targeted front companies acting on behalf of the Iranian Bank Melli, which, through two shell companies, owned an office tower in New York City for nearly two decades. Through a complex structuring of payments, the building acted as an important revenue stream for the country's nuclear program prior to the Iranian nuclear agreement.[83]

A legal remedy for this company anonymity vulnerability would be quite straightforward. FATF stated the problem for the United States: "Beyond [a SEC requirement for entities that issue securities] there is no requirement for other companies or company registries to obtain and hold up-to-date information on their [beneficial owner] or to take reasonable measures to do so."[84] Congress is the body capable of fixing this problem. Legislators have raised the issue in every Congress since 2008, but there is still a lack of political will to pass the legislation, as most attempts have been left to languish in committee. Former Senator Carl Levin and Representative Carolyn Maloney began introducing the Incorporation Transparency and Law Enforcement Assistance Act in 2008; however, efforts to pass that legislation stopped after Senator Levin retired in 2015. Since then, Representative Maloney and Senator Wyden have introduced the Corporate Transparency Act of 2017, and Senator Whitehouse has introduced the True Incorporation Transparency for Law Enforcement Act, or the TITLE Act. Within the past year, the Senate Banking Committee and the House Financial Services Committee have considered this issue, hearing from industry, independent experts, and government witnesses.[85]


*Former U.S. Senator Carl Levin (D-MI) and others have unsuccessfully pushed for legislation to require collection and disclosure of beneficial ownership information in the corporate formation process. (Win McNamee/Getty Images)*

The counterarguments to stronger requirements around the burdens of beneficial ownership reporting are understandable concerns, however they are overstated and can be spurious. Small and medium-size companies generally do not have a complicated ownership structure, and the burden of filling out one form to disclose it would not be significant. At present, companies shoulder the costs of trying to manage their vulnerability to being abused by criminals, including proliferators, but have limited guidance or benchmarks from authorities. A fairer policy approach would be to make clear beneficial ownership requirements for all companies, thereby more evenly distributing the costs that are already borne by many companies in the economy. The United States could be a leader and model for other nations to adopt similar preventative measures, insulating themselves from risky financial behavior and national security threats.

#### AN INCOMPLETE, INADEQUATELY ENFORCED GLOBAL REGIME

The question of political will and inadequate prioritization and enforcement is at least as paramount for the international community as it is for the United States. As referenced in the previous sections on legal framework, the international legal architecture begins with the United Nations with respect to formal legal requirements, and with FATF as regards what could be called "soft law" (requirements that have political, economic, and diplomatic consequences if they are not met adequately). However, a lack of political will has continually stymied international efforts. In one example, FATF member states cannot agree on an official definition of proliferation finance, because too many member states thought an official definition would compel restrictions on legitimate commerce.[86] The lack of a universal definition underscores the weak foundation upon which countering proliferation finance efforts rests.

Just as frequently, the gap between the capabilities and motivation of the private and public sectors to address this issue can be quite wide. While U.S. banks are required to have a risk-based program to detect and halt the financing of proliferation, there is no regulatory incentive to actively detect such activity. In most jurisdictions internationally, banks are not practically required to even have a risk-based approach to tracking proliferation finance. This leads most global banks to the inevitable cost-benefit decision to do only what is necessary to follow the law: check their record to ensure that they are not doing business with anyone on U.S. or U.N. sanctions lists.

These concerns are particularly acute for high-risk jurisdictions, where banks and regulators do not have the level of resources or political will that the United States and Western Europe have. Many bank compliance and government regulators highlight deficiencies in the regime, often because the transnational nature of proliferation networks means that the regime as a whole

**The lack of a universal definition underscores the weak foundation upon which countering proliferation finance efforts rests.**

is only as strong as its weakest member.[87] The irony of the situation is that with increasing attention being paid by U.S. regulators to the problems of correspondent banking, many banks around the world are being forced by their U.S. correspondents to adopt U.S. banking standards. If U.S. regulators required U.S. banks to specifically seek out proliferation financing, the mandate would be passed on to correspondent banks overseas, effectively strengthening the international countering proliferation financing regime.

To be clear, the public policy implication of this is that banks and companies around the world have virtually no incentives from their national authorities to actually seek out proliferation activities and halt them. Only some institutions have the sophisticated analytical capacities to shut down one of the gravest global security threats, and are properly incentivized to so. Often they do so because they have correspondent banking relationships with financial jurisdictions that have much stronger rules, and their correspondent banks require this of them. Others, however, lack resources and technical capacity, and their national authorities have not identified or put into place the correct incentives. In fact, because of the lack of safe harbor provisions in many jurisdictions, they may be penalized if they do turn up indications that they are being abused by proliferators, while they fail to see the entire value chain, or repeated incidences.[88]

Adding to this dynamic, some governments avoid applying strict scrutiny for diplomatic or political reasons.[89] The Russian Federation, for example, has sought to alleviate severe worker shortages by authorizing North Korean laborers to operate inside the country. While recent United Nations Security Council Resolutions 2375 and 2397 are meant to actively curtail this activity, there is no sign that Russia is slowing down. As recounted in a C4ADS report on North Korean

overseas labor, in July 2018, Russian President Vladimir Putin announced that the permits would be extended, despite a Chapter VII Security Council Resolution (Operative Paragraph [OP] 8 of resolution 2397 [2017]) that such activity should be curtailed.[90]

*Case Study: China's Enabling of North Korean Proliferation Finance*

Despite purported policy concerns related to nuclear proliferation and repeated requests from the United States and other international actors, China has not been forceful in combating proliferation finance. This is particularly concerning because China facilitates the overwhelming majority of North Korean trade and commerce and therefore has a major role in enabling North Korean proliferation. Prior U.S. administrations have publicly expressed the importance of China's place in convincing North Korea to denuclearize, with former Secretary of State John Kerry saying that China could play a "special role" in making the dream of a denuclearized North Korea become reality. The Trump administration has offered many of the same sentiments, asking China to do more to curb North Korea. But frustration that China seems to shield North Korea from punitive measures, perceived as largely due to its own self-interests, obscures the complex way in which China judges its interests and gauges its ability to control lower-level officials in provinces bordering North Korea.[91]

In China, trade with North Korea is an important source of revenue for the neighboring province of Liaoning, where the city of Dandong is located. This is why so many Dandong-based companies have conducted trade with North Korea, thereby violating international sanctions. Among those that have been identified, Dandong Hongxiang Industrial Development Company (DHID), which was sanctioned by the United States in September 2016, transacted more than $500 million worth of business with North Korea.[92] This kind of firm-level commercial activity is replicated in Dandong and throughout Liaoning and the neighboring province of Jilin, as demonstrated by the multiple Chinese businesses that remained open in defiance of recent U.N. Security Council Resolutions and as reported in the *South China Morning Post*.[93] Dandong relies on trade with the Kim regime for 40 percent of its total trade.[94]

It is clear that the most prominent reason for robust commercial activity with North Korea – in violation of sanctions and of Beijing's own purported interest in limiting North Korea's nuclear ambitions – is the economic impetus for provincial officials to generate growth. These officials must achieve growth targets that the central government sets. In order to meet them, provincial and city governments inflate growth numbers, degrade the environment, or, in the case of Dandong, exploit the lucrative and suspect trade with North Korea. In one example of this kind of trade, between 2013 and 2016, a single company, Dandong Dongyuan Industrial Co. Ltd., was able to export in excess of $28 million worth of materials to North Korea, including motor vehicles, electrical machinery, radio navigational components, and other items associated with nuclear reactors.[95] For context, North Korea's total imports were $3.71 billion in 2016, of which 92 percent came from China.[96] While some local government officials may not be fully aware of their enforcement obligations, resulting in uneven implementation of sanctions while achieving their growth targets, in other cases corrupt local officials are happy to pocket the profits of trading with North Korea. Since Xi Jinping came to power in 2013, the Central Commission for Discipline Inspection, the Chinese Communist Party's anti-graft body, has reportedly investigated more than 2.6 million officials and punished more than 1.5 million, including the former vice governor of Liaoning.[97]

China's continued trade with North Korea is also supported by its need to source carbon-intensive energy from outside its borders in order to meet domestic environmental goals. Transportation costs from North Korea are not high, and the coal itself is cheap to import. Starting in 2016, China made combating pollution,

**Dandong, a Chinese border city with North Korea, relies on trade with North Korea for 40 percent of its total trade.**

especially in the air, a clear priority. Chinese Premier Li Keqiang said in his 2016 *Report on the Work of the Government* that polluters and those who failed to report environmental violations would be "severely punished."[98] In accordance with the Environmental Protection Law, which was passed in 2014, and the environmental standards set out in the 13th Five-Year Plan, China canceled the construction of 103 coal power plants in 2017 alone, reduced the number of working days annually from 330 to 276, and cut up to 1 billion tons of coal production capacity within the next three to five years. These capacity cuts led to China reaching domestic demand for coal through imports – in 2016, China imported 22.5 million tons of coal from North Korea, almost 9 percent of China's total coal imports for that year.

*A North Korean restaurant worker tries to attract customers in the Chinese border city of Dandong. The United States has sanctioned restaurants that employ North Korean laborers, because these establishments have often been found to be acting as fronts for other North Korean companies to support the development of North Korea's nuclear program. (Kevin Frayer/Getty Images)*

For China, looking the other way on trade with North Korea also offers diplomatic dividends. While China has interests in avoiding an armed nuclear confrontation on its border, it also has national interests that prevent it from completely severing commerce with its neighbor. China does not want to see a refugee exodus into its own territory from North Korea. Allowing revenue streams to Pyongyang is a form of insurance that the North Korean regime and state structure will not collapse under severe financial duress, sending citizens fleeing beyond its borders for aid and services. Regime collapse or compromise would also undercut China's clear and longstanding desire to have a substantial physical buffer between China and Western military forces stationed in South Korea. In the instance that North Korea should collapse, or should unify with South Korea, the U.S. alliance presence in South Korea would presumably spread north to China's borders.

The diplomatic dividends extend beyond bilateral relations to the larger international community; trade flows that fund North Korea's nuclear program give China increased leverage as it negotiates with other countries. When China cracked down on illicit border trade at the end of 2017, it harmed the North Korean economy, with exports declining 37 percent. Due to the increased economic pressure from China, as well as additional sanctions pressures and new summit diplomacy with the United States and South Korea, North Korea has yet to conduct further tests of any weapons of mass destruction or their delivery systems.[99] The outsized control that China has over North Korea's economy, and through that on the scope of its nuclear program, also leads China to try to extract concessions from outside actors such as the United States who would like to see North Korea's nuclear program removed. For example, as tensions between the United States and China escalate on the economic front, White House officials have said that formal talks between the two countries on North Korea's denuclearization process have languished. This demonstrates that China has linked trade with the United States to North Korean denuclearization, refusing to use its leverage to stop North Korea from cheating on sanctions.[100]

Factors such as these will always limit the ability of China to exert economic leverage over North Korea. Even after a decade of international and U.S. financial controls on North Korea and 50 years of arms control agreements and treaties, on top of a regime of nuclear-related trade controls and intensive diplomacy dating back to 1993, years passed without China doing more to combat North Korean proliferation. The United States is in a position to take measures such as unilateral sanctions to hold other countries to account for blatantly abetting Pyongyang, but it has not, until recently, called out China for such activity. Even now, there is far more Washington could do to demand full disclosure of and create consequences for Chinese facilitation of North Korean proliferation activities.

**For China, looking the other way on trade with North Korea also offers diplomatic dividends.**

These trends are worth watching as the country's economic strength continues to grow. China helped develop Pakistan's nuclear and missile programs, and exported sensitive technologies and materials to countries such as Iran, Libya, North Korea, and Saudi Arabia.[101] If China decides to increase exports to the Middle East, it will use rail linkages through Belt and Road Initiative recipient countries in Central Asia, as many of them house WMD materials. Additionally, the

region is a possible transit node for parts and materials that originate elsewhere, due to the perception that its export and border control systems are inadequate for tracking and controlling the movement of parts across borders.[102] While proliferation finance networks have traditionally turned to manufacturers in the United States and Western Europe for their high quality manufacturers, the domestic upgrade of the Chinese defense industry could lead to other nations looking to Chinese manufacturers. This may implicate more Chinese firms in future proliferation efforts.

More generally, political leaders across the world have been and continue to be willfully blind to the enormous impact of a potential nuclear incident and their complicity in enabling this. Like China, they may have domestic economic self-interests that are more salient to political officials than North Korea's denuclearization. Such self-interests may similarly cause them to actually abet and indirectly and directly support North Korea. Proliferation finance and facilitation of North Korean sanctions circumvention is not just a regional problem – it touches upon every other continent, including Africa.

*Case Study: An Illicit Economic Relationship between Ethiopia and North Korea*

North Korea and many countries in the Horn of Africa and elsewhere in Africa have economic relationships that date back to the latter decades of the Cold War. North Korea's role as a cheap source of military goods fueled conflicts in the region during the 1970s, but also cemented bilateral relationships that have persisted through Pyongyang's most recent international ostracism.[103] This includes defense relationships with countries such as Ethiopia, where the


*During Xi's visit to the Middle East in July 2018, China upgraded its relationship with the Middle East to a "strategic partnership." China has a pattern of supporting the development of Middle Eastern countries' domestic nuclear and WMD programs. (Whang Zhao/ Getty Images)*

partnership has also extended into other sectors, for example construction. Successive United Nations Panel of Experts reports, as well as press coverage, have documented a mutually beneficial economic relationship.[104]

Ethiopia helps provide North Korea with essential revenue, much of which goes to its military, supporting weapons of mass destruction research and development through purchasing DPRK goods and acting as a conduit between North Korea and other African countries. The 1718 Sanctions Committee's (DPRK) 2017 annual report revealed a July 2016 interception of an air shipment of 45 boxes of military radio communications products and accessories from China to Ethiopia. Some of these products were labeled as being produced by Glocom, the Global Communications Company. The panel determined

**Successive United Nations Panel of Experts reports, as well as press coverage, have documented a mutually beneficial economic relationship between Ethiopia and North Korea.**

that while Glocom is based in Malaysia, it is actually a front company for the North Korean company Pan Systems Pyongyang Branch, which finances the North Korean WMD program.[105]

Ethiopia also commissioned Mansudae Overseas Project Group of Companies to build the Tiglachin Monument, which honors Ethiopian and Cuban soldiers who fought in the Ogaden War.[106] Mansudae is sanctioned by the U.S. Treasury Department and the United Nations for engaging in or facilitating the exportation of North Korean workers to generate revenue for North Korea, whose Munitions Industry Department uses part of the revenue to support North Korea's WMD program. Ethiopian Airlines, which is state-owned, has also been reported to have helped transport arms-related materials from North Korea to the Republic of the Congo, thereby violating U.N. sanctions.[107] These willful violations arise in part because countries like Ethiopia find North Korea to be a reliable, low-cost partner, particularly in the defense sector.[108]

Aside from the positive financial incentives to work with North Korea, another problem is that Ethiopia lacks the infrastructure and the political will to implement a legal framework or procedures related to proliferation financing. When FATF evaluated Ethiopia in 2015, it said that it had "not established a legal framework for

the implementation of targeted financial sanctions relating to the financing of proliferation," and rated it non-compliant with Recommendation 7 for this reason: Ethiopia had nothing in place "to comply with UNSCRs relat[ed] to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing."[110] In the same report, FATF noted that it was "unlikely" that Ethiopia was used as a jurisdiction to support proliferation activities outside of the country. As evidenced by these examples, Ethiopia is a nexus for sanctions evasion by North Korea, which should be

**These willful violations arise in part because countries like Ethiopia find North Korea to be a reliable, low-cost partner, particularly in the defense sector.**

a much more significant concern for the international community. Since 15 percent of the Kim regime's overall state budget is dedicated to military spending and only 26 percent of the state budget comes from domestic sources, international policymakers should assume that revenue raised overseas is going to support defense-related or proliferation-linked projects.[110]

Since the release of FATF's Mutual Evaluation Review of Ethiopia in 2015, that country remains on FATF's list of jurisdictions with strategic deficiencies.[111] While Ethiopia made a commitment to work with FATF, it has yet to establish or implement any targeted financial sanctions related to the financing of proliferation programs. However, the calculation behind Ethiopia's relations with North Korea is changing slowly. It has responded to the increased United Nations action by closing the bank accounts of many North Korean diplomats.[112] The United States can reinforce this strengthening of will through its leadership at FATF, as well as bilaterally by discussing with Addis Ababa technical deficiencies.

*Case Study: Letting Pakistan off the Hook on Proliferation Finance*

Several countries, including Pakistan, often slip under the radar of international efforts to find and halt proliferation finance. This is primarily because they are not currently subject to multilateral or even unilateral sanctions programs. The situation is ironic, given that Pakistan's A. Q. Khan helped create Pakistan's nuclear program and subsequently an entire network. This network spanned the United Kingdom, the Netherlands, Italy, Spain, Switzerland, Turkey, South Africa, the United Arab Emirates, Malaysia, Singapore, and South Korea, and supplied countries such as Iran, North Korea, and Libya with the parts and know-how needed to create domestic nuclear weapons programs. A decade and a half after A. Q. Khan confessed to illegally proliferating nuclear technology, Pakistani proliferation networks still operate. In 2014, the United States charged three individuals and two corporations with smuggling dual-use technologies to the Pakistan Atomic Energy Commission, which is an arm of the Pakistani military.[113]

In 2010, two other individuals in the United States were charged with exporting dual-use technology that could be used in nuclear weapons technology, including dosimeters, nuclear grade resins, and series 20M selector switches.[114] The technology eventually ended up in the hands of Pakistan's Space and Upper Atmosphere Research Commission, the Pakistan Atomic Energy Commission, Chashma Nuclear Power Plant, and the Pakistan Institute of Engineering and Applied Sciences, all entities instrumental to Pakistan's development of nuclear weapons.

Because Pakistan is not linked to a major country sanctions program, the international community and domestic political actors commonly overlook these transactions, due to a lack of political will and a lack of practical controls or a larger proliferation finance detection network. In 1979, President Jimmy Carter cut off all economic and military aid to Pakistan because of the development of nuclear weapons, using Section 101 of the Arms Export Control Act, which prohibits the United States from giving economic and military assistance to any country that the president determines is delivering or receiving nuclear equipment, materials, or technology.[115] However, in order to support the guerrillas in the Soviet-Afghan War, Carter lifted the sanctions, allowing Pakistan to expand its nuclear capabilities.

More recently, 11 days after 9/11, President George W. Bush officially lifted the sanctions that were reim-

**Pakistan's A. Q. Khan helped create Pakistan's nuclear program and subsequently an entire network.**

posed on Pakistan after its 1998 nuclear test, in order "to cooperate more easily with Pakistan in the fight against terrorism."[116] Other outside actors such as China also help reduce the incentives for Pakistan to better implement its own illicit financing laws. On June 28, 2018, Pakistan was put back on FATF's list of jurisdictions


*Members of Pakistan's Ministry of Defense and high-level military officials reveal a Pakistan-made, short-range, nuclear-capable missile. Pakistan's A. Q. Khan not only helped create that country's nuclear program, he also supplied countries including Iran, North Korea, and Libya with the parts and know-how to create domestic nuclear weapons programs. (Pakistan Ministry of Defense/Getty Images)*

with strategic deficiencies, which makes it harder for that country to borrow money from others to pay back its debt and deters other countries and international companies from investing in Pakistan.[117] While China did not oppose the motions to put Pakistan back on the list, two days after FATF's announcement, China gave Pakistan a $1 billion loan to help boost its foreign currency reserves.[118] Since then, the U.S. Department of State has said that Pakistan's implementation of terrorist financing through its Anti-terrorism Act of 1997 remains uneven, and the FATF assessment delegation is reportedly unimpressed with Pakistan's progress.[119]

Both international and domestic actors also seem to look past proliferation finance as long as nuclear weapons do not fall into the hands of terrorists. A. Q. Khan was forced to confess on live television in 2004 to finance proliferation, yet is now a free citizen protected by the Pakistani government from being questioned by foreign investigators. He was allowed to recant his confession and is widely known as the "Mohsin e-Pakistan," the savior of Pakistan.[120]

Resolution 1540 (2004), intended to keep WMD and their means of delivery out of the hands of non-state actors, was adopted unanimously by the Security Council in the aftermath of the A. Q. Khan affair. But the resolution focuses on equipment and materials, and requirements related to financing are relatively few. The resolution nevertheless underpins the current international countering proliferation financial regime framework, in its nascent form. But this framework, which includes U.N. sanctions on DPRK and Iran, largely misses Pakistan, as well as other major nuclear-enrichment programs in countries not targeted by the United States with high-priority diplomatic and economic measures, such as Iran and North Korea. Independent organizations, for example the Arms Control Association, say that Pakistan is "expanding its nuclear arsenal faster than any other country," yet it has largely avoided international pressure on nuclear proliferation.[121] Despite this assessment, not only has Pakistan avoided scrutiny from the United Nations, it now offers help to others under the

**Both international and domestic actors also seem to look past proliferation finance as long as nuclear weapons do not fall into the hands of terrorists.**

International Atomic Energy Agency's (IAEA) Technical Assistance and Technical Cooperation programs.[122] The only way that the international community can pressure Pakistan's, India's, or Syria's WMD programs is by unilateral sanctions (in the case of Syria) or export controls (for Pakistan and to a lesser extent India).

The case studies of the United States, China, Ethiopia, and Pakistan demonstrate that the problem of proliferation finance, particularly how political will undermines more aggressive action, impacts developed and developing countries alike, and countries with both weak and strong legal infrastructures. Having identified the scale and scope of the problem, the next section offers a roadmap for policymakers to address deficiencies in countering proliferation finance.

## What Do We Do About It? Policy Recommendations

There are no insurmountable obstacles facing the United States in its efforts to lead on strengthening the countering proliferation finance regime. Both Congress and the executive branch broadly agree on the extent to which countering weapons of mass destruction proliferation fits into wider U.S. national security priorities. They also both see a high degree of utility in using financial measures as tools of coercion against U.S. adversaries, as evidenced by the bipartisan consensus on the use of targeted financial sanctions. The United States and its partners have compelling reasons for strengthening the focus of countering proliferation finance work. Additional steps they can take include extending regulatory controls to industries such as shipping and insurance, or grappling with the impact that new technology (virtual currency, machine learning) will have on financial crimes compliance. These steps require additional resources – often a barrier to adoption – but the short- and long-term benefits of aggressive action far outweigh the immediate costs.

More aggressive U.S. leadership is important to strengthening the regime for several reasons. The first is that the U.S. dollar is still the preferred currency for international trade, and the U.S. financial sector is still an attractive partner for international businesses. This is because of its mature equity and debt markets, the easy convertibility of the U.S. dollar, and the strong and relatively predictable nature of its legal and regulatory system. As a result, international private sector firms are highly disincentivized to run afoul of U.S. law enforcement and regulators.

Second, U.S. law enforcement and regulators are very well resourced and invested in providing technical assistance to U.S. partners where appropriate. The United States can work directly to improve the global nonproliferation regime at a time when it is involved in controversial and high-stakes diplomatic engagement surrounding Iran's and North Korea's nuclear capabilities.

A third reason for the United States to take a strong lead on countering proliferation finance is that even if other countries do not welcome U.S. leadership in this space, the United States is nevertheless uniquely well placed to apply pressure to comply with international obligations and to offer support in doing so. The resources and operational capacity of the United States can compel others to lead politically, and the pressure of running afoul of U.S. authorities can change the calculus for other countries, convincing them that fighting proliferation networks is in their national interest. The U.S. administration has used this leverage in other instances, as well as its considerable technical assistance resources, and this outlook should be developed further in the proliferation space.

The following policy recommendations outline steps that the U.S. government and the private sector can take to address the political will and prioritization needed to better recognize and combat proliferation finance. These recommendations also account for the capacity challenges laid out in this paper. Adopting these measures in part or in whole will put the United States in a much stronger position of leadership to advance the global counterproliferation community and national security for the United States and its allies.

### Raise Awareness, Educate

The basic building block of a strong countering proliferation finance regime is ensuring that all relevant stakeholders are aware of what it is, why it presents such a dire risk to international peace and security, and what policies private and public sector actors can be taking to address it.

1. The Trump administration should raise awareness of and expand the expertise of the U.S. policy and intelligence community in countering proliferation finance. To that end, the president should direct the creation and publication (in unclassified form) of a U.S. National Intelligence Estimate (NIE) on proliferation finance. Such an NIE will draw widespread attention to the complex nature of the threat and underscore how different state actors, for example North Korea, Iran, and Syria, often collaborate to spread goods and know-how to advance weapons of mass destruction programs.
2. As part of that awareness raising and education effort, FinCEN should regularly release public and private advisories on proliferation finance typologies so that international financial institutions understand how these networks change their operations over time.
3. The Treasury Department should emphasize in any future guidance on proliferation finance that a rules-based, list-checking, sanctions-only approach is inadequate. Despite progress to date, far too many financial jurisdictions and institutions around the world still consider themselves in fulfillment of their regulatory obligations by taking a rules-based approach to countering illicit finance, including

proliferation finance. Foreign policy leaders and international financial institutions pay attention to statements from the U.S. Treasury Department, and they will note the emphasis on a more intensive risk-based approach to countering the financing of proliferation. U.S. banks should similarly ensure that their overseas respondents are adopting such policies toward proliferation finance.

4. The administration, particularly the Treasury Department, should partner with outside groups, and further refine its approach to public-private partnerships in order to raise awareness and further expand information-sharing efforts. A strong and growing open-source community is building knowledge about proliferation finance. Many private institutions, including think tanks, academia, and for-profit analytical firms, understand and support using financial and economic policy and tools for analysis and policy advancement on counterproliferation issues. The Trump administration can buttress these efforts by identifying opportunities to expand public-private partnerships. The Treasury Department, including FinCEN, should consider convening a formal outside advisory group to explore additional strategies for improving information sharing. These efforts could include strategies to gather and share data relevant to civil asset forfeiture, 314(b) information sharing between financial institutions, and data from demand letters. Legislation is currently pending in the U.S. House of Representatives that would provide safe harbor for nonprofit organizations to share information with financial institutions on activities potentially indicative of money laundering and human trafficking.[123] This could serve as a model for information sharing on proliferation finance for non-bank commercial institutions such as shipping, manufacturers, and freight forwarders.

5. In addition to the open-source analytical community, the administration should enhance public understanding of the proliferation threat and the importance of countering its financing. Greater discourse and outreach to explain the issue will help to dispel notions of proliferation finance being an issue for "experts" that is of significance to few. In addition, public funding to journalism on proliferation finance for "follow the money" press work would support the kind of difficult, long-term investigations that can focus attention on the seriousness of the threat. Such support will raise awareness and help to bring this into wider public consciousness, which in turn will lead to the political will for more aggressive action. Also, it will educate the frontline bank supervisors who often rely on their news consumption to understand some of the common money laundering and financial crime threats.

### Change Policy at Home

While the United States sits at the center of the international financial system, its leadership is weakened by the gaps that regulators permit in financial oversight. The relative openness of the U.S. financial sector is a source of economic strength, but it should not obscure the grave difficulties that these gaps present to countering proliferation finance. To reduce the vulnerabilities in the U.S. financial sector, the administration and Congress should do the following to specifically adapt domestic law and regulation:

1. Congress should pass legislation requiring the reporting to law enforcement of the ultimate beneficial ownership of corporate entities that are created in the United States. Doing so would provide an invaluable tool for information gathering about illicit financial actors, including proliferation networks. The existing Customer Due Diligence Rule is insufficient because it only requires certain financial institutions to collect such information, without a mandate that it be automatically transmitted to government authorities. Bills such as the Corporate Transparency Act of 2017, introduced in both the House and the Senate, and the True Incorporation Transparency for Law Enforcement Act (TITLE Act), introduced in the Senate, are examples of legislation that would establish legal requirements for accurate disclosure of beneficial owners of corporate entities. Congress must lead on this, first by passing such legislation and then by using its oversight authority to spur effective implementation by the executive branch.

2. The administration should proceed with the implementation of the Customer Due Diligence Requirements for Financial Institutions Rule, which became effective in May 2018. The rule strengthens the requirement for financial institutions to verify the identity of account holders. It requires the ongoing monitoring of customer accounts for suspicious transactions. Congress should use its oversight powers to ensure that the rule implementation proceeds broadly and expeditiously.

3. Congress should consider advancing a financial requirement to mandate the declaration of all

cross-border payments, possibly including information that would be relevant to bridging the gap between data about financial transactions and the physical shipment of potentially proliferation-related goods. As currently formulated, the Travel Rule is only for transactions above $3,000 and requires only retention, not transmittal to relevant authorities. Congress and the administration should consider the categories of information that would be feasible to incorporate in such a cross-border rule, including beneficial ownership, underlying goods, transaction participants, industry of senders and beneficiaries, and transparency about the final destination of goods for trade-specific transactions. U.S. partners Canada and Australia already operate significantly tougher Cross-Border Transfer Rules.

4. U.S. law enforcement agencies should expand their work on information sharing and public-private partnerships. This could be led by the weapons of mass destruction directorate at the FBI and Department of Homeland Security (DHS) investigations, as both agencies have taken the lead on evidence collection for past WMD proliferation prosecutions. The FBI director and the DHS secretary should make this a priority for their respective agencies. They should explore the creation of an external advisory group to pilot information sharing and, working with the Treasury Department and relevant financial regulators, safe harbor mechanisms. This effort should include shippers and manufacturers as well.

5. Executive agencies and financial regulators should explore regulatory carve-outs for innovations on countering proliferation finance. These innovations could include:

   - Major U.S. banks (and others that participate in dollar clearing through their correspondent banking relationships) investing in big data approaches to transaction monitoring and aggregating trade and financial data.
   - The federal banking agencies and state banking licensing authorities should give special recognition and dispensation to banks to train their correspondent institutions on using data to collect information on suspected proliferation finance activity.
   - The corresponding federal and state financial institution supervisory authorities should structure their exams so that financial activity that may be national security–sensitive is treated differently
   - The Financial Crimes Enforcement Network could create a dedicated supervisory team to examine for proliferation financing risk, as has been recommended previously by banking policy organizations such as the Clearing House.

6. Congress should prioritize additional funding increases on a yearly basis for the Treasury Department's Office of Terrorism and Financial Intelligence (TFI) in order to more adequately, and on an ongoing basis, provide resources for activities to counter proliferation finance. TFI is at the front line of policy innovation on countering proliferation finance. Its activities include the formulation and enforcement of all financial measures to counter weapons of mass destruction. Congress recently increased TFI funding, but the appropriation was less than what the Treasury Department had originally requested.

7. The Treasury Department should convene an interagency process to consider the development of new regulations that would require U.S. banks and the shipping, freight forwarding, and manufacturing sectors to collaboratively gather more information on the parties to, and purpose of, proliferation activities. The United States should furthermore initiate a formal process with international counterparts to push for complementary, joint compliance efforts abroad.

*The Financial Crimes Enforcement Network, whose director, Kenneth A. Blanco, is pictured here, could work with other U.S. law enforcement agencies to help combat proliferation financing through expanding information sharing and private-public partnerships. (Justin Sullivan/Getty Images)*

8. FinCEN should dedicate intensive efforts to analyze SARs for proliferation finance activities and develop refined indicators and explore opportunities for greater proactive sharing of relevant information with other proliferation-related U.S. government agencies and banks. When shared with the private sector, this information may lead to the most fruitful investigation and analysis of proliferation networks and the filing of so-called super-SARs that may be highly advantageous to law enforcement efforts.

### Lead Abroad

The United States has opportunities in both its bilateral and multilateral interactions to improve the global countering proliferation finance regime. U.S. government action is necessary to push these countries to accept a broader approach, given U.S. capacity and resources, as well as the economic and political impediments that prevent many foreign countries from undertaking concerted efforts to counter proliferation finance.

1. The Treasury Department, U.S. law enforcement agencies, and the intelligence community should launch a formal process to work with European Union jurisdictions to more formally align intelligence collection requirements, intelligence exchange, and information sharing on proliferation finance. Because proliferation finance networks desire high-quality goods for their weapons of mass destruction program, they prefer manufacturers from the United States and Western Europe, as evidenced by the purchase trail of prior procurement networks.[124] As a result, transatlantic coordination on countering proliferation finance must be a cornerstone of the wider regime. The administration should focus on identifying ideas for coping with legal and privacy impediments between the jurisdictions that have, in the past, been an obstacle to more aggressive action. While multilateral coordination is needed, the United States should be prepared to do more on its own, and with its own private sector, if the wider international community moves too slowly. This process should explore the possibility of a regulatory carve-out under the General Data Protection Regulation for anti-money laundering and proliferation finance information sharing.
2. The administration, with the Department of the Treasury in the lead, should model a proliferation finance threat cell on other financial crimes compliance data-sharing mechanisms. This could be created either as a U.S.-only or a multilateral data-sharing exercise.
3. The U.S. Treasury Department should continue to prioritize proliferation finance as part of its working agenda for its presidency of FATF. The current U.S. agenda at FATF emphasizes criminalization, expanded use of targeted financial sanctions by national authorities, and the weakness of the FATF standards for proliferation financing as compared with money laundering and terrorist financing. The United States delegation should support this work, as well as efforts by FATF to conceive of ways to gauge the feasibility of expanding this work so that it includes the following measures: encouraging the use of proliferation finance specific risk assessments, adding proliferation finance formally into the recommendations, and addressing the extent to which the shipping and insurance sectors serve as facilitators of proliferation finance. The overarching goal should be to bring FATF's approach on countering proliferation finance to the strength that both it and the United Nations demonstrate on countering terrorist financing. This should include ensuring that all nations are evaluated on the full suite of UNSCR 1540 financial requirements. The United States should ask FATF to prepare interpretive notes on United Nations obligations, including guidance on implementation of financial provisions of Resolution 1540.
4. The U.S. Treasury Department should encourage further cooperation between the high-risk jurisdictions of Hong Kong and Singapore. Both are at the front lines of proliferation finance concerns, particularly as related to North Korean networks. The United States could launch a pilot partnership with Hong Kong and Singapore so that, as a united effort, the jurisdictions could put together trade and financial data to understand the full breadth of proliferation threats and risks. These foreign jurisdictions are aware of their vulnerabilities, but they face restrictions due to legal barriers and other political and economic priorities. Such work could lead to the issuance of a series of public circulars and private advisories to banks about risks, which would help private sector actors in both jurisdictions who were eager to comply with the obligations.
5. The United States should lead the international community to develop a convention on countering proliferation finance, similar to the one that currently exists for countering terrorist financing. There are numerous opportunities for pushing for a multilateral consensus:

- Leverage the United Nations 1540 Committee expertise on countering weapons of mass destruction proliferation to focus on member states' performance on combating proliferation finance. UNSCR 1540 places very specific obligations on member states to place effective controls to prevent the proliferation of weapons of mass destruction, including on financing, but their work program to date has not included significant efforts against proliferation finance.
- Convene a major gathering of Group of 20 (G-20) finance ministers to address this topic at a forthcoming World Bank–International Monetary Fund meeting.
- Convene a major gathering of foreign ministers on the sidelines of the United Nations General Assembly to discuss how to augment capabilities and technical assistance globally.
- Put pressure on the Egmont Group, the global network of financial intelligence units, to enhance information sharing relevant to proliferation finance. These measures could include more detailed public and private advisories on proliferation finance typologies. The Egmont Group could create new information sharing mechanisms that do not violate individual member state privacy laws.


*World Bank President Jim Yong Kim listens to reporters' questions during a news conference at the IMF. Leading multilateral financial institutions such as the World Bank and the International Monetary Fund could play a role in helping to develop an international convention on countering proliferation finance. (Chip Somodevilla/ Getty Images)*

6. The U.S. Treasury and Commerce Departments should cooperate to identify which obstacles are preventing the extension to other industries and sectors in the global supply chain a consistent system of controls and regulations for countering proliferation finance. Other regulatory regimes that need to be built or strengthened include those in shipping, insurance, transhippers, and other nodes in the global supply chain. For the shipping industry in particular, there should be a requirement for the International Maritime Organization unique identifier numbers of ships to be added to bills of lading in trade transactions. Proliferation networks, particularly North Korean ones, have been adept at changing ship names after the vessels have been designated to evade scrutiny. The U.S. Treasury and Commerce Departments, in partnership with international regulators, should require that companies tracking ship transponders to immediately notify relevant authorities when those transponders are turned off mid-voyage. The incidences of transponder shut-off should inform private advisories to banks to flag which trading companies are utilizing vessels which are habitually tampering with transponder tracking.
7. The United States should work with counterpart governments to anonymize trade control violation data to issue joint advisories on proliferation threats. For example, the U.S.-U.K. Financial Regulatory Working Group, which seeks ways to deepen regulatory cooperation between the two countries, could issue joint recommendations on how to counter proliferation finance. The United States and the European Union also have a Joint Financial Regulatory Forum that regularly exchanges views on relevant developments. Both are models for developing fora to discuss emerging regulatory challenges. Regulators and law enforcement must enable global firms to link trade control violations to financial data, which are difficult for international banks to see on their own. Doing so can help motivate more data gathering, analysis, and operational activity on countering proliferation finance. Widening the aperture beyond attention to international banks can encourage an all-of-government effort to attack proliferation finance.
8. The U.S. administration should ask Congress for more resources to expand technical assistance programs run by the Departments of State (Export Control and Related Border

Security – EXBS – or the Bureau of International Security and Nonproliferation) and Defense (Defense Threat Reduction Agency). These programs enable partner countries to tighten their regulatory and legal regimes to combat proliferation finance. Their efforts are supported by a global network of FBI and Drug Enforcement Agency legal attachés serving in U.S. embassies throughout the world. Congress should provide additional targeted funding so that the administration can prioritize assistance to high-risk jurisdictions. Technical assistance should include efforts to share model laws from other jurisdictions. EXBS should be given funds to hold training overseas on countering proliferation finance. Coordination of outreach abroad is needed to ensure priorities are aligned and gaps filled.

9. Congress is currently taking steps to require the administration to create a Virtual Currency Task Force. If that is accomplished, the administration should instruct it to produce analysis on the impact of financial technology on financial crimes compliance, including its specific application to countering proliferation finance. If financial technology innovations circumvent those pathways, a countering proliferation finance regime will be harder to uphold.

10. The U.S. Treasury and its counterpart finance ministries in the European Union could explore the feasibility of expanding the amount of payment information that can be included in SWIFT messages. Current SWIFT messages do not allow for enough information to be conveyed about the underlying purpose of the transaction. Expanding the character limit for SWIFT messages, and requiring specific disclosures of the "who" and "why" of the transaction, would provide banks and law enforcement/intelligence agencies with more information about potential proliferation activity.

### Challenge Specific State Actors

In addition to the United States leading on strengthening the global regime, it should pay special attention to the intersection between proliferation finance issues and the U.S. approach to Iran and North Korea:

1. In denuclearization talks with North Korea, the United States should outline how Pyongyang's dedication to financial transparency and cessation of proliferation finance activities must be part of any sanctions-rollback framework. Additionally, the United States should take steps to address the issues that have put North Korea on FATF's black list. Ensuring that Pyongyang disassembles the proliferation networks that procured its weapons of mass destruction program will be an important confidence-building measure. It will be necessary for the administration to feel that it is depriving North Korea of a dangerous capability. Abandoning its proliferation finance activities will be the only way for the Kim regime to facilitate a credible reentry into the global economy, legitimizing much of China's trade with Pyongyang. If North Korea fails do so, it will face very difficult reputational risks, freezing reinvestment and setting it into a more adversarial relationship with the United States. The latter could encourage North Korea to submit a first report on implementation of Resolution 1540 (2004). North Korea is the most significant of 12 or so countries that have yet to submit a report.

2. Mindful of the differences in international approaches to Iran policy, the United States should work constructively with its partners on curtailing covert Iranian proliferation activities, which are a threat to the wider international community. The international community still maintains a broad consensus against Iran obtaining advanced nuclear capabilities. As concerns grow that a potential Iranian exit from the JCPOA will raise the proliferation risk emanating from that country, so too do specific fears about it operationalizing prior


*South Koreans watch U.S. President Trump meet with North Korean leader Kim Jong-un during the historic Singapore Summit. During its denuclearization talks with North Korea, the United States should ensure that the country disassembles the proliferation networks that enable its WMD program. (Chung Sung-Jun/Getty Images)*

proliferation networks, including sophisticated financial channels. The U.S. return to a maximum pressure campaign will include a comprehensive targeting of Iran's financial system. But should the United States not work on this with its partners, the JCPOA framework for inspection and verification will be undermined and political relations among the parties will be frayed. The U.S. government can build on FinCEN's October 11, 2018, advisory by regularly releasing advisories on Iranian proliferation finance concerns. Mindful of the major political disagreements among transatlantic allies about how to approach Iran issues, focusing on a CPF workstream may keep collaborators focused on common concerns.

### Lead in the Private Sector

Because private sector actors, especially financial institutions, sit at the front lines of countering proliferation finance, it is essential that they invest in building their subject matter expertise on this important issue. Support from national authorities, including information on specific threats, is essential. Those efforts must be joined up with aggressive private sector action:

1. The private sector has an essential role to play in implementing anti–proliferation finance measures and in collaborating on monitoring critical threats. Sophisticated private sector actors, such as major global banks, should consider collaborative analytics that bring together the results from transaction monitoring of networks from high-risk state actors, for example North Korea and Iran. The results of this analytical work should be published, building on examples provided by some global banks at professional gatherings, including Association of Certified Anti–Money Laundering Specialists (ACAMS) meetings.[125] High-risk but sophisticated jurisdictions, such as Singapore and Hong Kong, can lead in this effort. Existing models for this type of work include the way U.K. Finance and the Consortium, venues for private sector information sharing in the United Kingdom and the United States respectively, provide a forum for discussion of experiences and research on typologies and red flags. There would be no practical obstacle to substantive work on transaction monitoring strategies.
2. The private sector, especially banks with significant experience and expertise, should lead in making the most of existing information-sharing mechanisms, for example the Joint Anti–Money Laundering Intelligence Task Force (JMLIT) in the United Kingdom and the Consortium in the United States, to focus specifically on proliferation finance cases. For both JMLIT and the Consortium, proliferation finance is only one of an entire category of financial crimes issues considered, and many members fall into the trap of considering countering proliferation finance to be the concern of sanctions compliance or export control, rather than a unique challenge requiring more policy creativity.
3. The private sector should be proactive in compiling and sharing proliferation finance typologies, recognizing that there is substantial value in aggressive responses to serious national security threats. Such action offers significant reputational benefits. Private sector actors have been successful at identifying nodes of those networks through investigations within their own business operations. These firms do not have many opportunities to share relevant information about their discoveries. Doing so can avoid many privacy and information-sharing hurdles in the short term, as information about specific customers and companies can be safely anonymized and released publicly.

## Conclusion

Preventing the spread of weapons of mass destruction is an essential priority for the international community. Despite this, gaps in the countering proliferation finance regime exist at the multilateral and national level. Some of these are political; others are related to capacity and resources. Regardless of the source of the deficiency, it is essential for the world to get this issue right.

While filling in and strengthening the global legal and regulatory framework is a critical step, it is ultimately dependent on the exercise of political will. If years of grave conversation about nuclear threats at the United Nations, and the erosion of core arms control regimes, have not motivated political will, then the United States should take more aggressive leadership to push forward international laws and obligations on countering proliferation finance. Repeatedly, governmental officials, bank executives, and independent observers privately note that to overcome competing economic and political

*The advances in financial technology are causing major financial and transshipment hubs to understand how to regulate virtual currencies such as Bitcoin. It is highly likely that proliferation networks will try to exploit cryptocurrencies and other new financial technologies to continue their illicit activities. (Dan Kitwood/Getty Images)*

interests that serve to undermine true efforts to expose and halt proliferation finance, powerful legal compulsion or significant reputational risk will be required. The United States is unique in its capability to deliver this kind of change and thereby enable a change in political will. The Trump administration has emphasized, in its strategic approach to adversaries Iran and North Korea, that it is concerned about the proliferation of weapons of mass destruction. It has used diplomatic and economic tools to constrain the ability of both countries to expand their arsenal (especially in the case of North Korea) and return to an enrichment path that could include a weaponization component (in the case particularly of Iran).

The United States has a window to lead multilaterally at the United Nations and FATF, bilaterally in its diplomatic relationship with important financial jurisdictions, and nationally with its own laws, regulations, and procedures. The layers of cooperation required will

**The initial steps to counter WMD proliferation must be taken now, before the international community deals with a paradigm-shifting event.**

be built over the long term, but the initial steps must be taken now, before the international community deals with a paradigm-shifting event. If a U.S. adversary gains a permanent nuclear or other WMD capability and uses it during a crisis, the policy response will be much more overwhelming and restrictive than preventative measures that can be taken now to redress the gaps in the regulatory regime.

This urgency is underscored by the fact that the nature of the threat is continuously evolving. During the past few years, North Korea has demonstrated its sophisticated cyberspace capabilities. Recent reporting has identified new typologies showing that North Koreans are raising money through social media and mobile application software (apps) tied to the gig economy.[126] The U.S. Treasury Department has responded with sanctions targeting information technology firms in China and Russia, but, as this report has demonstrated, sanctions enforcement alone is insufficient to counter this threat.[127]

This is particularly true given the pace of technological change, particularly in the financial technology space. Virtual currency, distributed ledger technology, and the application of artificial intelligence to amassing and analyzing data all promise to remake how consumers and institutions interact with the global financial system. Jurisdictions are trying to understand how to regulate virtual currencies such as Bitcoin.[128] Several major financial and transshipment hubs are also working to understand how new technology is impacting the architecture of global trade.[129] International banks already have problems in matching trade data with

financial data, a situation that proliferation networks have exploited to obscure the illicit acquisition of WMD goods within the wider sphere of global trade. New data solutions, including artificial intelligence, may enable faster and more systematic analysis of this data, enabling banks to have significantly more visibility. While the exact course of those developments is hard to predict, because existing proliferation finance networks and methodologies are neutralized by actions of the international community, it is highly likely that proliferation networks will try to exploit new technology to continue their illicit activities. Regulators at both the international and national levels have an important role to play in advancing rules to leverage new technology solutions – and the time to do so is now.

Identification of proliferation financing offers the international community an additional tool to recognize emerging WMD proliferation networks. Effectively combating proliferation financing will not by itself stop this proliferation, but it is a tool with huge potential, particularly if deployed cross-jurisdictionally. The international community needs to grasp these tools now. Ultimately, U.S. leadership has a critical role to play in the process. The next few years will determine whether the gaps in the regime can be patched to the extent required to push back on the WMD threat from U.S. adversaries.

## Endnotes

1. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, S/2014/147 (March 6, 2014), http://www.un.org/ga/search/view_doc.asp?symbol=S/2014/147.

2 According to FATF, the definition of proliferation finance refers to "the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."

3. See, for example, adaptations in the use of export of coal through shipping networks. Joby Warrick, "High Seas Shell Game: How a North Korean Shipping Ruse Makes a Mockery of Sanctions," *The Washington Post*, March 3, 2018, https://www.washingtonpost.com/world/national-security/high-seas-shell-game-how-a-north-korean-shipping-ruse-makes-a-mockery-of-sanctions/2018/03/03/3380e1ec-1cb8-11e8-b2d9-08e748f892c0_story.html?utm_term=.71827c1f301f.

4. See Case Study 19 in Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation," Final Report (King's College London, October 2017), https://projectalpha.eu/wp-content/uploads/sites/21/2018/05/FoP-13-October-2017-Final.pdf.

5. Press coverage of the as-yet unreleased United Nations Panel of Experts report indicates that the U.N. experts have concluded that North Korea's networks "operate with little or no constraints in five main countries." Colum Lynch, "U.N. Report Details How North Korea Evades Sanctions," *Foreign Policy*, September 20, 2018, https://foreignpolicy.com/2018/09/20/un-report-details-how-north-korea-evades-sanctions/.

6. On enforcement actions, see the imposition of Patriot Act 311 measures against the China-based Bank of Dandong for "serving as a conduit" between North Korea and the international financial system, to the direct benefit of North Korea's nuclear program. Department of the Treasury, Financial Crimes Enforcement Network, "Imposition of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern," Federal Register 82, no. 215 (November 8, 2017): 51758, https://www.fincen.gov/sites/default/files/federal_register_notices/2017-11-08/Dandong%20Final%202017-24238.pdf. The U.S. objectives for its FATF presidency can be found at: "Objectives for FATF – XXX (2018-2019)," Financial Action Task Force, June 29, 2018, http://www.fatf-gafi.org/media/fatf/content/images/Objectives%20for%20FATF-XXX%20(2018-2019).pdf.

7. Richard A. Clarke, "Statement of Richard A. Clarke," Testimony before the U.S. Senate Banking Committee, October 22, 2003, https://www.banking.senate.gov/imo/media/doc/clarke.pdf.

8. "Bin Laden Papers Including Loving Notes, Terrorist Application," *Chicago Tribune*, May 20, 2015, http://www.chicagotribune.com/news/nationworld/ct-osama-bin-laden-documents-20150520-story.html.

9. Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: PublicAffairs, 2013).

10. "Global Terrorism in 2017," START Background Report (University of Maryland, August 2018), https://www.start.umd.edu/pubs/START_GTD_Overview2017_July2018.pdf.

11. Thomas Renard, "Europe's 'New' Jihad: Homegrown, Leaderless, Virtual," Security Policy Brief No. 89 (Egmont Institute, July 2017), http://www.egmontinstitute.be/content/uploads/2017/07/89.spb_amended.pdf?type=pdf.

12. United Nations 1540 Committee, "Message from the 1540 Committee Chair" (November 2018, issue 15), http://www.un.org/en/sc/1540/chair-message.shtml.

13. William B. Messmer and Carlos L. Yordán, "A Partnership to Counter International Terrorism: The U.N. Security Council and the U.N. Member States," *Studies in Conflict & Terrorism* 34 no. 11 (October 2011), http://www.tandfonline.com/doi/full/10.1080/1057610X.2011.611932?src=recsys.

14. United Nations Counter-Terrorism Committee, *Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States*, S/2011/463 (September 1, 2011), 6, https://www.un.org/sc/ctc/wp-content/uploads/2016/01/2011-globalsurvey1373.pdf.

15. United Nations General Assembly, *International Convention for the Suppression of the Financing of Terrorism*, Resolution 54/109 (December 9, 1999), http://www.un.org/law/cod/finterr.htm.

16. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, S/2018/171 (February 1, 2018), http://www.un.org/ga/search/view_doc.asp?symbol=S/2018/171.

17. Michelle Nichols, "U.N. to Vote on New North Korea Sanctions on Monday Afternoon: Diplomats," Reuters, September 10, 2017, https://www.reuters.com/article/us-northkorea-missiles-un/u-n-to-vote-on-new-north-korea-sanctions-on-monday-afternoon-diplomats-idUSKCN1BM06W.

18. Barry Hart Dubner and Mary Carmen Arias, "Under International Law, Must a Ship on the High Seas Fly the Flag of a State in Order to Avoid Being a Stateless Vessel? Is a Flag Painted on Either Side of the Ship Sufficient to Identify It?," Digital Commons @ Barry Law, 29 U.S.F.

Mar. L. J. 99 (2017), https://lawpublications.barry.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1120&context=facultyscholarship.

19. Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (February 2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

20. Financial Action Task Force, *FATF Guidance on Counter Proliferation Finance: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction* (February 2018), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf.

21. United Nations Security Council, *Letter from the Chair of the Security Council Committee Established Pursuant to Resolution 1540 (2004)*, S/2016/1038 (9 December 2016,), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/1038.

22. Authors' interviews with bank officials in Singapore and Hong Kong.

23. Kenneth A. Blanco, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, "S. 1241: Modernizing AML Laws to Combat Money Laundering and Terrorist Financing," Statement to the Committee on the Judiciary, U. S. Senate, November 28, 2017, https://www.judiciary.senate.gov/imo/media/doc/Blanco%20Testimony.pdf.

24. Jonathan Stempel, "U.S. Seeks Funds Tied to North Korea from Eight Big Banks," Reuters World News, July 6, 2017, https://www.reuters.com/article/us-usa-north-korea-banks-idUSKBN19S0I4.

25. "Taiwan Businessman Sentenced to 24 Months for Conspiring to Violate U.S. Laws Preventing Proliferation of Weapons of Mass Destruction," U. S. Department of Justice, press release, March 16, 2015, https://www.justice.gov/opa/pr/taiwan-businessman-sentenced-24-months-conspiring-violate-us-laws-preventing-proliferation.

26. Bureau of Industry and Security, *Export Administration Regulations: General Regulations*, Part 736 (March 16, 2016), https://www.bis.doc.gov/index.php/documents/regulation-docs/413-part-736-general-prohibitions/file.

27. Bureau of Industry and Security, *Control Policy: End-User and End-Use Base*, Part 744 (June 6, 2018), https://www.bis.doc.gov/index.php/documents/regulation-docs/418-part-744-control-policy-end-user-and-end-use-based/file.

28. Ibid.

29. Authors' interview with European bank official.

30. "Trade Finance Principles" (Wolfsberg Group, International Chamber of Commerce, and BAFT, 2017), 7, http://www.baft.org/docs/default-source/policy-department-documents/final-clean-trade-finance-principles-final.pdf?sfvrsn=2.

31. "Trade Finance Principles" (Wolfsberg Group, ICC, and BAFT, 2017), 19, https://cdn.iccwbo.org/content/uploads/sites/3/2017/01/ICC-Wolfsberg-Trade-Finance-Principless-2017.pdf.

32. Elizabeth Rosenberg, Senior Fellow and Director of the Energy, Economics, and Security Program, Center for a New American Security, "Countering the Financial Networks of Weapons Proliferation," Testimony to the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, July 12, 2018, https://www.cnas.org/publications/congressional-testimony/testimony-before-the-house-financial-services-committee-subcommittee-on-terrorism-and-illicit-finance.

33. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Update on the Continuing Illicit Finance Threat Emanating from North Korea," FinCEN Advisory FIN-2013-A005, July 1, 2013, https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2013-a005.

34. Financial Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures: United States: Fourth Round Mutual Evaluation Report* (December 2016), https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

35. United Nations Security Council, *Resolution 2397* (2017), http://undocs.org/S/RES/2397(2017).

36. U. S. Department of the Treasury, *Settlement Agreement*, COMPL-2013-193659 (June 30, 2014), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140630_bnp_settlement.pdf; "Treasury Department Reaches Landmark Settlement with HSBC," U.S. Department of the Treasury, press release, December 11, 2012, https://www.treasury.gov/press-center/press-releases/Pages/tg1799.aspx; U.S. Department of the Treasury, *Settlement Agreement between U.S. Department of Treasury's Office of Foreign Assets Control and Commerzbank AG*, FAC No. 713262 (March 12, 2015), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150312.aspx.

37. 18 U.S.C. § 1956, "Laundering of Monetary Instruments," https://www.law.cornell.edu/uscode/text/18/1956.

38. Sonia Ben Ouagrham-Gormley, "Banking on Nonproliferation: Improving the Implementation of Financial Sanctions," *The Nonproliferation Review* 19, no. 2 (June 2012), http://www.tandfonline.com/doi/full/10.1080/10736700.2012.690963?src=recsys#.

39. 31 CFR § 1020.220, "Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks," https://www.law.cornell.edu/cfr/text/31/1020.220.

40. Authors' interviews with U.S. government officials.

41. Authors' interviews with current and former U.S. law enforcement officials.

42. Emil Dall, Tom Keatinge, and Andrea Berger, "Countering Proliferation Finance: An Introductory Guide for Financial Institutions" (Royal United Services Institute [hereafter RUSI] Guidance Paper, April 2017), 12, https://rusi.org/sites/default/files/201704_rusi_cpf_guidance_paper.1_0.pdf.

43. "Treasury Designates Banco Delta Asia as Primary Money Laundering Concern under USA PATRIOT Act," U.S. Department of the Treasury, press release, September 15, 2005, https://www.treasury.gov/press-center/press-releases/Pages/js2720.aspx.

44. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies," FinCEN Advisory FIN -2017-A001, January 19, 2017, https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a001.

45. "FinCEN Further Restricts North Korea's Access to the U.S. Financial System and Warns U.S. Financial Institutions of North Korean Schemes," U.S. Department of the Treasury, Financial Crimes Enforcement Network, press release, November 2, 2017, https://www.fincen.gov/news/news-releases/fincen-further-restricts-north-koreas-access-us-financial-system-and-warns-us.

46. Financial Action Task Force, *Combating Proliferation Finance: A Status Report on Policy Development and Consultation* (February 2010), http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.

47. Anagha Joshi, "Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction," 2nd ed. (RUSI: July 2018), https://rusi.org/sites/default/files/20181002_model_law_2nd_edition_final_for_web.pdf.

48. European Commission, "Dual-use trade controls," May 28, 2018, http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/.

49. HM Treasury (United Kingdom), "HM Treasury Advisory Notice: Money Laundering and Terrorist Financing Controls in Higher Risk Jurisdictions," MLRs 2017, n.d. (2018), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664503/Money_laundering_and_terrorist_financing_controls_in_overseas_jurisdictions_____advisory_notice.pdf.

50. "Proceeds of Crime Act 2002 Part 7: Money Laundering Offences," s.330, Crown Prosecution Service, https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences.

51. "Proceeds of Crime: Prevention and Suppression of Terrorism," Criminal Finances Act 2017 (Commencement No. 3) Regulations 2017, No. 1028 (C.94), http://www.legislation.gov.uk/uksi/2017/1028/pdfs/uksi_20171028_en.pdf.

52. Anti-terrorism, Crime and Security Act 2001 (C.24), https://www.legislation.gov.uk/ukpga/2001/24/contents.

53. Office of Financial Sanctions Implementation, HM Treasury, *Financial Sanctions: Guidance* (March 2018), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/645280/financial_sanctions_guidance_august_2017.pdf.

54. Michael Sharvin, "UK Government to Implement a Register of Beneficial Owners of Overseas Entities That Own UK Real Estate," Ince & Co LLP, April 24, 2018, Lexology, https://www.lexology.com/library/detail.aspx?g=7384c063-c972-4c3a-acbf-4990d71264c0.

55. Andrea Berger and Anagha Joshi, "Guidance Paper: Countering Proliferation Finance: Implementation Guide and Model Law for Governments," (RUSI, July 2017), https://rusi.org/sites/default/files/201707_rusi_cpf_implementation_guide_and_model_law_berger_joshi_0.pdf.

56. Strategic Trade Act (STA) 2010, Ministry of International Trade and Industry, http://www.miti.gov.my/index.php/pages/view/sta2010?mid=105.

57. Financial Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Malaysia: Mutual Evaluation Report*, September 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Malaysia-2015.pdf.

58. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 2131 (2014)*, S/2015/131 (February 23, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=S/2015/131.

59. Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act, B.E. 2559 (2016), http://www.amlo.go.th/amlo-intranet/media/k2/attachments/CTPF%20Act_1.pdf.

60. "High-Risk and Other Monitored Jurisdictions," Financial Action Task Force, http://www.fatf-gafi.org/countries/#high-risk.

61. "Public Statement," Financial Action Task Force, press release, June 29, 2018, http://www.fatf-gafi.org/countries/d-i/iran/documents/public-statement-june-2018.html.

62. Financial Action Task Force, *Anti-Money Laundering and Combating the Financing of Terrorism, Mutual Evaluation,*

*8th Follow-up Report: China* (February 17, 2012), http://www.fatf-gafi.org/media/fatf/documents/reports/mer/Follow%20Up%20MER%20China.pdf.

63. "Improving Global AML/CFT Compliance: On-going Process – 29 June 2018," Financial Action Task Force, press release, June 29, 2018, http://www.fatf-gafi.org/countries/d-i/iraq/documents/fatf-compliance-june-2018.html.

64. "Outcomes FATF Plenary, 17–19 October 2018," Financial Action Task Force, October 19, 2018. http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html#two.

65. Ibid.

66. Andrea Berger, "A House Without Foundations: The North Korea Sanctions Regime and Its Implementation," (RUSI, June 9, 2017), https://rusi.org/publication/whitehall-reports/house-without-foundations-north-korea-sanctions-regime-and-its; Emil Dall, Tom Keatinge, and Andrea Berger, "Countering Proliferation Finance: An Introductory Guide for Financial Institutions" (RUSI, April 2017), https://rusi.org/sites/default/files/201704_rusi_cpf_guidance_paper.1_0.pdf; and Jonathan Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation" (Center for a New American Security, January 2018), among others.

67. Authors' interviews with bank executive in Hong Kong.

68. For discussions of improving guidance from regulators to financial institutions see, *inter alia*, Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation"; and Dall, Keatinge, and Berger, "Countering Proliferation Finance: An Introductory Guide."

69. Jersey Financial Services Commission, *Guidance on Proliferation and Proliferation Financing*. Jersey Financial Services Commission, October 2011; Central Bank of the Bahamas, Compliance Commission of the Bahamas, Insurance Commission of the Bahamas, and Securities Commission of the Bahamas, *Guidance Note on Proliferation and Proliferation Financing*, Central Bank of the Bahamas, Compliance Commission of the Bahamas, Insurance Commission of the Bahamas, and Securities Commission of the Bahamas, August 21, 2018.

70. Authors' interview with Western European banking regulation expert.

71. Authors' interviews with banking executives in Hong Kong, Singapore, and Malaysia.

72. The Clearing House, *A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement* (February 2017), 7, The Clearing House, https://www.theclearinghouse.org/-/media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.

73. David Thompson, "Risky Business: A System-Level Analysis of the North Korean Proliferation Financing System" (C4ADS, 2017), https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/59413c8bebbd1ac3194eafb1/1497447588968/Risky+Business-C4ADS.pdf.

74. Council Regulation 2016/679/EC on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), European Parliament, April 26, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679; and authors' interviews with bank officials.

75. See the text of the Final Customer Due Diligence Rule at Federal Register, U.S. Department of the Treasury, Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, 81, no. 91 (May 11, 2016), 29398-29458, https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

76. Financial Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Mutual Evaluation Report* (December 2016), 224, http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

77. "A New Standard on Beneficial Ownership: Where Do the U.S. and Canada Stand?" Transparency International, May 10, 2018, https://voices.transparency.org/a-new-standard-on-beneficial-ownership-transparency-where-do-the-us-and-canada-stand-fb8caa6bad66.

78. Nathalie Colin, Willem Van de Wiele, Alexandre Hublet, Olivier Van Wuowe, and Elien Claeys, "Adoption of Fifth Anti-Money Laundering Directive," White & Case, https://www.whitecase.com/publications/alert/adoption-fifth-anti-money-laundering-directive.

79. "Their overly broad and vague definitions, unworkable requirements, and severe penalties would do far more to impede law abiding small and medium-sized business than to hamper the use of so-called 'shell companies' to facilitate illicit activity." Brian O'Shea, Senior Director, Center for Capital Markets Competitiveness, U.S. Chamber of Commerce, "Beneficial Ownership: Fighting Illicit International Financial Networks Through Transparency," Testimony to the Senate Judiciary Committee, February 6, 2018, https://www.uschamber.com/sites/default/files/020618_brian_oshea_testimony_beneficial_ownership.pdf.

80. M. Kendall Day, Acting Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, "Beneficial Ownership: Fighting Illicit International Financial Networks through Transparency," Testimony to the Senate Judiciary Committee, February 6, 2018, https://www.judiciary.senate.gov/imo/media/doc/02-06-18%20Day%20Testimony.pdf.

81. Brewer, "Study of Typologies of Financing of WMD Proliferation."

82. Daniel Salisbury and Ian J. Stewart, "Li Fang Wei (Karl Lee)," Proliferation Case Study Series (Project Alpha, King's College, London, May 19, 2014), http://kcl-di-gi-prod-wa-wordp-ne-04.azurewebsites.net/alpha/wp-content/uploads/sites/21/2014/09/Karl-Li-case-study-final.pdf.

83. Glenn Kessler, "U.S. Links Iranian Bank to Fifth Avenue Building," *The Washington Post*, December 18, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/12/17/AR2008121703844.html.

84. Financial Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures: Mutual Evaluation Report*, 224.

85. "Hearing Entitled 'Countering the Financial Networks of Weapons Proliferation,'" House Financial Services Committee, July 12, 2018, https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=403709; "Hearing Entitled 'Implementation of FinCEN's Customer Due Diligence Rule – Financial Institutions Perspective,'" House Financial Services Committee, April 27, 2018, https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=403343.

86. Authors' interviews with government officials.

87. Authors' interviews with government regulators and bank executives in Hong Kong, Malaysia, Singapore, and the United Kingdom.

88. Elizabeth Rosenberg, Director and Senior Fellow, Center for a New American Security, testimony to the Committee Subcommittee on Terrorism and Illicit Finance, Financial Services Committee, U.S. House of Representatives, July 12, 2018, 6, https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-erosenberg-20180712.pdf.

89. Lynch, "U.N. Report Details How North Korea Evades Sanctions."

90. Jason Arterburn, "Dispatched: Mapping Overseas Forced Labor in North Korea's Proliferation Finance System" (C4ADS, 2018), https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5b631c9b2b6a2845024e4ff5/1533222111619/Dispatched+Final-2.pdf.

91. Donald J. Trump, Twitter post, July 9, 2018, 7:25 a.m., https://twitter.com/realDonaldTrump/status/1016327387154395138?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1016327387154395138&ref_url=https%3A%2F%2Fthehill.com%2Fhomenews%2Fadministration%2F396087-trump-china-may-be-exerting-negative-pressure-on-nuclear-deal-with.

92. "Treasury Imposes Sanctions on Supporters of North Korea's Weapons of Mass Destruction Proliferation," U.S. Department of the Treasury, press release, September 26, 2018, https://www.treasury.gov/press-center/press-releases/Pages/jl5059.aspx; Thompson,"Risky Business."

93. Agence France-Presse, "In China, North Korean Firms Still Trading Despite Shutdown Order," *South China Morning Post*, January 9, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2127530/china-north-korean-firms-still-trading-despite-shutdown.

94. Eleanor Albert, "The China-North Korea Relationship," CFR.org, March 28, 2018, https://www.cfr.org/backgrounder/china-north-korea-relationship.

95. "Treasury Sanctions Trading, Labor, and Shipping Companies and Vessels to Further Isolate North Korea," U.S. Department of the Treasury, press release, November 21, 2017, https://www.treasury.gov/press-center/press-releases/Pages/sm0220.aspx.

96. "2016 Nyeon bughan-ui daeoemuyeog donghyang [2016 Trends in North Korean Trade]," Korea Trade Investment Promotion Agency, July 27, 2017, https://news.kotra.or.kr/common/extra/kotranews/globalBbs/249/fileDownLoad/47252.do.

97. "CCDI: Liaoning vice governor under investigation," CGTN, November 23, 2017, https://news.cgtn.com/news/7a417a4c78637a6333566d54/share_p.html.

98. Li Keqiang, "Full Text: *Report on the Work of the Government (2016)*," State Council of the People's Republic of China, March 17, 2016, http://english.gov.cn/premier/news/2016/03/17/content_281475309417987.htm.

99. Adam Taylor and Min Joo Kim, "North Korean Economy Suffers Its Steepest Decline in Two Decades," *The Washington Post*, July 20, 2018, https://www.washingtonpost.com/world/north-korean-economy-suffers-steepest-decline-in-two-decades/2018/07/20/50a84dbc-8bd7-11e8-8b20-60521f27434e_story.html?utm_term=.d9ed8b2eb7fb.

100. Emily Rauhala and Damian Paletta, "China Warns It Could Fire Back with Tariffs on $60 Billion in U.S. Goods," *The Washington Post*, August 3, 2018, https://www.washingtonpost.com/world/asia_pacific/china-warns-it-could-fire-back-with-tariffs-of-60-billion-in-us-goods/2018/08/03/57ffbf56-9716-11e8-8ffb-5de6d5e49ada_story.html?utm_term=.0a69399bffe8.

101. The State Council of the People's Republic of China, "China's Arab Policy Paper," January 13, 2016, http://english.gov.cn/archive/publications/2016/01/13/content_281475271412746.htm; "Arms Control and Proliferation Profile: China," Arms Control Association, July 2017, https://www.armscontrol.org/factsheets/chinaprofile.

102. Kenley Butler, "Weapons of Mass Destruction in Asia," The Nuclear Threat Initiative, October 1, 2002, https://www.nti.org/analysis/articles/weapons-mass-destruction-central-asia/.

103. Samuel Ramani, "North Korea's Military Partners in the Horn of Africa," The Diplomat, January 6, 2018, https://thediplomat.com/2018/01/north-koreas-military-partners-in-the-horn-of-africa/.

104. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 2345 (2017)*, S/2018/171 (March 5, 2018), http://www.un.org/ga/search/view_doc.asp?symbol=S/2018/171.

105. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 2145 (2017)*, S/2017/742 (September 5, 2017), http://www.un.org/ga/search/view_doc.asp?symbol=S/2015/131.

106. United Nations Security Council, *Report of the Panel of Exports Established Pursuant to Resolution 1874 (2009)* (February 27, 2017), http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150.

107. United Nations Security Council, *Report of the Panel of Exports Established Pursuant to Resolution 1874 (2009)* (February 23, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=S/2015/131.

108. Kevin Sieff, "North Korea's Surprising, Lucrative Relationship with Africa," *The Washington Post*, July 10, 2017, https://www.washingtonpost.com/world/africa/north-koreas-surprising-lucrative-relationship-with-africa/2017/07/10/c4e6f65d-30fe-4bd2-b178-d90daaac3007_story.html.

109. Financial Action Task Force, *Mutual Evaluation Report: Anti-Money Laundering and Combating the Financing of Terrorism: The Federal Democratic Republic of Ethiopia* (May 2015), http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/WB-ESAAMLG-Mutual-Evaluation-Report-Ethiopia-2015.pdf.

110. While exact figures vary, the U.S. State Department estimates that North Korea dedicated about 24 percent of its gross domestic product to military expenditure. U.S. Department of State, *World Military Expenditures and Arms Transfers 2017* (December 2017), https://www.state.gov/t/avc/rls/rpt/wmeat/2017/index.htm.

111. Financial Action Task Force, *Mutual Evaluation Report: Anti-Money Laundering, Ethiopia*.

112. Hamish Macdonald, "Ethiopia Working to Restrict North Korean Embassy's Bank Accounts: MFA," NKNews.org, August 3, 2017, https://www.nknews.org/2017/08/ethiopia-working-to-restrict-north-korean-embassys-bank-accounts-mfa/.

113. "Export Scheme Charges Unsealed in U.S. District Court," The U.S. Attorney's Office Middle District of Pennsylvania, press release, April 2, 2014, https://www.justice.gov/usao-mdpa/pr/export-scheme-charges-unsealed-us-district-court.

114. Brewer, "Study of Typologies of Financing of WMD Proliferation."

115. Don Oberdorfer, "Pakistan: The Quest for Atomic Bomb," *The Washington Post*, August 27, 1979, https://www.washingtonpost.com/archive/politics/1979/08/27/pakistan-the-quest-for-atomic-bomb/a04882f4-1603-41f4-b168-8ba45057a10b/?noredirect=on&utm_term=.093aafdc4f73; Alex Wagner, "Bush Waives Nuclear-Related Sanctions on India, Pakistan," Arms Control Association, October 1, 2001, https://www.armscontrol.org/act/2001_10/sanctionsoct01.

116. Richard Boucher, daily press briefing, U.S. Department of State, September 24, 2001, https://2001-2009.state.gov/r/pa/prs/dpb/2001/5040.htm.

117. "Improving Global AML/CFT Compliance," Financial Action Task Force.

118. Drazen Jorgic, "China Lends $1 Billion to Pakistan to Boost Plummeting FX Reserves – Sources," Reuters, June 30, 2018. https://www.reuters.com/article/us-pakistan-china-loans/china-lends-1-billion-to-pakistan-to-boost-plummeting-fx-reserves-sources-idUSKBN1JQ0TV.

119. U.S. Department of State, *Country Reports on Terrorism 2017* (September 2018), https://www.state.gov/j/ct/rls/crt/2017/282845.htm; "FATF Unhappy with Pakistan's Efforts to Combat Terror," *Deccan Herald*, October 11, 2018. https://www.deccanherald.com/international/faft-team-not-happy-pakistans-697445.html.

120. Catherine Collins and Douglas Frantz, "The Long Shadow of A. Q. Khan," *Foreign Affairs*, January 31, 2018, https://www.foreignaffairs.com/articles/north-korea/2018-01-31/long-shadow-aq-khan; Declan Walsh, "Disgraced Atomic Scientist Disowns Confession," The Guardian, May 29, 2008, https://www.theguardian.com/world/2008/may/30/pakistan.nuclear.

121. "Arms Control and Proliferation Profile: Pakistan," fact sheet (Arms Control Association, July 2018), https://www.armscontrol.org/factsheets/pakistanprofile.

122. 1540 Committee, "Pakistan," United Nations 1540 Committee, http://www.un.org/en/sc/1540/assistance/offers-of-assistance/offers-from-member-states/pakistan.shtml.

123. U.S. House of Representatives, *Empowering Financial Institutions to Fight Human Trafficking Act of 2018*, H.R. 6729, 115th Cong., 2nd sess., https://www.congress.gov/bill/115th-congress/house-bill/6729/text?q=%7B%22search%22%3A%5B%22information+sharing%22%5D%7D&r=13.

124. Brewer, "Study of Typologies of Financing of WMD Proliferation."

125. For example, Wells Fargo's presentation at the ACAMS annual meeting in Las Vegas in September 2017, session titled: "A Clear and Present Danger: Developing Models to Combat Proliferation Financing."

126. Wenxin Fan, Tom Wright, and Alistair Gale, "Tech's New Problem: North Korea," *The Wall Street Journal*, September 14, 2018, https://www.wsj.com/articles/north-koreans-exploit-social-medias-vulnerabilities-to-dodge-sanctions-1536944018.

127. "Treasury Targets North Korea-Controlled Information Technology Companies in China and Russia," U.S. Department of the Treasury, press release, September 13, 2018, https://home.treasury.gov/news/press-releases/sm481.

128. Julia Solomon-Strauss, Edoardo Saravalle, and Claire Groden, "Uncharted Waters: A Primer on Virtual Currency Regulation around the World" (Center for a New American Security, October 2018), https://www.cnas.org/publications/reports/uncharted-waters.

129. Alan Juhn, "Hong Kong Regulator, Banks Launch Blockchain-Based Trade Finance Platform," Reuters, July 17, 2018, https://www.reuters.com/article/us-blockchain-trade/hong-kong-regulator-banks-launch-blockchain-based-trade-finance-platform-idUSKBN1K70AP.

130. Figure is based on Project Alpha Report on Typologies of Financing of Proliferation, October 2017, which is based on the 2017 Final Report of the U.N. Panel of Experts on DPRK. This figure is reprinted from Jonathan Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation," (Center for a New American Security, January 2018), 9.

## About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.



1152 15th Street, NW Suite 950 Washington, DC 20005
t. 202.457.9400 | f. 202.457.9401 | info@cnas.org | cnas.org


Center for a
New American
Security
Bold. Innovative. Bipartisan.

**"OPINION POLL—SMALL BUSINESS OWNERS SUPPORT LEGISLATION REQUIRING TRANSPARENCY IN BUSINESS FORMATION", SMALL BUSINESS MAJORITY**


## Opinion Poll

### Small Business Owners Support Legislation Requiring Transparency in Business Formation

April 4, 2018

**Small Business Majority**
1101 14th Street, NW, Suite 950
Washington, DC 20005
(202) 828-8357
*www.smallbusinessmajority.org*

## Executive Summary

Under current law, business owners are not required to list their identity when they establish a business, which has encouraged some to establish anonymous shell companies to engage in illicit behavior. However, Congress is currently considering bipartisan legislation that would require businesses to list the true identity of their owners when forming to address issues of fraud and abuse. The legislation provides that owners' names would be kept private and would only be made available to law enforcement with a proper subpoena or summons. Some have argued that this increased transparency could boost accountability and confidence in the system, while others have raised concerns that it could hinder business formation. Now, new scientific opinion polling shows small business owners decidedly support this legislation.

The survey, conducted by Chesapeake Beach Consulting for Small Business Majority, revealed that 77% of small business owners agree Congress should pass legislation that would require businesses to list the true identity of their owners when forming, with roughly half (49%) in strong agreement. The poll was an online survey of 500 small business owners nationwide conducted between March 5 and 11, 2018.

Additionally, the survey found a vast 84% of small business owners say the use of shell companies to win contracts or obtain government set-asides reserved for small businesses is a problem. Nearly 6 in 10 (58%) believe this is a major problem, and only 5% of small business owners say this is not a problem.

What's more, the survey results indicate that small business owners do not believe this disclosure would place a burden on their business. Indeed, 76% of small business owners feel legislation requiring small businesses to list the true identities of their owners would benefit them by protecting them from contract fraud and giving them fair access to government set asides, compared to just 9% who feel that such legislation would be a burden or would stifle business creation. Importantly, nearly all small business owners disclose their true identities when establishing their business. A mere 3% of respondents say they did not disclose their identity when setting up their small business.

These results are similar across all geographic regions and there is no difference among respondents based on political affiliation. Indeed, the same number of small business owners identifying as Democrat or Republican (79%) agree that Congress should pass a law requiring businesses to list the true identity of their owners when forming.

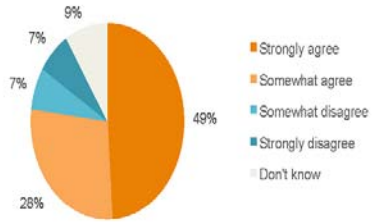
As these results show, small business owners are broadly supportive of legislation that would further improve accountability in rules regarding business ownership transparency.

## Methodology

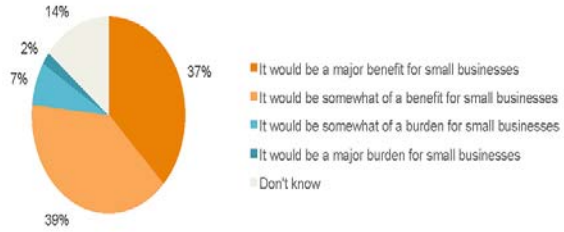
This poll reflects an Internet survey of 500 small business owners nationwide with 1-100 employees. The poll was conducted by Chesapeake Beach Consulting for Small Business Majority between March 5-11, 2018. The margin of error is +/-4.4%.

## Main Findings

- **Small business owners support legislation requiring disclosure of business owners:** 77% of small business owners agree Congress should pass legislation that would require businesses to list the true identity of their owners when forming. Under the bill, the owners' names would be kept private and would only be made available to law enforcement with a proper subpoena or summons. Roughly half (49%) strongly agree we need this disclosure in place.




- **Small business owners believe use of shell companies to fraudulently win contracts is a problem:** A vast 84% of small business owners say the use of shell companies to win contracts or obtain government set-asides reserved for small businesses is a problem. Nearly 6 in 10 (58%) believe this is a major problem.
- **Small business owners believe legislation requiring small businesses to list the true identities of their owners would benefit rather than burden their businesses:** More than 3 in 4 small business owners (76%) think legislation requiring a small business to list the true identities of their owners would benefit small businesses by protecting them from contract fraud and giving them fair access to government set-asides. Just 9% of small business owners think such legislation would be a burden on businesses and would stifle business creation.




- **Nearly all small business owners disclose their true identities when establishing their business:** A mere 3% of respondents say they did not disclose their identity when setting up their small business.
- **Small business owners are politically and geographically diverse:** 45% of respondents identify as Republican or Republican-leaning independents, 39% are Democrat or Democrat-leaning independents and 15% are pure independent. Additionally, 22% of respondents are from the West, 25% from the Midwest, 38% from the South and 16% from the Northeast.

## Toplines

500 Small Business Owners Nationwide (Online)
1-100 Employees
March 2018

1. Please indicate your gender

| | |
|---|---|
| Male | 60% |
| Female | 40% |

2. What state is your business in?

| | |
|---|---|
| West | 22% |
| Midwest | 25% |
| South | 38% |
| Northeast | 16% |

3. Do you own your own for-profit business?

| | |
|---|---|
| Yes | 100% |

4. How many people do you employ including yourself? *(Cap at 25% self-employed)*

| | |
|---|---|
| One | 25% |
| 2 to 9 | 56% |
| 10 to 19 | 9% |
| 20 to 49 | 6% |
| 50 to 100 | 4% |

5. How long have you been in business?

| | |
|---|---|
| Less than one year | 2% |
| One to three years | 11% |
| Four to six years | 13% |
| Seven to 10 years | 14% |
| More than 10 years | 60% |
| Don't know | 0% |
| Refused | 0% |

6. As you may know, current law allows a business to be established without listing the identities of the business' owners. Some have used these anonymous shell companies to engage in illicit behavior such as money laundering and financing criminal activity. Congress is considering legislation which would require businesses to list the true identity of their owners when forming. The owners' names would be kept private and would only be made available to law enforcement with a proper subpoena or summons.

   Do you strongly agree, somewhat agree, somewhat disagree or strongly disagree that Congress should pass such a law?

| | |
|---|---|
| Strongly agree | 49% |
| Somewhat agree | 28% |
| Somewhat disagree | 7% |
| Strongly disagree | 7% |
| Don't know | 9% |
| Refused | 0% |
| **AGREE** | **77%** |
| **DISAGREE** | **14%** |

7. Some have used shell companies to fraudulently win contracts or obtain government set-asides reserved for small businesses. Would you say these practices are a major problem, a minor problem, or not a problem?

| | |
|---|---|
| Major problem | 58% |
| Minor problem | 27% |
| Not a problem | 5% |
| Don't know | 11% |
| Refused | 0% |
| **PROBLEM** | **84%** |
| **NOT A PROBLEM** | **5%** |

8. ***Some people*** say that requiring small businesses to list the true identities of their owners would benefit small businesses by protecting them from contract fraud and giving them fair access to government set-asides.

   ***Other people*** say that requiring listing of business owners' identities places an unnecessary burden on businesses and would stifle business creation.

   Do you think it would be a benefit or a burden for small businesses such as yours to disclose the true identity of their owners?

| | |
|---|---|
| It would be a major benefit for small businesses | 37% |
| It would be somewhat of a benefit for small businesses | 39% |
| It would be somewhat of a burden for small businesses | 7% |
| It would be a major burden for small businesses | 2% |
| Don't know | 14% |
| Refused | 0% |
| **BENEFIT** | **76%** |
| **BURDEN** | **9%** |

9. Did you disclose your true identity when establishing your small business?

| | |
|---|---|
| Yes | 95% |
| No | 3% |
| Don't know | 1% |
| Refused | <1% |

Now, I have just a few questions for statistical purposes...

10. How would you categorize your business?

| | |
|---|---|
| Retail | 17% |
| Financial, insurance or legal services | 9% |
| Construction | 8% |
| Real estate | 6% |
| Information technology | 5% |
| Agriculture | 4% |
| Manufacturing | 3% |
| Medical or dental | 3% |
| Restaurant or food service | 3% |
| Other non-retail services | 9% |
| Wholesale trade | 3% |
| Other | 29% |
| Not sure/Refused to answer | 1% |

11. In what year were you born?

| | |
|---|---|
| 18-29 | 3% |
| 30-44 | 19% |
| 45-54 | 20% |
| 55-64 | 32% |
| 65+ | 25% |

12. Generally speaking, do you think of yourself as a Republican, a Democrat, or an Independent?

| | |
|---|---|
| Democrat | 26% |
| Independent | 33% |
| Republican | 35% |
| Other | 3% |
| Don't know | 1% |
| Refused | <1% |

12a. IF INDEPENDENT, OTHER OR DON'T KNOW, ASK: Do you think of yourself as closer to the Republican or Democratic Party? ***N=189***

| | |
|---|---|
| Closer to Democrats | 32% |
| Closer to Republicans | 26% |
| Neither | 39% |
| Don't know | 2% |
| Refused | 1% |

13. Again, just for statistical purposes what was the gross revenue of your business in 2017?

| | |
|---|---|
| Less than $100,000 | 39% |
| Between $100,000 and $250,000 | 16% |
| Between $250,001 and $500,000 | 13% |
| Between $500,001 and $1 million | 12% |
| Between $1 million and $2 million | 8% |
| Between $2 million and $5 million | 4% |
| More than $5 million | 2% |
| Don't know | 1% |
| Refused | 6% |

14. What is your race?

| | |
|---|---|
| White | 82% |
| African American or Black | 5% |
| Hispanic of Chicano | 4% |
| Asian or Pacific Islander | 4% |
| American Indian | 1% |
| Other | 1% |
| Biracial or multiracial | 1% |
| Don't know | 0% |
| Refused | 1% |

**LETTER SUBMITTED BY GLOBAL FINANCIAL INTEGRITY**

GLOBAL FINANCIAL INTEGRITY

June 26, 2019

The Honorable Mike Crapo
Chairman, Committee on Banking, Housing, and Urban Affairs
United States Senate
538 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Sherrod Brown
Ranking Member, Committee on Banking, Housing, and Urban Affairs
United States Senate
538 Dirksen Senate Office Building
Washington, D.C. 20510

**RE: June 20th Hearing on "Outside Perspectives on the Collection of Beneficial Ownership Information"**

Dear Chairman Crapo and Ranking Member Brown,

I offer these comments for the record on behalf of Global Financial Integrity (GFI) with reference to the June 20, 2019, U.S. Senate Committee on Banking, Housing, and Urban Affairs hearing titled "Outside Perspectives on the Collection of Beneficial Ownership". We firstly thank you for holding a hearing on this important issue and inviting opinions that reflect experience but also a multiplicity of views. Anonymous companies pose a serious threat to the security of the United States and GFI sees this hearing as the first of many steps critical to securing our country's financial system from being used as a conduit and a haven for illicit proceeds and criminal activity.

Global Financial Integrity (GFI) is a think tank specializing in research and government advisory services related to illicit financial flows, of which anonymous shell companies are a major facilitator. GFI's economic research on illicit financial flows shows that US$ 1Trillion leaves the developing world every year[1] and anonymous companies are vital in helping obfuscate the audit trail and location of these illicit funds. Our research has also shown that anonymous companies are a critical component of transnational crime, sponsoring everything from human, drug and arms trafficking to terrorist and rogue state financing.[2]

The question that frames this entire issue then becomes how easy it to set up a company in the United States. GFI in March 2019 published a report titled The Library Card Project: The Ease of Forming

[1] Illicit Financial Flows to and from 148 Developing Countries: 2006 – 2015, January 2019 accessible at https://secureservercdn.net/45.40.149.159/34n.8bd.myftpupload.com/wp-content/uploads/2019/01/GFI-2019-IFF-Update-Report-1_29_18.pdf?time=1561583768

[2] https://gfintegrity.org/anonymous-companies-and-transnational-crime/

1100 17th Street, NW, Suite 505 | Washington, DC | 20036 | USA
Tel. +1 (202) 293-0740 | Fax. +1 (202) 293-1720 | www.gfintegrity.org

Anonymous Companies in the United States. The report examined and compared the documentation required to be submitted to acquire a library card versus the documentation required to set up a company in the United States. In every instance, it was found that there were more stringent requirements from document collection, oversight, and verification of identity, in order to secure a library card. In one instance, in a library in Kentucky, biometric information was part of the information required to be submitted. By contrast, to set up a company not even a phone number, e-mail id, or the identity of key management personnel such as a director was required to be provided.[3] What this serves to underscore is that in both instances the State provides a benefit in some measure to the applicant. In the case of the library card, the individual concerned is eligible to apply for a public library card as a benefit to paying taxes and is required to verify his identity to establish that he/she is indeed eligible for the benefit conferred of accessing a public library in the State. When an applicant chooses to set up a company in a State, the applicant similarly receives a benefit of access to courts, ease of business registration, a well-regulated business environment, clearly defined laws, limited liability in the case of LLCs, and the only way to ensure that the applicant is deserving of said benefits is to provide minimal information to ensure that the company's activities are not designed to harm the economic interests of our country and threaten national security.

During the hearing, there were questions raised on the threat of crypto currency, the identities of its users, and its role as a vehicle to harm national security, and what efforts were being taken to address it. The Financial Action Task Force (FATF) , the standard setting body on anti-money laundering (AML) and combating terrorist financing (CFT), in the last year under the Presidency of the United States headed by Marshall Billingslea has undertaken work on proliferation financing, crypto currency otherwise referred to virtual assets, and, terrorist financing. On June 21, a day after the hearing, the FATF released further guidance on virtual assets (cryptocurrency) which requires them to be subject to the full gamut of AML/CFT norms that will at the minimum require customer due diligence including beneficial ownership, record keeping, and filing suspicious activities reports. This assumes vital importance because crypto currency played an instrumental role coupled with anonymous companies in keeping Backpage, the advertising website, and the largest marketplace in the world for buying and selling sex afloat. The company directly involved in the sex trafficking of minors, has been implicated in 7 out of every 10 reported child trafficking cases in the US. As law enforcement forced banks to close out the company's accounts, Backpage turned to crypto currency to continue to launder money and mask their identity.[4] The company additionally was able to evade law enforcement investigation for long by carrying out its operations through a complex network of American and international anonymous companies, starting in Delaware.[5]

Collecting beneficial ownership information at the time of corporate formation, requiring that it be updated whenever there are changes, and making that information available in a timely manner to law enforcement and those in the private sector that we entrust with anti-money laundering responsibilities would provide important new tools to effectively combat terrorism and financial crimes by ending the incorporation of anonymous companies in the United States.

---

[3] The Library Card Project: The Ease of Forming Anonymous Companies in the United States, March 2019 available at https://gfintegrity.org/report/the-library-card-project/

[4] https://www.nytimes.com/2018/04/12/us/backpage-plea-deal-ferrer.html

[5] https://qz.com/1204991/backpage-com-is-registered-in-delaware-heres-why/

In recent years, support for ending the incorporation of anonymous companies has expanded to include national security experts,[6] the police,[7] sheriffs,[8] local prosecutors, [9] state Attorneys General,[10] federal prosecutors,[11] human rights advocates,[12] anti-human trafficking groups,[13] faith-based networks,[14] international development NGOs,[15] CEOs,[16] big businesses,[17] small businesses,[18] banks,[19] credit unions,[20] real estate professionals,[21] insurance companies,[22] and scholars at both conservative[23] and liberal think tanks,[24] among others.

GFI is proud to extend our support to the various bipartisan efforts that have been introduced in both chambers of Congress that would end the abuses of anonymous companies. In the House of Representatives, the *Corporate Transparency Act of 2019* (H.R.2513), sponsored by Representatives Carolyn Maloney (D-NY) and Peter King (R-NY), was reported favorably out of the Committee on Financial Services on June 11–12, 2019 with a strong, bipartisan vote of 43 to 16. This marks the first time that any comprehensive beneficial ownership disclosure bill has made it out of a congressional committee.[25]

GFI has also endorsed bipartisan pieces of legislation in the Senate. Senators Ron Wyden (D-OR) and Marco Rubio (R-FL) cosponsored the companion bill to the Corporate Transparency Act last Congress.[26]

---

[6] Bipartisan Letter from 91 National Security Experts, June 10, 2019, *available at* http://bit.ly/2ZvJECj.

[7] Letter from the Fraternal Order of Police, May 6, 2019, *available at* http://bit.ly/2KoYC9W.

[8] Letter from the National Sheriffs' Association, May 7, 2019, *available at* http://bit.ly/2Fk7vxd.

[9] Letter from the National District Attorneys Association, May 6, 2019, *available at* http://bit.ly/2KoJDg9.

[10] Bipartisan Letter from Two Dozen State Attorneys General, August 2, 2018, *available at* http://bit.ly/2J5Bla3.

[11] Letter from the National Association of Assistant United States Attorneys, May 6, 2019, *available at* http://bit.ly/2L0fkvU.

[12] Letter from Amnesty International USA, EarthRights International, EG Justice, Enough Project, Freedom House, Global Witness, Human Rights First, Human Rights Watch, International Corporate Accountability Roundtable, and the International Labor Rights Forum, April 11, 2019, *available at* https://www.hrw.org/news/2019/04/11/letter-chairwoman-waters-and-ranking-member-mchenry-re-corporate-transparency-act.

[13] *See, for example*, Letter from Polaris, May 2, 2019, *available at* http://bit.ly/2WSJeUS; *and* Letter from Street Grace, March 10, 2019, *available at* http://bit.ly/2WOoti6.

[14] Letter from Jubilee Network USA, March 12, 2019, *available at* http://bit.ly/2IXMXLU.

[15] Letter from ActionAid USA, Bread for the World, Jubilee USA Network, The ONE Campaign, and Oxfam America, June 7, 2019, *available at* http://bit.ly/2MYVPpY.

[16] Letter from the CEOs of a Dozen Major Companies, April 30, 2019, *available at* http://bit.ly/31Ged1L.

[17] Richard Sawaya, "A maximum pressure campaign against the Kremlin," *The Hill*, April 30, 2019, https://thehill.com/opinion/international/441350-a-maximum-pressure-campaign-against-the-kremlin

[18] Letter from Small Business Majority, April 25, 2019, *available at* http://bit.ly/2KtteqK.

[19] *See, for example*: Letter from Nine Banking Associations, May 7, 2019, *available at* http://bit.ly/2XpRlwx; Letter from the Independent Community Bankers of America, May 8, 2019, *available at* http://bit.ly/31Rbc7o; *and* Letter from 51 State Banking Associations, June 10, 2019, *available at* http://bit.ly/2Kow6Fh.

[20] Letter from the Credit Union National Association, June 11, 2019, *available at* http://bit.ly/2KtIfgv.

[21] Letter from the American Escrow Association, American Land Title Association, National Association of REALTORS©, and Real Estate Services Providers Council, Inc. (RESPRO), May 7, 2019, *available at* http://bit.ly/2E2KQoq.

[22] Letter from the Coalition Against Insurance Fraud, April 15, 2019, *available at* http://bit.ly/2KYYygz.

[23] *See, for example*: Clay R. Fuller, "Dealing with anonymity in business incorporation," *American Enterprise Institute*, March 29, 2019, https://www.aei.org/publication/dealing-with-anonymity-in-business-incorporation/.

[24] *See, for example*: Molly Elgin-Cossart and Trevor Sutton, "The Real Scandal Behind the Panama Papers," Center for American Progress, May 10, 2016, https://www.americanprogress.org/issues/security/news/2016/05/10/137191/the-real-scandal-behind-the-panama-papers/.

[25] *See:* Committee on Financial Services, "Markup of H.R. 2162; H.R. 2513; H.R. 2763; H.R. 3018; H.R. 3111; H.R. 3141; H.R. 3154; and H.R. 3167;" *U.S. House of Representatives:* , June 11–12, 2019, *accessible at* https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=403829

[26] *See:* S.1889, 116th Congress, True Incorporation Transparency for Law Enforcement Act, or "TITLE Act"; *assessible at* https://www.congress.gov/bill/116th-congress/senate-bill/1889.

The *True Incorporation Transparency for Law Enforcement (TITLE) Act* (S.1889) — sponsored by Senators Sheldon Whitehouse (D-RI) and Charles Grassley (R-IA), as well as Ranking Member Feinstein (D-CA) — is a well thought out, bipartisan piece of beneficial ownership legislation, which is under consideration by your committee and is also strongly supported by GFI.

Both these bills, the Corporate Transparency Act and the TITLE Act, would allow law enforcement to more thoroughly and effectively conduct investigations and enhance safety by saving time and resources in pursuing complex money laundering operations, terrorist financing, and investigations against organized crime that are critical to safeguarding national security.

GFI also views positively the recent introduction of the bipartisan discussion draft of the *Improving Laundering Laws and Increasing Comprehensive Information Tracking of Criminal Activity in Shell Holdings (ILLICIT CASH) Act*, sponsored by Senators Mark Warner (D-VA), Tom Cotton (R-AR), Doug Jones (D-AL), Mike Rounds (R-SD), which only adds to the growing consensus that the abuse of the financial system through anonymous companies must end.[27]

We appreciate the opportunity to offer these comments. We hope they are helpful, and we look forward to working with you and the Committee in making progress on this important issue. Should you have any questions, please feel free to contact me at lkumar@gfintegrity.org

Sincerely,
**Lakshmi Kumar**
Policy Director

cc Members of the Senate Committee on the Judiciary

---

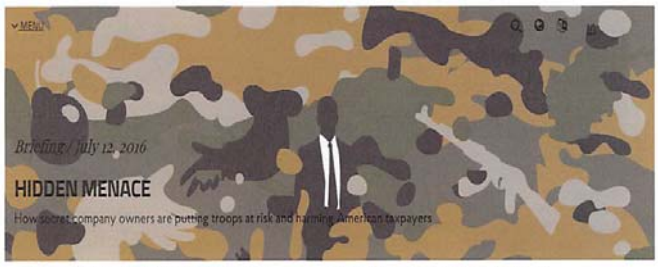
[27] *The FACT Coalition*, "Bipartisan Group of Senators Unveil Draft Anti-Money Laundering, Ownership Transparency Bill," June 10, 2019, *assessible at* http://bit.ly/2Fy2YY3.



1100 17th Street, NW, Suite 505 | Washington, DC | 20036 | USA
Tel. +1 (202) 293-0740 | Fax. +1 (202) 293-1720 | www.gfintegrity.org

**"HIDDEN MENACE", GLOBAL WITNESS**








Since the financial crisis and release of the Panama Papers (https://globalwitness.org/en/press-releases/shell-companies-secrecy-and-us/), we have heard a lot about the revenue governments lose to tax avoidance and evasion, but what about the losses resulting from corruption and fraud when governments spend money on goods, services and infrastructure?

Around the world governments spend $9.5 trillion each year (http://www.cgdev.org/publication/ft/publishing-government-contracts-addressing-concerns-and-easing-implementation) on public procurement. It should be no surprise that fraudsters, and corrupt officials, take advantage of this. According to research by the UN, corruption may amount to as much as 25% of the value of government procurement contracts worldwide.

*Hidden Menace (https://www.globalwitness.org/documents/18532/Briefing_-_Hidden_Menace_-_12072016.pdf)* reveals the seriousness of the problem of anonymously-owned companies in U.S. government spending and recommends what must be done to fix it. It focuses on the issue of anonymous shell companies in military contract spending, both because of the serious national security risks posed by their use for illicit purposes, and because of the significant proportion of the U.S. budget—approximately 8.5% of total U.S. federal government spending annually (https://www.cbo.gov/publication/45278).

According to the UN and other experts, at least 25% of government money spent in fragile states is illicitly diverted into the hands of U.S. enemies (https://globalecco.org/kirk-meyer-former-director-of-the-afghan-threat-finance-cell). For a country such as Afghanistan, where the U.S. has been engaged in military operations for over a decade, these diversions could amount to as much as $28 billion (https://www.sigar.mil/pdf/budget/FiscalYearBudget.pdf) of the amount the U.S. government has spent in the country since 2002.

"Criminals who are ripping off public budgets need to hide what they are up to. Anonymously-owned companies, or those whose owners are hidden, have proven to be a common facilitator of waste, fraud and abuse in government spending."

Eryn Schornick. Policy Advisor. Global Witness

*Hidden Menace (https://www.globalwitness.org/documents/18532/Briefing_-_Hidden_Menace_-_12072016.pdf)* shows that this massive theft of funds has been possible in part because of the lack of information about the ultimate owners of companies (often called 'beneficial owners') bidding for federal funds. This threatens the safety, security and well-being of people around the world, including in America. Yet, the U.S. is the easiest place (http://www.globalshellgames.com/) in the world to set up an anonymously-owned company. It is also one of the most popular places (http://star.worldbank.org/star/publication/puppet-masters) for corrupt government officials to create anonymously-owned companies to move ill-gotten gains through our financial system.

To fix this problem, Global Witness is calling for the Obama Administration to increase contract transparency through an open contracting system that includes a requirement for bidders to disclose who really owns or controls their companies. This information, along with awards and contracts, should be made public so that the government and businesses know who they are dealing with. Moreover, Congress should collect beneficial ownership information for American companies and put it into the public domain for all to see. All companies should publicly disclose who ultimately owns and controls them as an expression of business integrity and ethics.

## CONTACTS

Andy Stepanian, *US Communications*
andy@sparrowmedia.net (mailto:andy@sparrowmedia.net)
+1 631.291.3010

General/out of hours media enquiries
media@globalwitness.org (mailto:media@globalwitness.org)
+44 (0) 7912517127

**"HIDDEN IN PLAIN SIGHT—HOW CORPORATE SECRECY FACILITATES HUMAN TRAFFICKING IN ILLICIT MASSAGE PARLORS", POLARIS**

Polaris freedom happens now.

# Hidden in Plain Sight

## *How Corporate Secrecy Facilitates Human Trafficking in Illicit Massage Parlors*

Illicit massage businesses, commonly known as "massage parlors," have been ubiquitous in the American landscape for decades. Today, new research finds an estimated 9,000-plus of these businesses are operating in every state in the country, with earnings totaling nearly $2.5 billion a year across the industry.[1] These businesses dot the sides of highways and are tucked into suburban strip malls between fast food restaurants and dollar stores and behind darkened windows in storefronts in some of America's biggest cities. There may be women who choose to sell sex either along with or under the guise of massage therapy, but evidence suggests that behind these bland facades, many of the thousands of women engaging in commercial sex in illicit massage parlors are victims of human trafficking. And for the most part, thanks to corporate secrecy, their traffickers cannot be traced.

### About massage parlor trafficking

Contrary to popular portrayals, human trafficking does not always or even often involve force or the threat of force.

To be considered sex trafficking in any venue, a situation must include one of the following:

- **Force:** Violence or the threat of violence
- **Fraud:** Such as deceitful recruitment practices or fraudulent debt accumulation
- **Coercion:** Including emotional manipulation, document confiscation, or threats using legal processes like deportation

Labor trafficking is defined as force, restraint, threats of harm, abuse or threatened abuse of the legal system, or any scheme, plan, or pattern intended to cause the person to believe that if they did not perform labor, they would suffer serious harm or restraint.[2]

The victims of massage parlor trafficking in the United States almost all:

- Recently arrived from China or South Korea
- Carry debts or are otherwise under extreme financial pressure
- Speak little or no English
- Have no more than a high school education
- Are mothers in their mid 30s to late 50s

Force is rarely an element of massage parlor trafficking. Instead, victims are controlled by traffickers through a complex mixture of cultural manipulation, fraud, and coercion. Key among these are telling the women that the police are in the pockets of the traffickers and will simply arrest them, that the rest of society views the women as worthless, and that they have no real options but to stay at the massage parlor and do what the traffickers say.

1 Keyhan, Rochelle et al, "Trafficking in Illicit Massage Businesses." Polaris, (January 17, 2018)
2 U.S. Code Chapt. 77 Peonage, Slavery and Trafficking in Persons. http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter77&edition=prelim

## Illicit Massage Parlors and Corporate Secrecy

What is unique about this form of trafficking is that massage parlor traffickers actually go through the process of registering their businesses as if they were legitimate.

Conceivably then, it should be relatively simple to determine the basics about these businesses — such as what products or services they provide and who ultimately controls and makes money from the business. The actual or "beneficial" owner would then in most cases be the trafficker and could be prosecuted as such.

In reality, the laws governing business registration are almost tailor-made for massage parlor traffickers to hide behind. Neither states nor the federal government require people setting up companies to include the name of the actual owner of the business in the registration paperwork. What is actually required depends on the jurisdiction. Sometimes the owner's name is left blank. Sometimes it is filled in with the name of a registered agent or someone else paid to be the front person or point of contact. Sometimes the business is registered under the name of an anonymous shell company — another business that exists in name only but has no actual assets.[3] All of this obfuscation is perfectly legal.

*In reality, the laws governing business registration are almost tailor-made for massage parlor traffickers to hide behind.*

The figure of 9,000 illicit massage businesses operating across the country, first reported in Polaris's recently released report, "Human Trafficking in Illicit Massage Businesses," was difficult to come by because of these lax or nonexistent corporate transparency laws. It took extensive research, including cross-referencing publicly available datasets with websites on which commercial sex purchasers leave reviews of their sexual experiences at these illicit businesses, to arrive at this minimum figure.

It is hard to escape the irony here: Someone looking to purchase commercial sex from an illicit massage parlor can log in to any number of review boards and, sometimes for a small fee, get graphic descriptions of individual women's bodies and specific sexual experiences with those women. Meanwhile, while the businesses themselves are easy to find, the privacy of the actual owners of the businesses where these sexual acts take place is scrupulously protected by U.S. law.

Irony aside, the fact that the United States is among the easiest country in the world in which to hide who actually owns and benefits from a business[4] is part of the reason why massage parlor trafficking is so difficult to prosecute criminally. There are legitimate reasons why some businesses use anonymous shell companies and there is no reason why they cannot continue to do so. But if we are to end human trafficking in massage parlors, we must begin by lifting the veil of secrecy that protects the criminals who profit from it.

3 Staff, I. (2003, November 26). Shell Corporation. *Investopedia*. Retrieved from http://www.investopedia.com/terms/s/shellcorporation.asp#ixzz4vFwXidD

4 Findley, Michael et al. "Global Shell Games: Experiments in Transnational Relations, Crime, and Terrorism." *Cambridge University Press* (March 24, 2014), Page 74. http://bit.ly/2uTLpsQ .

## Who Actually Owns Massage Parlors

Polaris analysts used open-source data[5] to examine over 9,000 illicit massage parlors and their networks across the country to find ownership information.

- Of the more than 6,000 illicit massage businesses for which Polaris found business records, only 28 percent of these illicit massage businesses have an actual person listed on the business registration records at all.
- Only 21 percent of all the business records found for illicit massage parlors actually specifically name the owner — although even in those cases, there is no way to know for sure if that information is legitimate.

## Why corporate transparency matters in massage parlor trafficking

Most illicit massage parlors are part of an organized crime network. Generally, these networks include at least one other illicit massage parlor as well as non-massage venues such as nail salons, restaurants, grocery stores, and cleaners.

Criminal networks are necessary in large part for laundering money from the illicit massage parlors. These businesses generally operate out in the open, paying taxes and otherwise taking steps to avoid drawing attention to the true nature of the operation. A hallmark of an illicit massage business is that it advertises services at significantly lower rates than is the standard. For example, an illicit massage parlor will charge $40 for a one hour massage in a jurisdiction where a therapeutic massage performed by a licensed massage practitioner averages between $80 and $100 an hour. Of course, the $40 advertised price is just a baseline price. The real price is negotiated and paid based on the specific sexual act requested and performed.

A tax auditor would notice the discrepancy between what the business charges and the far higher amount the business actually brings in. To avoid detection, the business owner spreads the suspicious profits out to other businesses in the network.

**If the businesses were all registered under the name of the person who actually owned them — for example, "John Q. Smith," the connections would be clear and the money laundering operations obvious.** Because many of the businesses are registered anonymously, as shell companies ("Massage LLC" for example), or in the name of someone other than the actual owner, these connections are often missed, along with the opportunity to prosecute and shut down these human trafficking venues.

Historically, victims of massage parlor trafficking have been the main target of law enforcement activity, while the owners of the businesses — the traffickers — fly under the radar. Typical law enforcement activity around illicit massage parlors has involved raids in which officers sweep into the facility and arrest everyone on the premises. These raids are highly unlikely to net the actual owners of the businesses, as they are rarely on site or even necessarily involved in the day-to-day operations of the massage venues. That is left to managers (often referred to as "mamasan"), and sometimes a manager-in-training (someone who is still primarily selling sex, but who has begun assisting management in controlling victims).

Raids focusing on employees are antithetical to efforts to shut down human trafficking. First of all, vice raids don't do much to slow profits from these businesses. If a single venue in a criminal network is shut down, the trafficker is still pulling in profits from the other venues, and can simply

5 For a full list of open-source data used, please see methodologies section of full report at https://polarisproject.org/massage-parlor-trafficking

transfer the victims to another massage parlor. Rotating victims between businesses in the network, or within other networks in sharing agreements, is routine in massage parlor trafficking. This rotation process keeps the victims disoriented and makes them therefore easier to control while also ensuring buyers at a particular location have a steady supply of new women to choose from. On average, traffickers rotate victims between the businesses every 2-6 weeks.[6]

The frequent arrests of victims — not owners — strengthens the traffickers hold on the women, demonstrating their power while underlining the vulnerability of the victims they control and rotate at will. The traffickers routinely tell the women under their control that they have no options for seeking assistance once they become involved in the massage parlor world. They are told that police see them as prostitutes, not as victims, that they are considered trash, and that no one will help them out of their situations. When the women are then swept up in police raids, the traffickers are proven right.

To effectively and sustainably target massage parlor trafficking, law enforcement must undertake organized crime investigations, which focus on ownership by looking into money laundering or tax evasion. This would shut down entire networks, meaning that the women could not simply be moved around until the police interest had calmed down. Such prosecutions would not only punish perpetrators, but also send a strong signal that human trafficking in massage parlors is no longer a low-risk, high-profit venture, as it is widely seen today. Flipping the perception of the risk versus the reward of human trafficking in these and other venues is key to ending the proliferation of the crime.

Unfortunately, the ability of businesses to obscure ownership and therefore network ties, makes it incredibly time-consuming and resource-intensive, and sometimes impossible, for law enforcement to undertake such investigations.

CASE STUDY

### San Francisco Spa Obscures Ownership[7]

Shell companies are intended to make it difficult to discover true business ownership. One spa in San Francisco, CA, provides a good example of how confusing a purposely obscured business organization can be. The phone number and address for the spa, listed on the massage parlor review site RubMaps, also belong to a business bearing an individual's name. That business is classified under the Standard Industrial Classification: Religious Organizations (pretty unusual for a religious organization to be linked to a spa!). And it isn't the only linked business. The spa's phone number is also connected to another business in Los Angeles with a name advertising sexual products (classified under Miscellaneous Retail Stores), as well as a residential address in LA.

While there is no listed point of contact for the shell company, the address and phone number are that of the original advertised illicit massage business. The business name is also an alias for the name of the owner of the illicit massage business listed on RubMaps. Having a shell company registered at the same address as an illicit massage business facilitates the movement of illicitly gained funds, and allows the spa to keep its reported annual income under a figure that would raise red flags. Additionally, any income the shell company earns that exceeds the reported annual income can be passed off as donations, and because the spa is registered under Religious Organizations, the business owners can qualify for different tax breaks that normal small businesses do not receive.

7 Keyhan, Rochelle et al, "Trafficking in Illicit Massage Businesses." Polaris, (January 17, 2018)

6 Rotation can vary by geographic region. This figure is based on conversations between Polaris and partner city law enforcement and prosecutors between January 2015 and April 2016. (See Methodology, p. 87 of this report).

## Code Enforcement and Human Trafficking in Massage Parlors


Along with organized crime investigations and prosecutions, the most powerful tools for shutting down massage parlor trafficking are strong state and local civil laws that regulate how the businesses operate. For example, laws that require massage businesses to have front-door entrances can deter customers, who are often accustomed to frequenting illicit massage parlors with rear entrances, if they think they might be seen or noticed entering such an establishment by others in their community.

Enacting and enforcing such laws is among the most effective ways to shut down massage parlor trafficking and incorporation transparency is a necessary element. It is difficult to enforce civil code if the enforcing agency cannot identify the person who is actually responsible for paying a fine, or remediating a building issue.

Also worth nothing is that effective enforcement requires that businesses actually register that they are, in fact, massage businesses. Today, massage parlors can — and do — register as nail salons, modeling studios — whatever they want. This dishonest self-classification allows them to avoid regulations that would make it difficult for them to conduct illicit business.

For example, in Houston, many illicit massage parlors registered as modeling studios until the city rewrote its local ordinance to close this loophole.[8] In particularly egregious cases, traffickers register under unrelated industries such as religious organizations or educational institutions, making them eligible for tax breaks.

Again, it is hard to enforce rules requiring honest and accuracy in business registration if there is not a human being responsible for the business that anyone can find and hold accountable.

Unfortunately, even after a city or county closes the loopholes in its ordinance, traffickers have options. They can — and do — simply move to the next town over, where the regulations are still lax. Preventing regulation shopping will take a concerted, nationwide effort at the state and local level.

8 Massage Establishment Ordinance « Human Trafficking Houston. (n.d.). Retrieved November 12, 2017, from http://humantraffickinghouston.org/toolkits/massage-establishment-ordinance-toolkit/

## Recommendations

Requiring transparency around business ownership for law enforcement purposes is key to ending traffickers' ability to hide their networks and cash flow.

Both state and federal laws should:

- **Require businesses to register official operators and primary owners** (aka as the beneficial owner, partner, etc.), all of whom should be required to provide a valid phone number and address and a unique identifying number from a non-expired U.S. passport, a non-expired U.S. state identification card or driver's license, or a non-expired passport issued by a foreign government.
- **Require that covered entities file annual reports of beneficial owners** and provide updates to the government within 60 days of any change in the name or other information previously disclosed about a beneficial owner or in the list of people who are beneficial owners.
- **Provide state, local and federal law enforcement** with direct access to this information
- **Impose criminal and civil liability for failure to report** beneficial ownership information.
- **Hold the official operator listed on all registration records legally liable** for the business, unless it can be confirmed that the listed operator is a victim who was compelled to list herself as an operator.

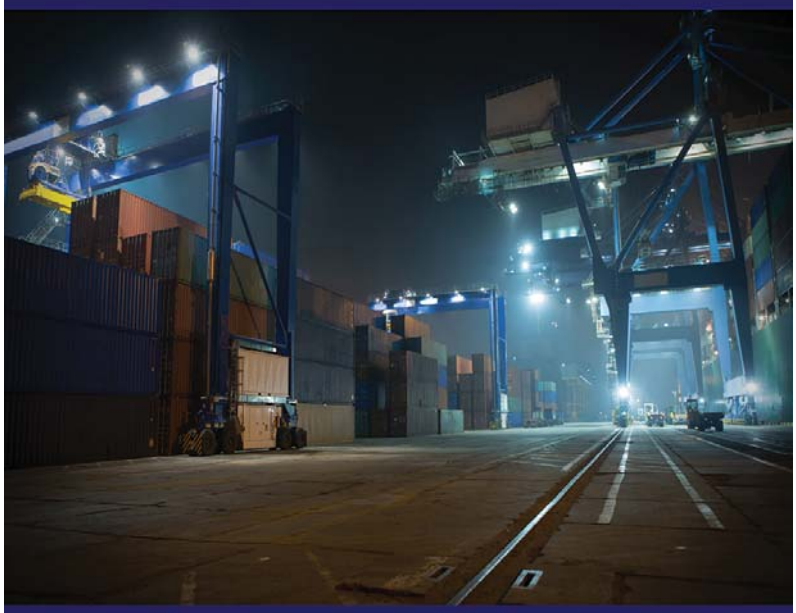
The U.S. Congress is currently considering several bipartisan pieces of legislation that meet these standards.[9]

Pending proposals differ on how information on beneficial ownership would be collected and stored. Options include having states collect the information or putting the responsibility on FinCen, the Financial Crimes Enforcement Network, a bureau of the U.S. Department of the Treasury. There are pros and cons to each approach. States already have forms for corporate registration so the transition would be somewhat smoother. The FinCEN approach would house all the information in a single place, which could potentially make it easier for law enforcement to access in a timely manner.

With comprehensive federal legislation setting the standards for incorporation by which federal laws and tax liability are applied, state and local law enforcement investigating massage parlor trafficking networks will have the ability to more easily follow the money and build strong organized crime cases. And most importantly, traffickers will no longer have the strong incentive of a system that allows them to obscure their illicit activities.

9 Legislation pending as of 4/1/2018 that meets these standards includes H.R.3089, introduced 6/28/2017 by Reps. Carolyn Maloney (D-N.Y.) and Pete King (R-N.Y.) and S.1454, introduced 2/6/2018 by Sens. Sheldon Whitehouse (D-R.I.) and Chuck Grassley (R-IA)

**"ANONYMOUS COMPANIES HELP FINANCE ILLICIT COMMERCE AND HARM AMERICAN BUSINESSES AND CITIZEN", FACT COALITION**



# Anonymous Companies Help Finance Illicit Commerce and Harm American Businesses and Citizens

*A Need for Incorporation Transparency*

By David M. Luna

May 2019

FACTCOALITION

Financial Accountability & Corporate Transparency

# Anonymous Companies Help Finance Illicit Commerce and Harm American Businesses and Citizens

*A Need for Incorporation Transparency*

FACTCOALITION
Financial Accountability & Corporate Transparency

*May 2019*

By David M. Luna

## *Acknowledgements*

The FACT Coalition would like to thank the Ford Foundation for supporting this report.

The FACT Coalition would also like to thank Amie Breslow, Dr. Chris Corpora (Mercyhurst University), Tyler Crowe (Motion Picture Association of America), Mark Hays (Global Witness), Lakshmi Kumar (Global Financial Integrity), Jane Ley, Jack Radisch (OECD), Alexandria Robins (Global Witness), Richard Sawaya (National Foreign Trade Council), Steven J. Shapiro (Federal Bureau of Investigation, National Intellectual Property Rights Coordination Center), Dr. Louise Shelley (George Mason University), Piotr Stryszowski (OECD), and Kelsey Wallace for their contributions to the report.

**Cover Image Sources:** Alexey Lesik / Shutterstock.
**Cover Image Copyright:** All Rights Reserved.
**Cover Design**: Clark Gascoigne and Jacob Wills, The FACT Coalition



Founded in 2011, the Financial Accountability and Corporate Transparency (FACT) Coalition is a non-partisan alliance of more than 100 state, national, and international organizations working toward a fair tax system that addresses the challenges of a global economy and promoting policies to combat the harmful impacts of corrupt financial practices. More information about the coalition can be found at the back of this report or on the FACT Coalition website at www.thefactcoalition.org.

# Table of Contents

## Executive Summary

Illicit commerce remains the lifeblood of today's bad actors, criminal organizations, and terrorist groups. A very profitable illicit activity for many of today's criminals and illicit networks is their involvement in the trafficking and smuggling of counterfeit and pirated goods.

In the United States, there are enormous threats posed by counterfeits and internet pirates — impacting legitimate commerce, markets, and financial systems, including critical national industries and local economies, placing consumers at risk, and harming the market reputational value of American brands and companies.

- The OECD and European Union Intellectual Property Office (EU IPO) estimated the value of imported fakes worldwide at US$509 billion in 2016, or up to 3.3 percent of world trade.
- In a 2017 report by the International Chamber of Commerce's Business Action to Stop Counterfeiting and Piracy (BASCAP) and the International Trademark Association (INTA), it is projected that the global economic value of counterfeit and pirated goods alone will reach close to US$3 trillion by 2022. It is expected that the total employment losses globally due to counterfeiting and piracy will rise from 2 to 2.6 million jobs lost in 2013 to 4.2 to 5.4 million jobs lost in 2022.
- A recent report by Cybersecurity Ventures estimates that the financial costs from cybercrime will double from US$3 trillion in 2015 to US$6 trillion by 2021.

From recent scandals to successful criminal prosecutions, we have gleaned sharper insights into how criminal networks evade detection and how dirty money is hidden — through the use of anonymous shell and front companies. A few summaries of the cases outlined in this Report's Section V include the following:

- Anonymous companies have helped criminals across the United States sell in recent years several billion dollars in fake and counterfeited luxury handbags and apparel accessories branded as Burberry, Louis Vuitton, Gucci, Fendi, Coach, and Chanel, as well as sportswear and gear from the NFL, NBA, and MLB including Nike, Adidas, and Under Armour, among many others.
- Anonymous companies were used to import and sell to American consumers, through internet pharmacies, counterfeit medicines from India and China worth hundreds of millions of dollars. These counterfeits included fake versions of Arimidex, a breast cancer treatment, Lipitor, the cholesterol drug, Diovan, for high blood pressure, and other medications such as illicit OxyContin, Percocet, Ritalin, Xanax, Valium, and NS Ambien.
- Anonymous companies assisted in selling knock-off parts to the Pentagon that have cost the US military tens of millions of dollars.
- Anonymous companies helped an organized criminal network sell counterfeit cellphones and cellphone accessories on Amazon.com and eBay.com. They also misrepresented goods worth millions of dollars as new and genuine Apple and Samsung products.
- Anonymous companies were leveraged to help criminals sell millions of dollars' worth of counterfeit computer anti-virus software over the internet.

vi

- Anonymous companies assisted in selling Venezuelan oil, false securities, and fraudulent contractual relationships in the United States that have cost American businesses millions of dollars.

As a direct consequence, the use of such anonymous companies impacts the economic and financial interests of US companies and markets, as criminals and counterfeiters expand their market share of fake products across American cities and on-line markets.

> *Anonymous companies created by criminals help to finance the distribution of harmful counterfeits across the US economy that seriously harm and even kill Americans — from illicit opioids and fake medicines, food, and alcohol to fake parts in cars and airplanes to counterfeited apparel and toys that are sometimes made with deadly chemicals and toxic materials.*

There is a global trend toward transparency.

- The United Kingdom now has a public registry that includes the names of the beneficial owners of companies formed in the country. They have recently passed a law to require its overseas territories (i.e. Anguilla, Bermuda, British Virgin Islands, Cayman Islands, Gibraltar, Montserrat, and Turks and Caicos Islands) to create public registers as well.
- The European Union has adopted new rules to require all member nations to establish public registers of beneficial owners by 2020. In addition to the 28 members of the EU, this also effectively extends to members of the European Economic Area (Norway, Iceland, and Liechtenstein).
- Additional nations and jurisdictions that have enacted or are pursuing enactment of beneficial ownership registration laws include: Afghanistan, Brazil, Costa Rica, Curacao, Dominican Republic, Ghana, Guernsey, Isle of Man, Jersey, Nigeria, South Africa, Ukraine, and Uruguay.

## *Top Recommendations: End Abuse of Anonymous Shell Companies*

### 1. Enact Legislation to Require Beneficial Ownership Disclosure

The United States Congress must pass legislation to end the abuse of anonymous shell companies by requiring the collection of "beneficial ownership" information — the natural person who controls the entity and has an entitlement to the funds — at the point of corporate formation. The legislation should ensure that federal, state, and local law enforcement agencies as well as those with anti-money laundering responsibilities in the private sector have full access to the information. Foreign law enforcement should also have appropriate access to the beneficial ownership information.

### 2. Require Beneficial Ownership Disclosure from Government Contractors

Either Congress or the administration should require bidders for federal contracts, sub-contracts, and grants to disclose their beneficial ownership information at the time of their bids, as a means to ensure that counterfeiters, fraudsters, sanctioned individuals, and other criminals are neither able to undercut bids from honest businesses nor receive taxpayer money.

# I. Introduction

The global illegal economy is booming, financed by trillions of dollars being generated every year by kleptocrats, organized criminals, terrorists, and other threat networks. Illicit commerce remains the lifeblood of today's bad actors, criminal organizations, and terrorist groups. Through dirty money derived from criminal activities and illicit commerce, these malefactors finance their illicit empires to foment greater criminality, chaos, insecurity, and violence around the world.

In the United States, the threats posed by counterfeits and internet pirates harm legitimate commerce, markets, and financial systems including critical national industries, regional and local economies, and the reputational values of American brands and companies.

These threats also put the safety and health of all Americans in danger when criminals put counterfeit medicines, food, automotive and airplane parts, toys, apparel, footwear, pirated film and television content, and fast-moving consumer goods (FMCG) into our distribution networks and supply chains — including pharmacies, workplaces, hospitals, schools, cars, airlines, grocery stores, restaurants, retailers, and online marketplaces.

> **"In too many places around the world, criminals have built their illicit empires on dirty money and laundered funds that are used to infiltrate and corrupt government institutions. In this shadowy, illegal economy traffickers and narcotics kingpins act as CEOs and venture capitalists to finance instability, jeopardize public health and safety, emaciate communities' human capital, erode our collective security, and destabilize fragile governments."**
>
> — David M. Luna
> Former Chair, OECD Task Force on Countering Illicit Trade;
> Former Senior Director for National Security & Diplomacy, Bureau of International Narcotics and Law Enforcement Affairs, US Department of State

As criminal entrepreneurs profit from American creativity and innovation and help grow the illegal economy, so also grows the need for them to launder their illicit wealth through reinvestments into the legitimate economy. From the recent scandals related to the Panama Papers to the successful criminal prosecutions against organized crime, the public has gained insights into the nefarious use of anonymous companies, both foreign and domestic, for such purposes that have further fueled corruption, fraud, organized crime, and terrorism in many parts of the world.

Left unchecked, and without urgent responses, the criminal infiltration and penetration into the American economy imperils the integrity of public and private institutions, supply chains, businesses, communities, and the physical welfare of people across the country.

The continued abuse of anonymous companies, financial safe havens, and US banks by corrupt officials, criminals, counterfeiters, money launderers, and terrorists are converging harms that endanger US economic and national security and damage American interests globally.

## II. Background: Current Threat Landscapes

### *A. Dark Commerce: A Booming Illegal Economy*

While there have been benefits to globalization, it has also provided opportunities for criminals, their supporting facilitators, and their networks to expand their corruptive influence. The scale of illicit operations directly impacts the US and other global economies. The growth of the illegal economy distorts markets, disrupts communities, and harms individual people around the world.

> "In this new world of dark commerce, which benefits states and diverse participants, trade is impersonal and anonymized, and vast profits are made in short periods with limited accountability to sellers, intermediaries, and purchasers.... [N]ew technology, communications, and globalizations fuel the exponential growth of dangerous forms of illegal trade."[1]
>
> — Dr. Louise I. Shelley
> Nancy Hirst Endowed Chair and University Professor, Schar School of Policy and Government, George Mason University, and Director, Terrorism, Transnational Crime and Corruption Center (TraCCC)

From the coca and opium poppy fields of Colombia and Peru, Afghanistan, and Southeast Asia to the counterfeit producers in China, India, and Paraguay; from arms dealers in Africa to the Free Trade Zones (FTZs) in Panama and the United Arab Emirates (UAE); and across illicit financial hubs throughout North America and Europe, kleptocrats, drug cartels, criminal syndicates, and terrorist networks launder and move their dirty money through the US and global financial system.[3] They also navigate trade superhighways that meet an insatiable demand for narcotics, contraband, and an array of illicit goods that meet consumers' appetites and serve thriving illicit markets around the world.

*Figure 1: Estimated Global Illegal Trade, Corruption, and Illicit Markets.*[2]

| CRIMES | Estimated Annual Dollar Value |
|---|---|
| Money Laundering | At least $2.6 trillion (between 2 and 5 percent of world GDP) |
| Transnational Crime | $1.6 trillion to $2.2 trillion |
| Bribery | Significant portion of $1 trillion |
| Narcotics Trafficking | $750 billion to $1 trillion |
| Counterfeited and Pirated Products | $500 billion to $1 trillion |
| Environmental Crime (illegal wildlife trade, logging, IUU Fishing, trade in CFCs, and toxic waste) | $91 billion to $258 billion |
| Human Trafficking/Modern Slavery | Up to $150 billion |
| Illegal Tobacco | $40 to $50 billion |
| Illegal Mining | $12 to $48 billion |

*Source: World Economic Forum, World Bank, UNODC, OECD, ILO, GFI*

4

The most alarming part of today's dark commerce is not only the staggering amount of illicit wealth that is being created[4], but the growth rate of illicit trade. A 2017 joint study commissioned by the International Trademark Association (INTA) and the International Chamber of Commerce's Business Action to Stop Counterfeiting and Piracy (BASCAP) found that the market for counterfeit and pirated goods is expected to double within five years.[5]

Determining the scale of both the illicit trade and the amount of money that is being laundered and hidden behind anonymous companies is a complex exercise. Specific data sets are generally only snapshots of any given period of time. However, according to the World Economic Forum (WEF), the global value of illicit trade and transnational criminal activities is estimated at between 8 percent to 15 percent of Gross Domestic Product (GDP).[6]

*According to the World Economic Forum (WEF), the global value of illicit trade and transnational criminal activities is estimated at between 8 percent to 15 percent of Gross Domestic Product (GDP).*[7]

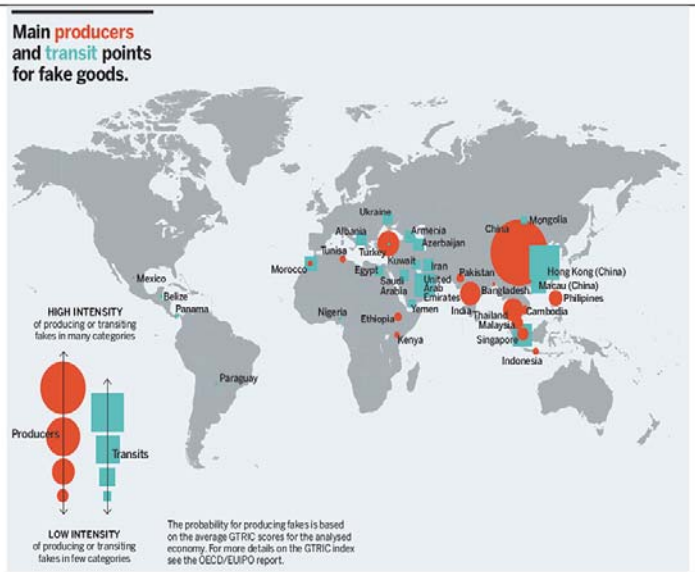
In 2017, the World Bank projected the World's GDP at US$80 trillion.[8] Even if we take the conservative 8 percent estimate from above, it is fair to assume that today's global illicit markets generate several trillions of dollars every year for transnational criminal organizations, complicit corrupt facilitators, and other illicit networks. The types of criminal activities involve the trafficking of narcotics, arms, humans, counterfeit and pirated goods, and illegal tobacco and alcohol; illegally-harvested timber, wildlife, and fish; pillaged oil, diamonds, gold, and other natural resources and precious minerals; stolen antiquities; pirated film and television content; and other illicit commodities and contraband.[9]

Corruption and money laundering currently provide several trillions of dollars to the global illegal economy that enable illicit networks to corrupt critical institutions and enforcement systems, undermining the rule of law and exacerbating an already dire security situation in many parts of the world.

In a March 2019 report by the Organization for Economic Cooperation and Development's (OECD) Task Force on Countering Illicit Trade, "Trends in Trade in Counterfeit and Pirated Goods", the OECD and European Union Intellectual Property Office (EUIPO) estimated the value of imported fakes worldwide at US$509 billion in 2016, or up to 3.3 percent of the global trade in goods.[10]

*The OECD and European Union Intellectual Property Office (EUIPO) estimated the value of imported fakes worldwide at US$509 billion in 2016, or up to 3.3 percent of the global trade in goods.*[11]

*Figure 2: Main Producers and Transit Points for Fake Goods.*[12]




*Source: Trends in Trade in Counterfeit and Pirated Goods, OECD & EUIPO 2019*

Of this US$509 billion in imported fakes worldwide, the top 10 product categories (See *Figure 4*) in terms of values of fakes in trade were: electronics & electrical equipment (US$138bn); jewelry (US$49.8bn); optical, photographic & medical equipment (US$26.7bn); clothing & textile fabrics (US$24.8bn); footwear (US$13.9bn); toys (US$11.8bn); foodstuff (US$6.1bn); leather, handbags (US$8.5bn); perfumery and cosmetics (US$5.4bn); and watches (US$4.2bn).[13]

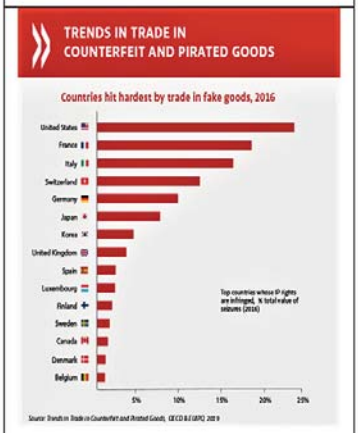
The joint analyses by the OECD and EUIPO showed that China is the top producer of counterfeit goods in nine out of ten product categories, while Hong Kong (China), Singapore, and the United Arab Emirates are global transit hubs for the trade in counterfeit goods (See *Figure 2*).[14]

Brands suffering the most from counterfeiting were largely from OECD and EU member countries with US companies at the top of the list (See *Figure 3*).[15]

*Brands suffering the most from counterfeiting were largely from OECD and EU member countries with US companies at the top of the list.*[16]

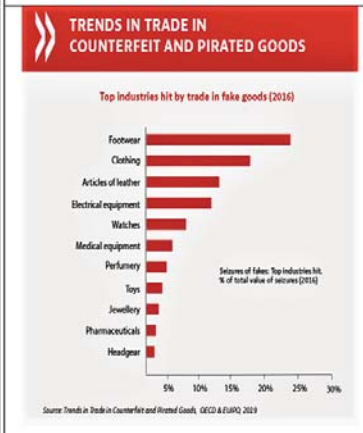
6

*Figure 3: Countries Hit Hardest by Trade in Fake Goods 2016.*[17]




*Source: Trends in Trade in Counterfeit and Pirated Goods, OECD & EUIPO 2019*

*Figure 4: Top Industries Hit by Trade in Fake Goods 2016.*[18]




*Source: Trends in Trade in Counterfeit and Pirated Goods, OECD & EUIPO 2019*

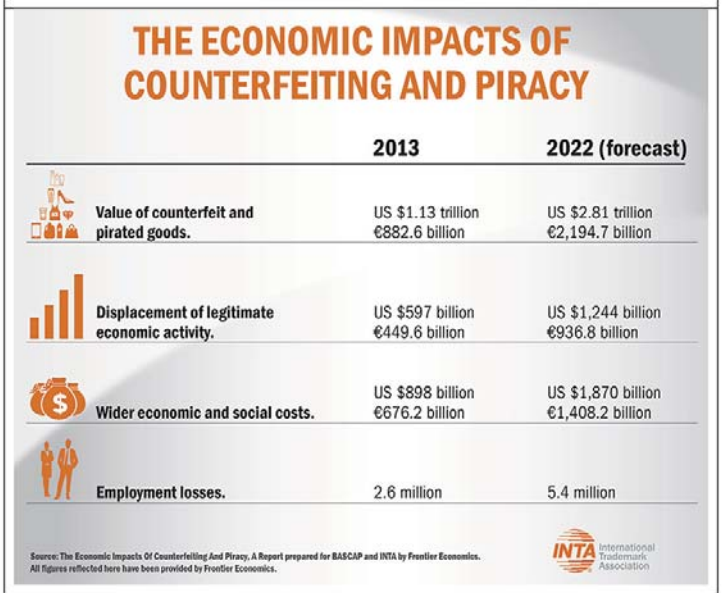
Building on the work of the OECD Task Force, the 2017 joint report by BASCAP and the INTA, it is projected that the global economic value of counterfeit and pirated goods alone will reach close to US$3 trillion by 2022 (See *Figure 5*).[19]

It is estimated that the total economic and social costs due to counterfeiting and piracy worldwide stood at US$737 billion to US$898 billion in 2013 and are expected to rise to US$1.54 trillion to US$1.87 trillion by 2022, suggesting an approximate increase of 108 percent (See *Figure 5*).[20]

> *The total economic and social costs due to counterfeiting and piracy worldwide stood at US$737 billion to US$898 billion in 2013 and are expected to rise to US$1.54 trillion to US$1.87 trillion by 2022, suggesting an approximate increase of 108 percent.*[21]

It is also expected that the total employment losses globally due to counterfeiting and piracy will rise from 2 to 2.6 million jobs lost in 2013 to 4.2 to 5.4 million jobs lost in 2022 (See *Figure 5*).[22]

*Figure 5: The Economic Impacts of Counterfeiting and Piracy.*[23]




*Source: The Economic Impacts of Counterfeiting and Piracy. A report prepared for BASCAP and INTA by Frontier Economics.*

## B. The Growing Threat of Illicit Markets Concerning Counterfeit and Pirated Goods

As in other parts of the world, dangerous contraband and counterfeits exact a heavy toll on the safety and health of Americans.

The use of such anonymous companies impacts the economic and financial interests of US businesses and markets, as criminals and counterfeiters expand their market share of fake products across American cities and online markets. [25] While tens of millions of fakes do real damage to companies financially, tens of thousands of fakes have caused grave physical and health injuries to countless American citizens — and many more globally. In the process of laundering illicit funds, opaque corporate vehicles have helped to inflate real estate prices and hollow out neighborhoods, hurting local businesses and forcing working families to live farther away from their jobs.[26]

Illegal goods such as illicit opioids, illegally mislabeled or contaminated "fake" foods[27] (e.g. Italian olives painted with copper sulphate solution, Sudanese sugar tainted with fertilizer, or chemically-doused seafood), falsified medicines, and toxic goods are harming and killing tens of thousands of people every year.[28]

> "Criminals and terrorists have always used anonymous shell companies to finance their operations, because they never have to disclose who actually owns these shell companies. There is no way for law enforcement to figure out who is involved in the transaction conducted by a shell company. Law enforcement tells me that whenever they're following the money in an investigation, they always hit a dead end at an anonymous shell company. They can't figure out who is behind it so they can't follow the money any further."[24]
>
> — Representative Carolyn B. Maloney New York's 12th Congressional District

The alarming rise in fake products is occurring in a range of industries: from consumer goods that have an impact on public health and safety (such as pharmaceuticals, food and drink, medical equipment, or toys), to intermediary products (such as machines, spare parts, or chemicals), to luxury items (such as fashion apparel or deluxe watches).[29]

Counterfeit medicines alone destroy the lives of adults and children seeking to treat malaria, tuberculosis, heart disease, and other medical conditions. In many of these cases, the fakes either did not contain the right medicinal ingredients or, in other instances, contained high levels of impurities, contaminants, and poisonous chemicals.

Reporting has also shown how online pharmacies are a growing threat. According to the World Health Organization (WHO), more than 50 percent of the medicines purchased over the internet from illegal sites that conceal their physical addresses are counterfeits.[30] Such e-commerce provides criminals the opportunity to easily sell these counterfeit medicines to innocent consumers, without subjecting themselves to any enforcement risks.

*According to the World Health Organization (WHO), more than 50 percent of the medicines purchased over the internet from illegal sites that conceal their physical addresses are counterfeits.*[31]

Unsuspecting consumers can also find themselves at risk for malware from accessing pirated film and television content. According to 2018 data from Carnegie Mellon University, more time spent on sites with infringing content led to an increase in malware on users' computers. Researchers noted, in particular, that the doubling of a user's time on an infringing site accounted for a 20 percent increase in total malware files and a 20 percent increase in malware files after removing potential adware.[32] Without question, malware's effects on consumers and the US economy are vast, including: identity theft, credit card fraud, spam emails, and DDoS attacks.[33]

The risk to consumers has also grown as piracy activities evolve. An April 2019 report from the Digital Citizens Alliance found that growing use of "illicit devices" to stream pirated film and television content brought malware to consumers' doorsteps. Of a DCA survey of 2,073 Americans, 44 percent of respondents that reported using such a device in their home had an issue with malware in the prior 18 months.[34]

The Trump Administration continues to work with the US Congress and a diversity of market stakeholders and communities at the federal, state, and local levels on intellectual property policy, enforcement and protection issues. In advancing future strategies for action, the Trump Administration is committed to promote a robust intellectual property environment that "reduces counterfeiting, copyright piracy, trade secret theft, and patent infringement, and that provides government agencies, rights holders, and other stakeholders with effective legal tools for addressing these illicit activities."[35]

> *"We will stand up to any country that unlawfully forces American companies to transfer their valuable technology as a condition of market access. We will combat the counterfeiting and piracy that destroys American jobs, we will enforce the rules of fair and reciprocal trade that form the foundation of responsible commerce."*[36]
>
> ***President Donald J. Trump***

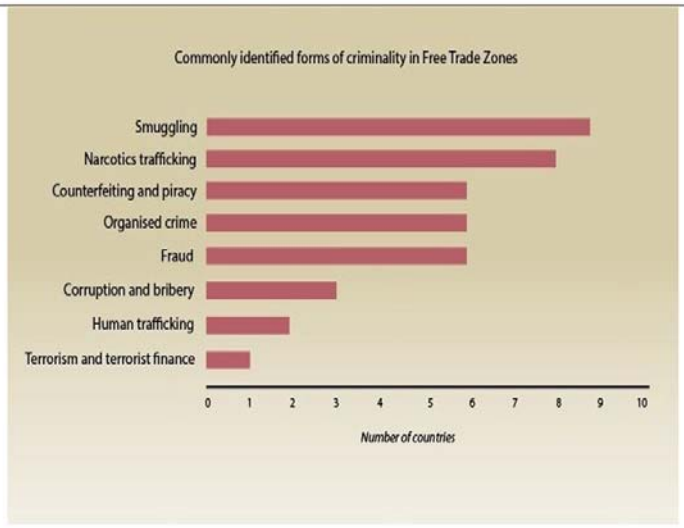
The OECD has conducted numerous, quantitative national case studies on the trade in counterfeits that infringe intellectual property rights of right holders from a given country. These national case studies have provided policymakers not only with reliable, evidence-based information on the overall threat to an economy, but also about its pernicious effects on lost industry profits, tax revenues, and jobs in the analyzed country.

Over the past year, there have been efforts to encourage the US government to work with the OECD on a possible national case study that can help inform numerous diverse communities and market stakeholders on the existing and future harms of counterfeit and pirated goods to American innovation, the health and safety of the American people, harms to US companies and industries, and the security impacts to the American homeland and national interests overseas.

## C. Free Trade Zones (FTZs): Illicit Hubs for Dark Commerce and Hiding Dirty Money

Free Trade Zones can have a catalytic effect on economies, including attracting Foreign Direct Investment and helping to expand economic growth. But in too many parts of the world, FTZs are also exploited on a daily basis by some to facilitate illicit activities that produce broader market reputational harm and put the physical security of many communities in danger (See *Figure 6*).[37]

*Figure 6: Commonly Identified Forms of Criminality in Free Trade Zones.*[38]




*Source: FATF, 2010-in OECD Governance Frameworks to Counter Illicit Trade (2018)*

For example, as reported by the US State Department in the 2018 Country Reports on Terrorism, the free trade zones in Panama and the Tri-Border Area of Argentina, Brazil, and Paraguay remained regional nodes for money laundering and were vulnerable to terrorist financing.[39]

Illicit trade and associated webs of corruption and criminality in one FTZ can have serious ripple effects in other FTZs all around the world. Such connectivity and convergence between the world's various free trade zones help to create a bigger cross-border threat, as various reports have underscored.[40] For example, payments for counterfeit products being trafficked through the United Arab Emirates from China and on to Africa and Europe may eventually wind up in Panama where they then — through anonymous shell companies — help to fund other types of illegal activity, be it more illicit trade, other forms of criminality, or terrorist attacks.[41]

"We must elevate our international efforts across borders to fight illicit trade. A global problem requires a global solution. We continue to support comprehensive anti-illicit trade strategies that focus on more effective law enforcement, actionable intelligence, information-sharing, and public-private partnerships to disrupt black markets and illicit trade flows. Yet even this is not enough. To truly make progress against these criminal enterprises, we must also have stronger legal frameworks to enhance transparency and target the illicitly obtained funds. Anonymous shell companies and unregulated free trade zones serve as vehicles to hide and launder money. They enable criminals to further profit from the booming global illegal economy, destabilizing communities and hindering foreign investment across the globe. It is time to close these criminal loopholes and fix the problem."[42]

– Alvise Giustiniani, Vice President, Illicit Trade Prevention, Philip Morris International

## *D. Counterfeits Exploding in Cyberspace and Online Marketplaces*

The success of Amazon, Alibaba, E-Bay, and many other innovative, internet marketplaces has led to an explosion of millions of online stores.[43] However, as the saying goes: "if you can make it, they can fake it." Shutting an online store that is selling counterfeit products typically leads to criminals opening a new one within hours.[44] This problem is often exacerbated by e-commerce platforms' reticence to verify sellers' identities combined with the ease and speed with which criminals can form new anonymous companies to evade detection. Intellectual property theft is a serious crime that is getting worse every day due to the fast-growing online markets around the world.[45]

The expansion of internet shopping and cybercrime presents a growing threat to companies and consumers alike. E-commerce sales of an array of counterfeit products are distributed through internet, social media websites, and search engines, where there can be hundreds of millions of counterfeit listings online on a daily basis.[46]

A recent report by Cybersecurity Ventures estimates that the financial costs from cybercrime will double from US$3 trillion in 2015 to US$6 trillion by 2021.[47] This report also predicts that there will be 6 billion internet users by 2022 (75 percent of the projected world population of 8 billion) and more than 7.5 billion internet users by 2030 (90 percent of the projected world population of 8.5 billion, 6 years of age and older).[48]

When one couples these statistics with the fact that the global illegal economy is booming and that cybercrime is exploding, one has to be incredibly concerned about the massive convergence threats in the future related to the nexus between cybercrime and intellectual property infringement.

12

## *E. Convergence Crime and Money Laundering Help Multiply Transnational Threats*

What happens in one market impacts many others. One illicit threat spawns many other harms. No country, no region, no community is untouched by the corruptive influence of global crime, exploitative bad actors, and illicit networks. As threat multipliers, such converging threats metastasize and imperil broader economic and national security objectives.

*No country, no region, no community is untouched by the corruptive influence of global crime, exploitative bad actors, and illicit networks.*

This is certainly the case with regard to the use and exploitation of anonymous companies by today's criminals and counterfeiters. As illustrated by the revelations in the 2016 Panama Papers and 2017 Paradise Papers, anonymous companies help finance other crimes and hide the illicit proceeds.[49]

What happened in Panama's financial safe havens has had a ripple effect in other markets and "makes the business of offshore accounts into a sort of global shell game".[50] US Senator Marco Rubio, chairman of a Senate subcommittee that covers transnational crime, noted that anonymous shell companies hurt Americans as criminals fly under the radar of law enforcement and reinvest their dirty monies in real estate.[51]

Unfortunately, without making the fight against anonymous companies a higher priority and requiring the disclosure of beneficial ownership information, current regulatory and legal regimes do not provide the necessary tools for US law enforcement agencies to track, trace, and seize hidden illicit proceeds either within the country, or in other jurisdictions that have a direct harm to American businesses and citizens.

To win the fight against illicit trade, including combatting sophisticated criminal networks and the counterfeit goods that they introduce to the marketplace, we must close the gaps in current laws that enable anonymous incorporation.[52]

"Like any Internet-based venture, the operations of a website dedicated to enabling or promoting online copyright theft would not be possible without the use of a wide spectrum of supporting services. Combating systematic online infringement of copyright requires the active cooperation of all participants in the e-commerce ecosystem, including online advertising players (advertisers, ad agencies, ad networks, and the providers of advertising placement and related services); payment processors; hosting providers (including reverse proxy providers and related optimization services); domain name registrars and registries; and search engines. As entities with a direct stake in a secure and stable Internet, and in the healthy growth of e-commerce (including e-commerce in products and services protected by copyright), cooperation against threats to that security, stability and health is part of a sound business strategy for all Internet intermediaries. Governments in many countries should be doing much more than they are currently to foster and encourage such cooperation, and the development of best practices to advance the common goal of a safer, cleaner online marketplace."[53]

— Steven J. Metalitz, International Intellectual Property Alliance

## III. US Law Enforcement Concerned About the Challenges of Organized Crime Using Anonymous Companies

**Kenneth A. Blanco, Director, Financial Crimes Enforcement Network (FinCEN), US Department of the Treasury:**

> "The misuse of legal entities to disguise illicit activity has been a key vulnerability in the US financial system. Corporate structures have facilitated anonymous access to the financial system for criminal activity and terrorism. Narcotraffickers, proliferation financiers, money launderers, terrorists and other criminals have been able to establish shell companies, which then use accounts at financial institutions, directly or indirectly, without ever having to reveal who ultimately is behind the transactions being facilitated. This has made it difficult for law enforcement to pursue investigative leads, and for financial intelligence units to produce those leads in the first instance. And, just as important, this has made it difficult for financial institutions to apply effective risk-based AML programs."[54]

**M. Kendall Day, Acting Deputy Assistant Attorney General, US Department of Justice:**

> "The pervasive use of front companies, shell companies, nominees, or other means to conceal the true beneficial owners of assets is one of the greatest loopholes in this country's AML regime. Indeed, the Financial Action Task Force (FATF), the inter-governmental body responsible for developing and promoting policies to protect the global financial system against money laundering and other threats, highlighted this issue as one of the most critical gaps in the United States' compliance with FATF standards in its most recent evaluation. FATF noted that the lack of beneficial ownership information can significantly slow investigations because determining the true ownership of bank accounts and other assets often requires that law enforcement undertake a time-consuming and resource-intensive process. For example, investigators may need grand jury subpoenas, witness interviews, or foreign legal assistance to unveil the true ownership structure of shell or front companies associated with serious criminal conduct."[55]

**Steven D'Antuono, Section Chief, Financial Crimes Section, Federal Bureau of Investigation (FBI):**

> "Under our existing regime, corporate structures are formed pursuant to state-level registration requirements, and while states require varying levels of information on the officers, directors, and managers, none requires information regarding the identity of individuals who ultimately own or control legal entities – also known as beneficial ownership – upon formation of these entities... Criminals exploit these gaps for their illicit purposes, often seeking to mask the nature, purpose, or ownership of their accounts and the sources of their income through the use of front companies, shell companies, or nominee accounts... [T]he lack of an obligation to collect beneficial ownership information at the time of company formation is a significant gap. More effective legal frameworks are needed to ensure that criminals cannot hide behind nominees, shell corporations, and other legal structures to frustrate law enforcement, including stronger laws that target individuals who seek to mask the ownership of accounts and sources of funds."[56]

**Cyrus R. Vance Jr., New York County District Attorney:**

> "[O]btaining data on financial transactions can be challenging because our country's lax incorporation laws make it easy for criminals to hide money behind anonymous shell companies and launder it through US and foreign banks and their branches. It is almost a certainty that, at this very moment, a human trafficker, terrorist cell, drug cartel, or [a] corrupt government official is using an anonymous US shell corporation to finance illicit activities. On a near-daily basis we encounter a company or network of companies involved in suspicious activity, but we are unable to glean who is actually controlling and benefiting from those entities, and from their illicit activity. In other words, we cannot identify the criminal because the criminal has used layers of shell companies to frustrate investigators and protect himself from prosecution."[57]

**Dominick L. Stokes, Vice President for Legislative Affairs, Federal Law Enforcement Officers Association (FLEOA):**

> "Suspected terrorists, drug trafficking organizations and other criminal enterprises continue to exploit the anonymity afforded to them through the current corporate filing process in a few states. Hiding behind a registered agent, these criminals are able to incorporate without disclosing who the beneficial owners are for their company(s). This enables them to establish corporate flow – through entities, otherwise known as "shell companies," to facilitate money laundering and narcoterrorist financing. Even through the due process of proper service of a court order, law enforcement officers are unable to determine who the beneficial owners are of these entities. This has to stop. While we fully recognize and respect the privacy concerns of law abiding citizens, we need to install a baseline of checks and balances to deter the criminal exploitation of our corporate filing process."[58]

## IV. How It Works: Laundering Money Through Anonymous Shell Companies

It has become evident that the anonymous company structure is being abused regularly, if not daily. Anonymous companies are exploited by an array of criminals, rogue states, and terrorists to both launder funds from illicit markets to licit ones and mask the true beneficial owners of these corporate structures.[59]

In illicit financial centers that function as offshore hubs of secrecy, professional service facilitators — accountants, incorporators, lawyers, and others — help criminals, corrupt officials, and other bad actors create anonymous companies and other legal structures to hide their funds, launder them into the international banking system, and reinvest them into legitimate commerce and investments.

The International Monetary Fund (IMF) has estimated that money laundering constitutes approximately 2 to 5 percent of the world's gross domestic product (GDP) each year, or approximately US$1.5 trillion to US$3.7 trillion in 2015.[60]

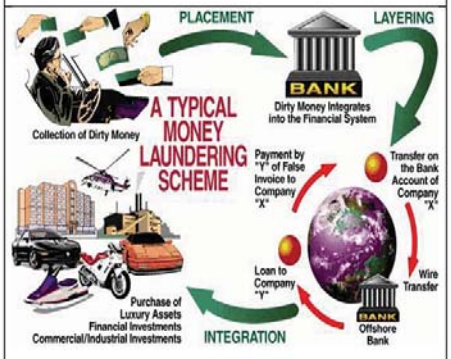
However, to more fully understand the array of harms that anonymous companies can cause in the United States and many other countries, we must first understand how money laundering works at the operational level.

Money laundering is an art form and process by which criminals "disguise the original ownership and control of the proceeds of criminal conduct" by making such criminal proceeds appear to have been "derived from a legitimate source" instead of their illegal origin.[61] In other words, it is the dirty money obtained through an illegal or criminal activity that is then processed through and integrated into the legal monetary market.

According to the United Nations Office on Drugs and Crime (UNODC), money laundering is a dynamic three-stage process (See *Figure 7*).[63] The International Compliance Association (ICA) provides a similar framework.[64] They both agree that the stages are:

- Placement, the stage at which criminally derived funds are introduced into the financial system;
- Layering, the stage of the process in which the funds are disguised ("washed") and its ownership and source is disguised;
- Integration, the final stage at which the "laundered" property is reintroduced and reinvested into the legitimate economy via purchases of real property or luxury assets and an array of investments.

*Figure 7: A Typical Money Laundering Scheme.*[62]




*Source: United Nations Office on Drugs and Crime (UNODC)*

16

According to the US Treasury Department, there are multiple ways to approach each stage to make dirty money appear legal.[65] Within the placement stage, some options allow the illicit funds to be introduced (or "placed") into the financial system through cash deposits, monetary instruments (money orders, value cards, checks), or through casinos.[66] The layering stage is the most elaborate, where money launderers may move "funds electronically from one country to another" through a series of complex illicit-licit financial transactions using multiple overseas accounts and anonymous corporate structures to conceal the illegal source of the funds and elude detection, including through "payments of goods or services, thus giving them a legitimate appearance".[67] The final stage "integration" is then utilized to reintroduce the funds back into the legal economy, and to provide the "clean" cash or value back to the criminal. Such funds are frequently used to buy real property, artwork, yachts, jewelry, vehicles, or other assets.[68]

Money laundering is often difficult to detect due to opaque corporate vehicles that are manipulated and exploited by criminals to hide their dirty money.

These anonymous companies facilitate money laundering through the lack of transparency of beneficial ownership information.[69] The lack of information can be used to disguise the identity of known or suspected criminals, the real purpose of an account or property held by a corporate vehicle, or the source or use of funds or property associated with a corporate vehicle.[70]

A good example of cleaning dirty money, disguising and laundering it, is through trade-based money laundering (TBML). TBML is increasingly leveraged by criminals to launder money, transfer or move value, and avoid paying the requisite tax on goods by under- or over-invoicing the value of goods.[71] In fact, in examining 2013 US trade data, Dr. John Zdanowicz, a TBML expert, estimated that 6 to 9 percent of overall US trade is "tainted by customs fraud and perhaps trade-based money laundering."[72]

In its 2015 National Money Laundering Risk Assessment, the US Department of the Treasury estimated that about US$300 billion in illegally-concealed proceeds is generated annually in the United States alone.[73] That money comes from many sources, including fraud, narcotics-trafficking, international organized crime, foreign corruption and kleptocracy, trade-based money laundering, and other criminal activities.

The Financial Action Task Force (FATF) recently noted in their Mutual Evaluation Report of the United States, regarding Recommendation 24 – transparency and beneficial ownership of legal persons – that the US was non-compliant because it does not require disclosure of beneficial ownership information when a company is formed.[74]

**"Anonymous shell companies have been implicated in a myriad of schemes to launder the proceeds of criminal activity and defraud legitimate businesses and governments around the world. New rules to combat illicit finance have been enacted in many countries but the US does not require the collection of beneficial ownership information."** [75]

– Oliver Bäte, CEO, Allianz;
Josh Bayless, CEO, Virgin Group;
Marc Benioff, Founder, Chairman and CEO, Salesforce;
Andrew Liveris, Chairman and CEO, The Dow Chemical Group;
François-Henri Pinault, CEO and Chairman of the Board of Directors, Kering Group; and
Paul Polman, CEO, Unilever

# V. Case Studies: Anonymous Companies and Illicit Commerce

## *Clear and Present Dangers to Americans*

Most states within the United States remain open to criminals that want to incorporate an anonymous shell company to hide illicit profits.[76] Under many state entity formation laws in the United States, the real owners of companies are not required to be disclosed, thus enabling corporate anonymity. It was recently reported that it requires less information to incorporate an anonymous shell company in the United States than is necessary to obtain a library card – where one provides "far more personal information to a state" than to create a company.[77]

**Obscured Beneficial Ownership:** Increasingly, sophisticated criminals seek access to the US financial system by masking the nature, purpose, or ownership of their accounts and the sources of their income through the use of front companies, shell companies, or nominee accounts with unknown beneficial owners. Front companies typically combine illicit proceeds with lawful proceeds from legitimate business operations, obscuring the source, ownership, and control of the illegal funds. Shell companies typically have no physical operations or assets, and may be used only to hold property rights or financial assets. Nominee-held "funnel accounts" may be used to make structured deposits in multiple geographic locations and corresponding structured withdrawals in other locations. All of these methods obscure the true owners and sources of funds.[78]

*Source: Federal Bureau of Investigation (FBI)*

Over the years, US law enforcement agencies have indicted and prosecuted numerous criminals and counterfeiters for conspiracies to traffic and smuggle counterfeited and pirated goods into the United States for sale on streets across America, the black market, or on the internet and of laundering for their dirty monies through the US financial system. Through a combination of prolonged and difficult investigations, whistleblowers, and — on occasion — luck, the following are a sample of counterfeit and piracy cases that have come to light.

### *Anonymous companies helped an organized criminal network in a multi-million-dollar counterfeit cellphone scheme*

In 2018, ten individuals were indicted in the Federal District of Idaho over a multi-million-dollar fraudulent scheme selling counterfeit cellphones and cellphone accessories that were misrepresented as new and genuine Apple and Samsung products on Amazon.com and eBay.com.[79] The counterfeit cellphones and cellphone accessories were obtained in bulk from manufacturers in Hong Kong, repackaged in Idaho, and then individually resold to consumers online as genuine and new.[80]

### *Anonymous companies helped an organized criminal network import US$300 million in luxury counterfeited goods*

In 2014, several Chinese and US-based individuals pleaded guilty to profiting from the trafficking of counterfeit goods through a series of shell companies based in the United States and Hong Kong.[81] From August 2008 through February 2012, convicted criminals conspired to run an international counterfeit goods smuggling and distribution operation by importing hundreds of containers of counterfeit goods, primarily handbags, footwear, and perfume from China into

the United States.[82] These goods – including counterfeit Nike sneakers and UGG boots; Louis Vuitton, Coach, and Gucci handbags; and cigarettes, among other items – if legitimate, would have had a retail value of more than US$300 million. The conspirators sought help in importing counterfeit goods into the United States and used a corporation to import the goods through Port Newark-Elizabeth Marine Terminal in Elizabeth, New Jersey. This corporation was actually a front company set up by law enforcement to act as an importer. The conspirators imported the counterfeit goods using fraudulent customs paperwork, which, among other things, falsely declared the goods within the containers. To hide the origin of the profits from the sale of fake goods, some of the conspirators laundered the proceeds of counterfeit goods trafficking, the sale of narcotics, and illegal gambling activity through bank accounts opened in China, the United States, and elsewhere.[83]

*Anonymous companies helped criminals sell US$100 million worth of fake luxury handbags and apparel accessories in one of the largest counterfeiting luxury goods cases in US history with criminal associates that sympathized with terrorist groups*

In 2010, criminals from a large organized illicit network were convicted in Virginia by a jury in one of the largest counterfeit goods prosecutions in US history.[84] Defendants were convicted of importing from China more than 300,000 fake luxury handbags and wallets worth more than US$100 million, bearing counterfeit trademarks including those of Burberry, Louis Vuitton, Gucci, Fendi, Coach, Chanel, and other luxury brands.[85] In laundering the proceeds, these criminals created 13 anonymous shell companies shifting money from one entity to another to delay detection.[86] According to the indictment, the criminals "engaged in a corporate shell game whereby they would import counterfeit luxury goods in the name of different corporations using different names. If customs authorities in a US port identified one of their corporations as an importer of counterfeit luxury goods, [the criminals] would continue to import such goods in the same port under a different corporate name. [The criminals] would shift from one shell corporation to another to facilitate their conspiracy to import counterfeit luxury goods."[87] This particular Asian criminal syndicate partnered with at least eight manufacturing plants in China to import and traffic in these counterfeit luxury goods, which were also supplied to smaller operators including some controlled by Hezbollah and Hamas sympathizers.[88]

According to the indictment, the criminals "engaged in a corporate shell game whereby they would import counterfeit luxury goods in the name of different corporations using different names. If customs authorities in a US port identified one of their corporations as an importer of counterfeit luxury goods, [the criminals] would continue to import such goods in the same port under a different corporate name. [The criminals] would shift from one shell corporation to another to facilitate their conspiracy to import counterfeit luxury goods."

*Anonymous companies helped criminals evade US$34M in tobacco taxes*

A three-year investigation exposed systematic and widespread fraud and tax evasion in the distribution of some tobacco products in California. To evade taxes and undercut their competitors (honest, law-abiding companies), illicit distributors set up businesses outside of California, then smuggled tobacco into California using anonymous shell companies to receive the products, false documents to understate the amount of tobacco received, and untraceable cash sales to transfer money.[89]

*Anonymous companies assisted in selling counterfeit parts to the Pentagon*

In 2011, US government agencies awarded 93 contracts worth over US$1.6 million (90 percent from DOD) to individuals that defrauded the Department of Defense. An investigation revealed that Eagle Logistic Solutions and Eagle Logistics Aerospace, two anonymous Wyoming companies registered at the same address, won four contracts worth more than US$50,000, and sold knock-off parts to the Pentagon. In one case, the government found that the firms "knowingly supplied air and fluid-filtering kits for military tractor-trailers between 2001 and 2005 that were reverse-engineered in Turkey to look like they were made by Parker Hannifin, the required manufacturer."[90]

*Anonymous companies assisted in enabling convicted criminals to defraud the US Army on government contracts*

In 2010, several Missouri-based individuals created a shell company to win bids to procure telecommunications and networking equipment for the US Department of Defense (DOD). Instead of providing legitimate equipment to the DOD, this shell company supplied counterfeit products.[91] Convicted criminals defrauded the US Government in a US$1 million wire fraud scheme to sell counterfeit and modified computer equipment to the US Army.[92] After receiving a contract from the Army, Missouri Office Systems and Supplies, Inc. (MOSS) conspired with PRM Technology Equipment LLC, incorporated in North Carolina, to procure and provide more than US$1 million worth of counterfeit computer products from Hong Kong and China and Cisco products that were used and modified post-manufacture, outside of Cisco's authorized distribution channels. The counterfeits were in turn delivered to the US Army Recreation Machine Program (ARMP).[93]

*Anonymous companies assisted in financing an illicit trade in misbranded food that endangered consumers*

In 2017, numerous criminals were indicted for willfully trafficking in counterfeit goods and conspiracy to commit criminal copyright infringement and to introduce 3.7 million bottles of misbranded counterfeit 5-Hour ENERGY into interstate commerce.[94] These unsafe counterfeits put millions of users of this consumer product at risk by endangering their health and safety. Defendants' company Tradeway International Inc., which was doing business as Baja Exporting, LLC in California, sold the counterfeit-labelled product throughout the United States. These counterfeits were manufactured using an unsanitary facility, untrained day workers, and mixed unregulated ingredients in vats in an attempt to mimic the real 5-Hour ENERGY products.[95]

*Anonymous companies assisted in selling Venezuelan oil, false securities, and fraudulent contractual relationships in the United States*

In July 2018, the United States Attorney's Office for the Southern District of Florida indicted 8 individuals with conspiracy to commit criminal racketeering related to a US$1.2 billion international scheme to launder funds embezzled from Venezuelan state-owned oil company, Petróleos de Venezuela, S.A. (PDVSA).[96] Numerous anonymous companies incorporated in the United States were complicit and involved in laundering fraudulent transactions involving the sale of false securities, the sale of high-end real estate, and fraudulent contractual relationships.[97]

*Anonymous companies assisted in the importation and sale of counterfeit medicines from both India and China to American citizens and the transfer of funds from their sale through an internet global pharmacy and other illicit commodities that transited through Free Trade Zones*

Online pharmacy pioneer, Andrew Strempler, was sentenced to 4 years for conspiracy to commit mail fraud after an investigation by the Food and Drug Administration (FDA) found that his internet pharmacy business, RX-North, had

sold counterfeit medicines to American consumers including fake versions of Arimidex, a breast cancer treatment, Lipitor, the cholesterol drug, and Diovan for high blood pressure.[98]

*Anonymous companies assisted in the distribution of US$100 million worth of counterfeit Schedule II, III, and IV controlled substances to internet customers throughout the United States*

From March 2009 to April 2012, Muhammad Aijaz Sarfraz and his co-conspirators operated numerous illegal websites through which they undertook an international counterfeit drug and criminal money laundering operation.[99] The counterfeit pills included popular prescription medications such as OxyContin, Percocet, Adderall, Ritalin, Hydrocodone, Xanax, Valium, Ambien, and others.[100] The counterfeit drugs, which were generally manufactured in China, Singapore, Malaysia, India, Pakistan, and Hong Kong, often contained incorrect active pharmaceutical ingredients or the wrong quantity and dosage strength of those substances. Sarfraz and other conspirators moved their criminally-derived proceeds through a network of banks and shell companies.[101]

*Anonymous companies leveraged to help criminals sell millions of dollars' worth of counterfeit computer anti-virus software over the internet*

In June 2011, US authorities seized nearly US$15 million from a Swiss bank account belonging to fugitive Shaileshkumar "Sam" Jain, who had fled the United States following his indictment in 2008 on federal charges for trafficking and selling millions of dollars' worth of counterfeited Symantec computer goods on various fraudulent internet websites.[102] "To hide the proceeds from his criminal activities, Jain established shell corporations [in the United States] and overseas and opened bank and investment accounts in the United States, Uruguay and Switzerland," according to US law enforcement.[103]

*A transnational criminal network based in Colorado leveraged more than 20 anonymous shell companies to finance a global illicit counterfeiting ring*

In 2017, a Colorado police officer and other criminal defendants were convicted of racketeering, money laundering, and conspiracy for illegally selling counterfeit NFL sports merchandise of the Denver Broncos and other professional and college teams throughout the country.[104] According to US law enforcement officials, the group had imported the fake merchandise from known counterfeiters and exporters located in Hong Kong and mainland China.[105] David A. Thompson, special agent in charge of HSI in Denver, stated that, "This investigation uncovered hundreds of thousands of dollars in money wired to China to finance these counterfeit products and more than 20 shell companies furthering this illegal activity."[106]

*Anonymous companies provide a conduit for criminal networks in West Africa to sell stolen oil internationally and escape accountability*

A report by the London-based think tank Chatham House found that proceeds of stolen oil — and the oil itself — move through anonymous companies to escape accountability. As reported in *The Economist*, "Profits are laundered abroad in financial hubs, including New York, London, Geneva and Singapore. Money is smuggled in cash via middlemen and deposited in shell companies and tax havens... Some of the proceeds—and stolen oil—end up in the Balkans, Brazil, China, Indonesia, Singapore, Thailand, the United States and other parts of west Africa."[107]

## VI. Global Trends in Incorporation Transparency

Around the world, more countries are realizing the looming threats posed by the infiltration of illicit financial flows that empower adversaries and undermine the legitimate economy.[109] In the process of confronting the deluge of dirty money into their economies, numerous jurisdictions are legislating new policies to require corporate entities to disclose the true owners (a.k.a. beneficial owners) who ultimately control an entity and have entitlement to the funds.[110]

> **"I do believe generally [that the Corporate Transparency Act is] headed in the right direction, and I appreciate [Rep. Carolyn Maloney's] work on this. I hope this is something that, on a bipartisan basis, we can get accomplished."[108]**
>
> – Steven T. Mnuchin
> Secretary of the Treasury
> April 9, 2019

Unfortunately, the United States remains a top destination for creating anonymous companies for hiding all sorts of assets and monies.[111] A 2014 report by scholars at the University of Texas-Austin, Brigham Young University, and Griffith University noted that the United States was the easiest jurisdiction in which criminals and terrorists could open anonymous companies to cloak their identities and launder money with few questions asked.[112] Corporate service providers continue to incorporate in the United States with minimal due diligence and no beneficial ownership information.[113]

Greater transparency would empower law enforcement agencies across borders to harness such information to investigate corrupt financial practices and an array of illicit trade harms, including those caused by today's counterfeiting criminal networks.[114]

### *United States (US)*

- The US Department of the Treasury recently extended and expanded to twelve jurisdictions coverage of their Geographic Targeting Orders (GTOs).[115] GTOs require title insurance agents to collect beneficial ownership information for companies engaged in higher cost, cash financed real estate transactions.[116]
- In the Fiscal Year 2018 National Defense Authorization Act, Congress included a provision for the Department of Defense to collect beneficial ownership information of landlords when leasing high security office space.[117]
- In May of 2018, new rules promulgated by the Department of the Treasury through the Financial Crimes Enforcement Network went into effect.[118] They implemented rules requiring banking institutions to collect beneficial ownership information for companies seeking to open accounts.
- In the February 2019 budget agreement, Congress included a provision to direct the US Executive Directors of each international financial institution to vote against loans or other financing for projects unless entities provide beneficial ownership information.[119]
- Congress remains interested in the array of national security dimensions of beneficial ownership information.[120] Such a convergence of national security threats may pave the way for Congress to pass legislation that would require the collection of beneficial ownership information.[121]

22

## United Kingdom (UK)

- In 2016, the United Kingdom became one of the first countries to establish a national registry that publicly disclosed information on the beneficial ownership of companies.[122]
- In 2018, the UK voted to require its Overseas Territories with financial centers — Anguilla, Bermuda, British Virgin Islands, Cayman Islands, Gibraltar, Montserrat, and Turks and Caicos Islands — to implement public registries of beneficial ownership information by the end of 2020.[123]
- The UK Parliament has recently enacted new measures that would empower British law enforcement agencies to investigate criminality in the use of such UK-registered companies, including the leverage of Account Freezing Orders (AFO) to remove dirty money from the UK financial system. In implementing these new AFOs, Donald Toon, director for economic crime at the UK's National Crime Agency (NCA), underscored: "Unexplained wealth orders have the potential to significantly reduce the appeal of the UK as a destination for illicit income. They enable the UK to more effectively target the problem of money laundering through prime real estate in London and elsewhere. We are determined to use all of the powers available to us to combat the flow of illicit monies into, or through, the UK."[124]

## European Union (EU)

- In 2015, the EU agreed that all 28-member states (including the UK) establish national beneficial ownership registries and make that information available to various entities, including financial institutions, to meet customer due diligence requirements.[125]
- In 2018, the European Union required that its member states collect and make public the beneficial ownership information of companies formed within their bloc by 2020.[126]
- These requirements also effectively extend beyond the 28 members of the European Union to also include members of the European Economic Area — Norway, Iceland, and Liechtenstein, which are required to follow all European Union directives in order to remain in the open market.

## Rest of the World

In addition to the UK, the UK Overseas Territories, the EU member states, and the European Economic Area member states, a number of other jurisdictions have enacted beneficial ownership registration laws. They include Brazil, Costa Rica, Curacao, Dominican Republic, Ghana, Guernsey, Isle of Man, Jersey, Ukraine, and Uruguay.

That said, there are an estimated 235 countries, territories, or jurisdictions where companies can be incorporated, according to Global Witness.[127] Only about 6 percent of these jurisdictions have online registries in which some basic company information can be publicly-accessed, and less than 50 percent of these jurisdiction provide additional information, including specific data on directors and shareholders.[128]

In addition to specific efforts by some of the G20 countries noted above, these countries have taken positive steps, but progress has generally been slow in recent years. The majority of G20 members have not taken much action to fully implement their agreed upon commitments to the G20 Beneficial Ownership principles.[129] In Africa and Latin America, several countries appear to be making some progress on beneficial ownership and towards establishing national registries, but much work remains to be done to reach ideal levels of transparency.[130]

## *In Summary*

As of June 2018, 34 jurisdictions have enacted laws requiring the registration of beneficial ownership information. They include: Austria, Belgium, Bermuda, Brazil, British Virgin Islands, Bulgaria, Cayman Islands, Costa Rica, Croatia, Curacao, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Germany, Ghana, Gibraltar, Guernsey, Hungary, Isle of Man, Italy, Jersey, Latvia, Lithuania, Malta, Portugal, Slovenia, Sweden, Turks & Caicos Islands, Ukraine, United Kingdom, and Uruguay. An additional 11 jurisdictions are legally required to implement beneficial ownership registers by 2020. They include Anguilla, Cyprus, Greece, Ireland, Luxembourg, Montserrat, Netherlands, Poland, Romania, Slovakia, and Spain.[132]

**"Beneficial ownership through shell companies has been a [serious] vulnerability to our financial system and an impediment for law enforcement for much too long... We need to have a central repository for beneficial ownership... By collecting beneficial ownership information, and making it available to law enforcement, valuable investigative time will be saved."[131]**

– Dennis M. Lormel,
President & CEO, DML Associates, LLC
Former Chief, Financial Crimes Section, FBI, US Department of Justice

## VII. Recommended Courses of Action

### *1. Enact Legislation to Require Beneficial Ownership Disclosure*

The United States Congress must pass legislation to end the abuse of anonymous companies by requiring the collection of "beneficial ownership" information — the natural person who controls the entity and has an entitlement to the funds — at the point of corporate formation. The information should be updated whenever the ownership changes. The legislation should ensure that federal, state, and local law enforcement agencies as well as those with anti-money laundering responsibilities in the private sector have full access to the information. Foreign law enforcement should also have appropriate access to the beneficial ownership information.

Doing so will enable law enforcement agencies at the international, federal, state, and local levels to more effectively target corrupt financial practices and transnational criminal activities, including the trafficking of counterfeit and pirated goods.

> "To ensure that persons who form corporations or limited liability companies in the United States disclose the beneficial owners of those corporations or limited liability companies, in order to prevent wrongdoers from exploiting United States corporations and limited liability companies for criminal gain, to assist law enforcement in detecting, preventing, and punishing terrorism, money laundering, and other misconduct involving United States corporations and limited liability companies, and for other purposes."[133]
>
> — H.R.___ "Corporate Transparency Act of 2019"

### *2. Require Beneficial Ownership Disclosure from Government Contractors*

Either Congress or the administration should require bidders for federal contracts, sub-contracts, and grants to disclose their beneficial ownership information at the time of their bids, as a means to ensure that counterfeiters, fraudsters, sanctioned individuals, and other criminals and corrupt facilitators are neither able to undercut bids from honest businesses nor to receive taxpayer money.

### *3. Deny Entry to Counterfeiters and Corrupt Actors*

The United States government should deny entry into the United States to complicit and corrupt actors and their facilitators, including criminals engaged in the illicit trade of counterfeited and pirated goods. Bad actors should not benefit from their corruption and criminality.

### *4. Make All Felonies Predicate Offences for Money Laundering*

The United States is one of only a small number of industrialized countries that enumerates a list of predicate offenses for money laundering, rather than referencing all serious crimes as recommended by the international anti-money laundering standards body, the Financial Action Task Force (FATF). Worse, the United States uses one list for crimes committed in the US and another list for crimes committed abroad. Most industrialized countries instead use a "threshold" approach to predicate offenses, where all crimes that carry a certain minimum sentence or fine are considered predicate offenses. In the United States, the equivalent would be to amend the money laundering statutes to make all felonies predicate offenses for money laundering. Legislation to make all felonies predicate offenses for money laundering has been introduced by both Sen. Charles Grassley (R-IA) and Rep. Maxine Waters (D-CA) in previous Congressional sessions but has not yet been adopted.

## 5. Establish a Global Network of Trade Transparency Units (TTUs)

One key countermeasure for trade-based money laundering (TBML) is to establish trade-transparency units (TTUs) between affected countries. TTUs are formed when two countries agree to exchange transaction-level trade data on trade between individuals or trading companies of the two countries in order to detect and combat wrongdoing. For the vast majority of global trade, government authorities are only able to see one side of cross-border trade transactions. Importers and exporters are subject to reporting in the jurisdiction where they operate, but not in the jurisdictions where their counterparties operate. This practice means that parties on either side of a cross-border transaction are able to report different information to their respective authorities, without the authorities of either jurisdiction being aware of the discrepancies.

The concept behind TTUs is simple. By providing government authorities access to information reported on both sides of a trade transaction, anomalies can be spotted. The anomalies, like the misinvoicing of price, value, quantity, or quality of goods, could be indicative of simple customs fraud, TBML, or even underground financial systems. TTUs can provide additional value in TBML analysis by adding law enforcement data, financial intelligence, and commercial information. The creation of these additional data sources is key to identifying more sophisticated schemes, where false information is reported identically on both sides of a transaction.

The United States pioneered the concept of TTUs. Today, approximately 16 TTUs exist around the world, loosely cooperating under a US-sponsored TTU umbrella. Most are in Latin America. Other countries around the world are interested in TTUs. Not only is trade transparency a proven countermeasure to TBML, but, by cracking down on customs fraud, it enhances revenue collection. TTUs have only been in existence a few years, but the network has already recovered well over US$1 billion.[134]

Specific line item funding should be provided to fund a TTU in the United States so as to enhance its analytic capabilities and augment the personnel necessary to foster trade transparency across the country and to continue to expand the international network of TTUs.

## 6. Expand Due Diligence Obligations to All Gatekeepers to the Financial System

In December 2016, the FATF came out with its latest mutual evaluation report on the progress of the United States in meeting international anti-money laundering (AML) and counter-terrorism financing standards.[135] While the report gave the United States strong marks overall, it highlighted two key deficiencies. First, it stated that the lack of timely access to adequate, accurate, and current beneficial ownership information remained one of the fundamental gaps in the US AML regime. Second, the evaluation noted that lawyers, accountants, real estate agents, and other significant professional service providers operating in the US were still largely exempt from the AML requirements levied on financial institutions under the Bank Secrecy Act, and that this exemption presented a real vulnerability given the propensity for abuse in this area.

Congress should pass legislation requiring persons who form legal entities, including transactional lawyers, to carry out AML due diligence. Specifically, the legislation should require formation agents to conduct a risk-based due diligence review before accepting a client; to identify higher risk clients; to conduct risk-based monitoring of client funds and activities; and to report suspicious transactions to law enforcement. These AML obligations have long been part of the international AML standards set by FATF, and the US should take the steps necessary to meet its FATF commitments.

## VIII. Conclusion: Target Dirty Money, Disrupt Illicit Markets, Expose Anonymous Companies

Illicit trade is a serious security threat multiplier, which fuels a multi-trillion-dollar global illegal economy every year. It harms every sector, market, industry, and community every day. Today's bad actors, criminal organizations, and terrorist groups are building their illicit empires on illicit trade with illicit profits that are simply staggering. Through dirty money derived from criminality, these malefactors finance corruption, chaos, insecurity, violence, and instability around the world.

Anonymous companies provide an accessible and licit vehicle to finance greater illicit threats and enable criminals to hide behind a veil of secrecy. As long as kleptocrats, criminals, and terrorists have the ability to hide and move their illicit wealth, American national security and commercial interests remain at risk. US law enforcement agencies and globally-recognized experts call for enhanced transparency and access to information on the beneficial owners of companies. It is a critical tool to mitigate a myriad of security threats and vulnerabilities across sectors.

> "If Congress wants to give sanctions real teeth, they should pass beneficial ownership legislation and more aggressively seek domestic asset forfeitures of sanctioned individuals. After all, there are few things that kleptocrats and transnational criminals love more than their Malibu mansions, New York condos, Miami villas, and Delaware yachts. A private beneficial ownership registry at home would take the US's highly targeted sanctions a step further, increasing the likelihood they will actually change the behavior of US adversaries."[136]
>
> – Clay R. Fuller, Ph.D.
> Foreign and Defense Policy Fellow, American Enterprise Institute

We cannot continue to hamstring and undercut those on the front lines of law enforcement that protect our nation, financial system, businesses, and citizens. As many senior security experts have underscored in recent years, we need meaningful action to empower our law enforcement agencies with the robust authorities, tools, and resources to effectively prosecute the fight against illicit trade and money laundering, and to prevent dirty money from tainting and corrupting the rule of law and our democratic institutions.

28

## How to Report Counterfeited and Pirated Goods and Related Fraud and Criminality

**National Intellectual Property Rights Coordination Center (IPR Center):** The US Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) led IPR Center stands at the forefront of the United States Government's response to global intellectual property (IP) theft and enforcement of its international trade laws. The mission of the IPR Center is to ensure national security by protecting the public's health and safety, the US economy, and our war fighters, and to stop predatory and unfair trade practices that threaten the global economy.

To accomplish this goal, the IPR Center brings together 23 partner agencies, consisting of 19 key federal agencies, Interpol, Europol and the governments of Canada and Mexico in a task-force setting. The task force structure enables the IPR Center to effectively leverage the resources, skills, and authorities of each partner and provide a comprehensive response to IP theft. The IPR Center also engages in public-private partnerships to increase information sharing in order to combat the illegal importation and distribution of counterfeited and tainted goods.

**Report Violations of intellectual property rights, including counterfeiting and piracy, to the IPR Center:** https://www.iprcenter.gov/referral/view **or Telephone:** 1-866-DHS-2-ICE

Source: National Intellectual Property Rights Coordination Center (IPR Center)

# About the Author and Publisher

## *About the Author*

**David M. Luna** is the chief executive and president of Luna Global Networks and Convergence Strategies LLC, an international security consultancy that provides strategic advisory services to businesses and NGOs to tackle the most pressing illicit trade and governance challenges and related security threats across borders, markets, and industries through convergence strategies and tactical plans that holistically target webs of corruption and criminality, and illicit markets.

A former US Diplomat and national security official, Mr. Luna is a frequent speaker on transnational threats, international affairs, geopolitical risks, illicit trade, and the global illegal economy ("dark side of globalization"), including transnational organized crime, corruption, money laundering, terrorist financing, intellectual property rights enforcement, counterfeit and pirated goods, cybersecurity/cybercrime, environmental crime, and smuggling/trafficking crimes that impact economies and communities around the world, and destabilize global security and world order.

With 22 years of federal service in the US Government, Mr. Luna held numerous senior positions with the US Department of State, Bureau of International Narcotics and Law Enforcement Affairs (INL), including directorships for national security, transnational crime, and illicit networks, and anti-corruption and good governance; and served as an advisor to the Secretary's Coordinator for the Rule of Law. Mr. Luna also served as an Assistant Counsel to the President, Office of the Counsel to the President, The White House, as well as in other positions with the US Department of Labor, and the US Senate Committee on Banking, Housing, and Urban Affairs.

Mr. Luna is the new chair of the Anti-Illicit Trade Committee of the United States Council for International Business (USCIB) and is also currently a Senior Fellow for National Security at the Terrorism, Transnational Crime, and Corruption Center, Schar School of Policy and Government, George Mason University.

Mr. Luna previously served as the President (Chair) of the OECD Task Force on Countering Illicit Trade; Chair and Vice Chair of the APEC Anti-Corruption and Transparency (ACT) Working Group; US Coordinator, APEC ACT Pathfinder Dialogues on Fighting Corruption and Illicit Trade; Vice Chair of the World Economic Forum's Global Agenda Council on Illicit Trade and Organized Crime (and Member of the Human Trafficking Task Force); Co-Chair, G-7 Experts Group on Combating Illegal Wildlife Trade; US Coordinator, Dialogues on the Crime-Terror Nexus and Dismantling Transnational Illicit Networks; US Representative, Global Forum on Fighting Corruption II-VI; and other diplomatic initiatives and public-private partnerships on anti-crime and global security.

Mr. Luna is a graduate of the US Army War College and received his B.A. from the University of Pennsylvania and his J.D. from The Columbus School of Law, The Catholic University of America.

30

## *About the FACT Coalition*

The **Financial Accountability and Corporate Transparency (FACT) Coalition** is a non-partisan alliance of more than 100 state, national, and international organizations promoting policies to combat the harmful impacts of corrupt financial practices.

The Coalition calls for an end to corrupt financial practices that prop up autocratic regimes and undermine democratic institutions, allow for and foster human rights abuses, and are a leading contributor to global poverty. The underlying problems are global in scope and require multilateral cooperation. While a growing number of nations are stepping up to address these issues, the US needs to lead on the international stage and fight to eliminate roadblocks to effective reform.

FACT works closely with our international partners while focusing on educating US policymakers on internal reform measures — encouraging those policymakers to provide positive leadership internationally.

Long term, through transparency and accountable international agreements, we seek to create stable funding sources for development and incentivize future investments that measurably reduce global poverty.

For more information, visit thefactcoalition.org.

## References


[1] Louise I. Shelley, "Dark Commerce: How A New Illicit Economy is Threatening Our Future," *Princeton University Press*, 2018.

[2] The sources for this chart come from the following entities: World Economic Forum, World Bank, UN Office on Drugs and Crime (UNODC), Organization for Economic Cooperation and Development (OECD), International Labor Organization (ILO), and Global Financial Integrity (GFI). See:

- World Economic Forum, Global Agenda Council on Illicit Trade & Organized Crime, 2012-2014, *"Out of the Shadows: Why Illicit Trade and Organized Crime matter to us all,"* accessible at https://www.oas.org/en/sms/downloads/BROCHURE_GAC14.pdf.
- Channing (May) Mavrellis, "Transnational Crime and the Development World," *Global Financial Integrity*, March 27, 2017, accessible at https://www.gfintegrity.org/report/transnational-crime-and-the-developing-world/.
- Organization for Economic Cooperation and Development (OECD) and European Union Intellectual Property Office (EUIPO), *Trends in Trade in Counterfeit and Pirated Goods*, March 2019, accessible at http://www.oecd.org/gov/risk/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm and https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Mapping_the_Economic_Impact_study/Mapping_the_Economic_Impact_en.pdf.
- OECD (2016) "Illicit Trade: Converging Criminal Networks," OECD Reviews of Risk Management Policies, OECD Publishing, Paris, April 18, 2016, accessible at https://read.oecd-ilibrary.org/governance/charting-illicit-trade_9789264251847-en#page1.
- Financial Action Task Force, *Money Laundering*, *Financial Action Task Force*, 2016, accessible at http://www.fatf-gafi.org/faq/moneylaundering/.
- INTERPOL, United Nations Environment Programme (UNEP), *The Rise of Environmental Crime: A Growing Threat to Natural Resources, Peace, Development and Security*, June 4, 2016, accessible at https://wedocs.unep.org/bitstream/handle/20.500.11822/7662/-The_rise_of_environmental_crime_A_growing_threat_to_natural_resources_peace%2C_development_and_security-2016environmental_crimes.pdf.pdf?sequence=3&isAllowed=y.
- Office of the Director of National Intelligence (ODNI), "Transnational Organized Crime: A Threat to National and International Security" (Foldout), Estimated Annual Costs and Revenues Generated by TOC, 2011, accessible at https://www.dni.gov/files/documents/NIC_toc_foldout.pdf

[3] Bureau of International Narcotics and Law Enforcement Affairs, "International Narcotics Control Strategy Report, Volume II: Money Laundering", *United States Department of State*, March 2018, accessible at https://www.state.gov/documents/organization/278760.pdf.

[4] Louise I. Shelley, "Dark Commerce: How A New Illicit Economy is Threatening Our Future," *Princeton University Press*, 2018.

[5] A Frontier Economics 2017 Report, "Economic impacts of counterfeiting and piracy," which was commissioned by the International Trademark Association (INTA) and the International Chamber of Commerce's Business Action to Stop Counterfeiting and Piracy (BASCAP), found that the total international trade estimated for counterfeiting and piracy is forecast to reach US$991 billion. A 2019 joint report by the Organization for Economic Cooperation and Development (OECD) and European Union Intellectual Property Office, "Trends in Trade in Counterfeit and Pirated Goods," found international trade in such products represented up to 3.3 percent of world trade, or as much as US$509 billion.

[6] World Economic Forum, Global Agenda Council on Illicit Trade & Organized Crime, 2012-2014, *"Out of the Shadows: Why Illicit Trade and Organized Crime matter to us all,"* accessible at https://www.oas.org/en/sms/downloads/BROCHURE_GAC14.pdf.

[7] Ibid.

[8] World Bank, *Gross Domestic Product 2017*," World Development Indicators database, September 21, 2018, accessible at http://databank.worldbank.org/data/download/GDP.pdf.

[9] Channing (May) Mavrellis, "Transnational Crime and the Development World," *Global Financial Integrity*, March 27, 2017, accessible at https://www.gfintegrity.org/report/transnational-crime-and-the-developing-world/.

[10] Organization for Economic Cooperation and Development (OECD) and European Union Intellectual Property Office (EUIPO), *Trends in Trade in Counterfeit and Pirated Goods*, March 2019. In an earlier 2016 OECD-EUIPO report, the international trade in such products represented up to 2.5 percent of world trade, or as much as US$461 billion in 2013, accessible at http://www.oecd.org/gov/risk/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm and https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Mapping_the_Economic_Impact_study/Mapping_the_Economic_Impact_en.pdf.

[11] Organization for Economic Cooperation and Development (OECD) and European Union Intellectual Property Office (EUIPO), *Trends in Trade in Counterfeit and Pirated Goods*, March 2019. In an earlier 2016 OECD-EUIPO report, the international trade in such products represented up to 2.5 percent of world trade, or as much as US$461 billion in 2013, accessible at http://www.oecd.org/gov/risk/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm and https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Mapping_the_Economic_Impact_study/Mapping_the_Economic_Impact_en.pdf.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] US House Committee on Financial Services. *Hearing titled "Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crime"*, 13 March 2019 (Statement of Rep. Carolyn Maloney), accessible at https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402387.

[25] US House Committee on Financial Services. *Meeting to approve the Authorization and Oversight Plan of the Committee on Financial Services for the 115th Congress* Hearing, 7 February 2017 (Statement of Rep. Steven Pearce), accessible at https://thefactcoalition.org/video-financial-services-markup-oversight-plan?utm_medium=press/videos.

[26] Claire Coleman, "Priced Out: How Anonymous Companies Contribute to the Rising Cost of Housing," *The FACT Coalition*, April 4, 2018, accessible at https://thefactcoalition.org/priced-out-how-anonymous-companies-contribute-to-the-rising-cost-of-housing?utm_medium=blog.

[27] INTERPOL, *Operations*, Opson V (March 2016) and Opson VI (April 2017) , accessible at https://www.interpol.int/Crime-areas/Trafficking-in-illicit-goods-and-counterfeiting/Operations.

[28] The World Health Organization (WHO), "Growing Threats from Counterfeits," April 2010, accessible at https://www.who.int/bulletin/volumes/88/4/10-020410/en/.

[29] Organization for Economic Cooperation and Development (OECD), *Trade in Counterfeit Goods and Free Trade Zones: Evidence from Recent Trends*, March 2018, accessible at http://www.oecd.org/gov/trade-in-counterfeit-goods-and-free-trade-zones-9789264289550-en.htm.

[30] The World Health Organization (WHO), "Growing Threats from Counterfeits," April 2010, accessible at https://www.who.int/bulletin/volumes/88/4/10-020410/en/.

[31] Ibid.

[32] Telang, Rahul, Does Online Piracy Make Computers Insecure? Evidence from Panel Data (March 12, 2018). Accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3139240

[33] Association of Internet Security Professionals (AISP), "Illegal Streaming and Cyber Security Risks: A Dangerous Status Quo?"AISP Working Paper, Autumn 2014. Accessible at https://cryptome.org/2014/09/illegal-streaming-malware-epoch-times-full-14-0923.pdf

[34] Digital Citizens Alliance (DCA), "Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm." April 2019. Accessible at https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf

[35] United States Intellectual Property Enforcement Coordinator (IPEC), "Annual Intellectual Property Report to Congress," *The White House*, February 2019, accessible at https://www.whitehouse.gov/wp-content/uploads/2019/02/IPEC-2018-Annual-Intellectual-Property-Report-to-Congress.pdf.

[36] Remarks by the President on Signing a Memorandum on Addressing China's Laws, Policies, Practices, and Actions Related to Intellectual Property, Innovation, and Technology (August 14, 2017), accessible at https://www.govinfo.gov/content/pkg/DCPD-201700571/pdf/DCPD-201700571.pdf.

[37] Organization for Economic Cooperation and Development (OECD), "Trade in Counterfeit Goods and Free Trade Zones: Evidence from Recent Trends," *OECD*, March 2018, accessible at http://www.oecd.org/gov/trade-in-counterfeit-goods-and-free-trade-zones-9789264289550-en.htm.

[38] *OECD (2018), Governance Frameworks to Counter Illicit Trade, Illicit Trade, OECD Publishing, Paris, https://doi.org/10.1787/9789264291652-en.*

[39] Bureau of International Narcotics and Law Enforcement Affairs, "*International Narcotics Control Strategy Report: Money Laundering (Volume II),*" US Department of State, March 2018, accessible at https://www.state.gov/documents/organization/278760.pdf.

[40] *The Economist Intelligence Unit (EIU)*, "2018 Global Illicit Trade Environment, and, Free Trade Zones: Five Case Studies," commissioned by the Transnational Alliance to Combat Illicit Trade, 2018, accessible at https://www.tracit.org/publications_gitei.html.

[41] Ibid.

[42] Alvise Giustiniani, Vice President, Illicit Trade Prevention, Philip Morris International, in February 2019, quote submitted by PMI as requested by Author for publication of this report.

[43] Alana Semuels, "Amazon may have a counterfeit problems," *The Atlantic*, April 20, 2018, accessible at https://www.theatlantic.com/technology/archive/2018/04/amazon-may-have-a-counterfeit-problem/558482/.

[44] Ibid.

[45] Spencer Soper and Scott Soshnick, "Feds are losing the war on fake Superbowl merchandise," Interview with the National Intellectual Property Coordination Center regarding on-line sales of counterfeits, *Bloomberg News*, February 2, 2017, accessible at https://www.chicagotribune.com/business/ct-fake-super-bowl-merchandise-20170202-story.html.

[46] Barry Brager, "How retailers and brands can fight the online scourge of counterfeit goods," *Digital Commerce 360*, January 2, 2019, accessible at https://www.digitalcommerce360.com/2019/01/02/how-retailers-and-brands-can-fight-the-online-scourge-of-counterfeit-goods/.

[47] *CyberVentures Security*, "Cybercrime Damages US$6 Trillion by 2021," December 7, 2018, accessible at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[48] Ibid.

[49] *International Consortium of Investigative Journalists*, "The Panama Papers: Exposing the Rogue Offshore Financial Industry," An ICIJ Investigation, January 31, 2017, accessible at https://www.icij.org/investigations/panama-papers/.

[50] Christine Spolar, Book Review, "The Panama Papers", by Bastian Obermayer and Frederik Obermaier, *The Financial Times*, June 25, 2016, accessible at https://www.ft.com/content/0dd65f22-38a7-11e6-9a05-82a9b15a8ee7.

[51] Senator Marco Rubio, Tweet from @MarcoRubio, *Twitter*, July 19, 2018, accessible at https://twitter.com/marcorubio/status/1019907395504533504?lang=en.

[52] Nathan Proctor and Julia Ladics, "Anonymity Overdose," *Fair Share Education Fund*, April 2016, accessible at https://www.fairshareonline.org/sites/default/files/AnonymityOverdose_Aug1_2016.pdf.

[53] Steven J. Metalitz, "IIPA 2017 Special 301 Letter to USTR," *International Intellectual Property Alliance*, February 9, 2017, page xi, assessible at https://www.regulations.gov/document?D=USTR-2016-0026-0011.

[54] Kenneth A. Blanco, Director, Financial Crimes Enforcement Network US Department of the Treasury, *Testimony before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance*, May 16, 2018, accessible at https://republicans-financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-kblanco-20180516.pdf.

[55] M. Kendall Day, Acting Deputy Assistant Attorney General, Criminal Division, US Department of Justice, *Testimony before the Senate Committee on the Judiciary*, February 6, 2018, accessible at https://www.justice.gov/opa/speech/acting-deputy-assistant-attorney-general-m-kendall-day-criminal-division-delivers-0.

[56] Mr. Steven D'Antuono, Section Chief, Financial Crimes Section, Federal Bureau of Investigation, *Testimony before the Senate Committee on Banking, Housing, and Urban Affairs*, November 29, 2018, accessible at https://www.banking.senate.gov/imo/media/doc/D'Antuono%20Testimony%2011-29-18.pdf.

[57] Cyrus R. Vance, Jr., New York County District Attorney, *Testimony before the House Financial Services Committee's Subcommittee on Oversight and Investigations*, January 30, 2018, accessible at https://republicans-financialservices.house.gov/uploadedfiles/hhrg-115-ba09-wstate-cvance-20180130rv.pdf.

[58] Dominick L. Stokes, Vice President for Legislative Affairs, Federal Law Enforcement Officers Association (FLEOA), Letter to the House Committee on Financial Service, July 15, 2017. https://thefactcoalition.org/wp-content/uploads/2017/07/FLEOA-House-Support-Letter-Corporate-Transparency-Act-HR-3089-July-2017.pdf

[59] *FACT Coalition*, "FACT Sheet, Anonymous Companies and National Security," August 16, 2017, accessible at https://thefactcoalition.org/fact-sheet-anonymous-companies-and-national-security-august-2017?utm_medium=policy-analysis/fact-sheets.

[60] Financial Action Task Force, *Money Laundering*, Financial Action Task Force, 2016, accessible at http://www.fatfgafi.org/faq/moneylaundering/.

[61] Financial Action Task Force, What is money laundering? accessible at http://www.fatf-gafi.org/faq/moneylaundering/. International Compliance Association (ICA), *"What is money laundering?"* accessible at *https://www.int-comp.org/careers/a-career-in-aml/what-is-money-laundering/*.

[62] United Nations Office on Drugs and Crime (UNODC), *The Money Laundering Cycle*, (Chart: *A Typical Money Laundering Scheme)*, accessible at https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html.

[63] Ibid.

[64] ICA *"What is money laundering?"* accessible at *https://www.int-comp.org/careers/a-career-in-aml/what-is-money-laundering/.*

[65] US Department of The Treasury, Financial Crime Enforcement Networks, History of Anti-Money Laundering Law, accessible at https://www.fincen.gov/history-anti-money-laundering-laws.

[66] Financial Action Task Force, *"What is Money Laundering; How is Money Laundered," FATF,* 2018, accessible at http://www.fatf-gafi.org/faq/moneylaundering/.

[67] Ibid.

[68] Ibid.

[69] Financial Action Task Force, FATF Guidance: Transparency and Beneficial Ownership, accessible at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.

[70] Ibid.

[71] John Cassara, Center on Sanctions and Illicit Finance, Foundation for Defense of Democracies, *Testimony before the US Senate Judiciary Committee: Hearing on S.1241 Modernizing AML Laws to Combat Money Laundering and Terrorist Financing*, November 28, 2017, accessible at https://www.judiciary.senate.gov/imo/media/doc/Cassara%20Testimony.pdf.

[72] Ibid.

[73] *US Department of The Treasury*, "2015 National Money Laundering Risk Assessment," 2015, accessible at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

[74] Financial Action Task Force, "Anti-money laundering and counter-terrorist financing measures — United States," Fourth Round Mutual Evaluation Report, FATF, December 2016, accessible at http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

[75] Andrew Liveris, Paul Polman, Marc Benioff, François-Henri Pinault, Oliver Bäte, and Josh Bayliss, "US Government Action Crucial to Fighting Corruption," *The B Team*, July 12, 2017, accessible at http://bit.ly/2vGYDLQ.

[76] *Global Financial Integrity*, Webpage, *"Anonymous Companies,"* (accessed March 26, 2018) accessible at https://www.gfintegrity.org/issue/anonymous-companies/.

[77] The Global Financial Integrity, *The Library Card Project: The Ease of Forming Anonymous Companies in the United States*, March 2019. https://www.gfintegrity.org/wp-content/uploads/2019/03/GFI-Library-Project_2019.pdf

[78] Steven M. D'Antuono, Section Chief, Criminal Investigative Division, Federal Bureau of Investigation, *Testimony before the Senate Committee on Banking, Housing, and Urban Affairs at a hearing titled "Combating Money Laundering and Other Forms of Illicit Finance: Regulator and Law Enforcement Perspectives on Reform,"* November 29, 2018, accessible at https://www.fbi.gov/news/testimony/combating-money-laundering-and-other-forms-of-illicit-finance.

[79] US Attorney's Office, District of Idaho, "Sixteen Treasure Valley Residents Indicted in Federal Court," US Department of Justice, August 23, 2018, accessible at https://www.justice.gov/usao-id/pr/sixteen-treasure-valley-residents-indicted-federal-court.

[80] Ibid.

[81] US Attorney's Office, District of New Jersey, "Member of Massive Counterfeit Goods Conspiracy Sentenced to 38 Months in Prison", US Department of Justice, March 21, 2014, accessible at https://archives.fbi.gov/archives/newark/press-releases/2014/member-of-massive-counterfeit-goods-conspiracy-sentenced-to-38-months-in-prison

[82] US Attorney's Office, District of New Jersey, "Member of Largest Counterfeit Goods Conspiracy Ever Charged Sentenced to 46 Months in Prison," *US Department of Justice*, June 2, 2014, accessible at https://www.justice.gov/usao-nj/pr/member-largest-countefeit-goods-conspiracy-ever-charged-sentenced-46-months-prison.

[83] US Attorney's Office, District of New Jersey, "Twenty-Nine Charged in New Jersey for Related, International Schemes to Import Counterfeit Goods and Drugs, Launder Profits," *US Department of Justice*, March 2, 2012, accessible at https://archives.fbi.gov/archives/newark/press-releases/2012/twenty-nine-charged-in-new-jersey-for-related-international-schemes-to-import-counterfeit-goods-and-drugs-launder-profits

[84] Office of Public Affairs, Public Release, "Jury Convicts Two New York Importers in One of the Largest Counterfeit Goods Prosecutions in US History: Infringed Goods Valued at More Than $100 Million," *US Department of Justice*, June 10, 2010, accessible at https://www.justice.gov/opa/pr/jury-convicts-two-new-york-importers-one-largest-counterfeit-goods-prosecutions-us-history.

[85] Ibid.

[86] Ibid.

[87] See United States v. Lam et al., Case 3:07-cr-00374-JRS, Document 3, Filed 10/02/07.

[88] Hitha Prabhakar, "Black Market Billions: How Organized Retail Crime Funds Global Terrorists," *FT Press*, 2012, accessible at https://books.google.com/books?id=DIfoGviNKSAC&printsec=frontcover#v=onepage&q&f=false.

[89] California Attorney General Xavier Becerra, "Investigation Leads to Arrest of 15 Individuals who Evaded $34 Million in Tobacco Taxes," August 2010, accessible at https://oag.ca.gov/news/press-releases/investigation-leads-arrests-15-individuals-who-evaded-34-million-tobacco-taxes.

[90] Brian Grow and Kelly Carr, "How Two Shell Companies Duped the Pentagon," *Reuters*, June 28, 2011, accessible at http://reut.rs/mNuVbA.

[91] US Attorney's Office, Western District of Missouri, "Kansas City Business Owner Among Three Sentenced in $1 Million Scheme to Defraud the Army," *US Department of Justice*, October 31, 2014, accessible at https://www.fbi.gov/contact-us/field-offices/kansascity/news/press-releases/kansas-city-business-owner-among-three-sentenced-in-1-million-scheme-to-defraud-the-army.

[92] Ibid.

[93] US Attorney's Office, Western District of Missouri, "*Business Owner Indicted in $2.8 Million Scheme to Defraud the US Army*," *US Department of Justice*, May 23, 2013, accessible at https://archives.fbi.gov/archives/kansascity/press-releases/2013/business-owner-indicted-in-2.8-million-scheme-to-defraud-the-u.s.-army.

[94] US Attorney's Office, Northern District of California, "Counterfeiters Sentenced For Convictions In Nationwide Conspiracy To Distribute Fake 5-Hour Energy Drink," *US Department of Justice*, June 21, 2017, accessible at https://www.justice.gov/usao-ndca/pr/counterfeiters-sentenced-convictions-nationwide-conspiracy-distribute-fake-5-hour.

[95] Ibid.

[96] US Attorney's Office, Southern District of Florida, "Former Executive Director at Venezuelan State-Owned Oil Company, Petroleos de Venezuela, S.A., Pleads Guilty to Role in Billion-Dollar Money Laundering Conspiracy," *US Department of Justice*, November 2, 2018, accessible at https://www.justice.gov/usao-sdfl/pr/former-executive-director-venezuelan-state-owned-

oil-company-petroleos-de-venezuela-s-0 https://www.moneylaunderingwatchblog.com/2018/08/8-charged-in-highly-sophisticated-1-2-billion-international-money-laundering-conspiracy/.

[97] Terence M. Grugan, *"8 Charged With Highly Sophisticated $1.2 Billion International Money Laundering Conspiracy," Ballard Spahr, LLP*, August 2, 2018, accessible at https://www.moneylaunderingwatchblog.com/2018/08/8-charged-in-highly-sophisticated-1-2-billion-international-money-laundering-conspiracy/.

[98] Walt Bogdanich, "Counterfeit Drugs' Path Eased by Free Trade Zones," *The New York Times*, December 17, 2007, accessible at https://www.nytimes.com/2007/12/17/world/middleeast/17freezone.html.

[99] US Attorney's Office, Eastern District of Texas, Press Release, "Sherman Jury Finds Pakistani National Guilty of International Drug Conspiracy and Money Laundering Crimes," *US Department of Justice*, May 22, 2015, accessible at https://www.justice.gov/usao-edtx/pr/sherman-jury-finds-pakistani-national-guilty-international-drug-conspiracy-and-money.

[100] Ibid.

[101] Ibid.

[102] US Department of Homeland Security, US Immigration and Customs Enforcement, News Release (and Indictment), *Feds seize nearly $15 million from investment account of fugitive in ICE counterfeit software case," US Department of Homeland Security*, June 8, 2011, accessible at https://www.ice.gov/news/releases/feds-seize-nearly-15-million-investment-account-fugitive-ice-counterfeit-software-case.

[103] Ibid.

[104] US Immigration and Customs Enforcement, News Release, "Former Colorado police officer sentenced for selling Denver Broncos merchandise," *US Department of Homeland Security*, January 25, 2017, accessible at https://www.ice.gov/news/releases/former-colorado-police-officer-sentenced-selling-counterfeit-denver-broncos.

[105] US Immigration and Customs Enforcement, News Release, "Former Colorado police officer sentenced for selling Denver Broncos merchandise," *US Department of Homeland Security*, January 25, 2017, accessible at https://www.ice.gov/news/releases/former-colorado-police-officer-sentenced-selling-counterfeit-denver-broncos.

[106] US Immigration and Customs Enforcement, News Release, "4 Colorado men charged in counterfeit Denver Broncos merchandise scheme," *US Department of Homeland Security*, August 3, 2016, accessible at https://www.ice.gov/news/releases/4-charged-counterfeit-denver-broncos-merchandise-scheme#wcm-survey-target-id.

[107] *The Economist*, "A Murky Business," October 3, 2013, accessible at https://www.economist.com/baobab/2013/10/03/a-murky-business.

[108] Steven Mnuchin, Secretary of the Treasury, *Statement made before the United States House of Representatives Committee on Financial Services at the Hearing titled "The Annual Testimony of the Secretary of the Treasury on the State of the International Financial System"*, April 9, 2019, accessible at https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402506.

[109] Ibid.

[110] Ibid.

[111] Samuel Rubenfeld, "US Becomes World's Second-Biggest Tax Haven," *The Wall Street Journal*, January 30, 2018, accessible at https://blogs.wsj.com/riskandcompliance/2018/01/30/u-s-becomes-worlds-second-biggest-tax-haven/.

[112] Stephen F. O'Grady, "New rules fail to clean out dirty money," *Griffith University*, October 3, 2012, accessible at https://app.secure.griffith.edu.au/news/2012/10/03/new-rules-fail-to-clean-out-dirty-money/.

[113] Jodi Vittori, "How Anonymous Shell Companies Finance Insurgents, Criminals, and Dictators," *Council of Foreign Relations*, September 1, 2017, accessible at https://www.cfr.org/report/how-anonymous-shell-companies-finance-insurgents-criminals-and-dictators.

[114] Clay Fuller, "How to fight authoritarian corruption when sanctions fail," *American Enterprise Institute*, November 28, 2018, accessible at https://www.aei.org/publication/fighting-corruption-when-sanctions-fail/.

[115] Financial Crimes Enforcement Network, News Release, "FinCEN Reissues Real Estate Geographic Targeting Orders and Expands Coverage to 12 Metropolitan Area," *US Department of the Treasury*, November 15, 2018, accessible at https://www.fincen.gov/news/news-releases/fincen-reissues-real-estate-geographic-targeting-orders-and-expands-coverage-12.

[116] Ibid.

[117] H.R. 2810, Public Law 115-91, "National Defense Authorization Act for Fiscal Year 2018," 115th Congress, December 12, 2017, accessible at https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf.

[118] Financial Crimes Enforcement Network, News Release, "FinCEN Reminds Financial Institutions that the CDD Rule Becomes Effective Today," *US Department of the Treasury*, May 11, 2018, accessible at https://www.fincen.gov/news/news-releases/fincen-reminds-financial-institutions-cdd-rule-becomes-effective-today.

[119] H.J.Res.31, Title VII Sec.7029(f), "Consolidated Appropriations Act, 2019," 116th Congress February 15, 2019, accessible at https://www.govtrack.us/congress/bills/116/hjres31/text.

[120] Josh Rudolph, "Financial Transparency Legislation Would Help Defend US National Security," *The Atlantic Council*, January 4, 2019, accessible at https://www.atlanticcouncil.org/blogs/new-atlanticist/financial-transparency-legislation-would-help-defend-us-national-security

[121] Elizabeth Rosenberg and Neil Bhatiya, "Congress must face reality in exposing Russian aggression," *The Hill*, December 14, 2018, accessible at https://thehill.com/opinion/national-security/421404-congress-must-face-reality-in-exposing-russian-aggression.

[122] Press Release, "New measures to tackle international money laundering," *United Kingdom Government*, December 10, 2018, accessible at https://www.gov.uk/government/news/new-measures-to-tackle-international-money-laundering.

[123] Andrew MacAskill, "UK territories ordered to open up about secretive companies," *Reuters*, May 1, 2018, accessible at https://www.reuters.com/article/uk-britain-tax-territories/uk-territories-ordered-to-open-up-about-secretive-companies-idUSKBN1I23RR.

[124] *UK National Crime Agency (NCA)*, "NCA secures first unexplained wealth orders," February 28, 2018, accessible at http://www.nationalcrimeagency.gov.uk/news/1297-nca-secures-first-unexplained-wealth-orders.

[125] EU Directive 2015/849 of the European Parliament and the Council of the European Union, "Amendment to the 4th Anti-Money Laundering (AML) Directive of 2016," May 20, 2015, accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES. Andres Knobel, "The EU's latest agreement on amending the anti-money laundering directive: at the vanguard of trust transparency, but still further to go," Tax Justice Network, April 9, 2018, accessible at https://www.taxjustice.net/2018/04/09/the-eus-latest-agreement-on-amending-the-anti-money-laundering-directive-still-further-to-go/.

[126] Philipp Zünd, "The beneficial ownership register leads to further transparency," *KPMG Switzerland*, November 5, 2018, accessible at https://blog.kpmg.ch/the-beneficial-ownership-register-leads-to-further-transparency/.

[127] Robert Palmer, "Why We Have a Long Way to Go on Open Company Data," *Global Witness*, October 7, 2016, accessible at https://www.globalwitness.org/ru/blog/why-we-have-long-way-go-open-company-data/.

[128] Ibid.

[129] *Transparency International*, "G20 Leaders or Laggards: Reviewing G20 commitments to end anonymous companies," 2018, accessible at https://knowledgehub.transparency.org/assets/uploads/kproducts/2018_G20-Leaders-or-Laggards_EN.pdf.

[130] Andres Knobel, Moran Harari, and Markus Meinzer, "The state of play of beneficial ownership registration: A visual overview," *Tax Justice Network*, June 27, 2018, accessible at https://www.taxjustice.net/wp-content/uploads/2018/06/TJN2018-BeneficialOwnershipRegistration-StateOfPlay-FSI.pdf.

[131] Dennis M. Lormel, President & CEO, DML Associates, LLC, *Testimony before the United States House of Representatives Committee on Financial Services Subcommittee on National Security, International Development, and Monetary Policy at the Hearing titled "Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crimes"*, March 13, 2019, accessible at https://financialservices.house.gov/uploadedfiles/hhrg-116-ba10-wstate-lormeld-20190313.pdf.

[132] Andres Knobel, Moran Harari, and Markus Meinzer, "The state of play of beneficial ownership registration: A visual overview," *Tax Justice Network*, June 27, 2018, accessible at https://www.taxjustice.net/wp-content/uploads/2018/06/TJN2018-BeneficialOwnershipRegistration-StateOfPlay-FSI.pdf.

[133] H.R.___ "Corporate Transparency Act of 2019", sponsored by Representative Carolyn Maloney of New York, March 13, 2018. https://financialservices.house.gov/uploadedfiles/bills-116pih-corporatetransparency.pdf

[134] Hector X. Colon, Unit Chief/Director TTU, as quoted in March 26, 2015 email with John A. Cassara.

[135] *Financial Action Task Force*, "Anti-money laundering and counter-terrorist financing measures: Mutual Evaluation Report of the United States," December 2016, accessible at http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

[136] Clay Fuller, "How to fight authoritarian corruption when sanctions fail," *American Enterprise Institute*, November 28, 2018, accessible at https://www.aei.org/publication/fighting-corruption-when-sanctions-fail/.




1225 Eye St. NW, Suite 600 | Washington, DC | 20005 | USA
+1 (202) 827-6401 | @FACTCoalition | www.thefactcoalition.org