AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–158

COMBATING MONEY LAUNDERING AND OTHER FORMS OF ILLICIT FINANCE: OPPORTUNITIES TO REFORM AND STRENGTHEN BANK SECRECY ACT ENFORCEMENT

HEARING

BEFORE THE

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

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING THE ISSUES UNDERLYING THE MODERNIZATION OF SYSTEMS DESIGNED TO COMBAT MONEY LAUNDERING, TERRORIST FINANCING, CORRUPTION, WEAPONS PROLIFERATION, SANCTIONS EVASION, AND OTHER THREATS

JANUARY 9, 2018

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

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

U.S. GOVERNMENT PUBLISHING OFFICE

28–675 PDF WASHINGTON : 2018

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama
BOB CORKER, Tennessee
PATRICK J. TOOMEY, Pennsylvania
DEAN HELLER, Nevada
TIM SCOTT, South Carolina
BEN SASSE, Nebraska
TOM COTTON, Arkansas
MIKE ROUNDS, South Dakota
DAVID PERDUE, Georgia
THOM TILLIS, North Carolina
JOHN KENNEDY, Louisiana
JERRY MORAN, Kansas

SHERROD BROWN, Ohio
JACK REED, Rhode Island
ROBERT MENENDEZ, New Jersey
JON TESTER, Montana
MARK R. WARNER, Virginia
ELIZABETH WARREN, Massachusetts
HEIDI HEITKAMP, North Dakota
JOE DONNELLY, Indiana
BRIAN SCHATZ, Hawaii
CHRIS VAN HOLLEN, Maryland
CATHERINE CORTEZ MASTO, Nevada
DOUG JONES, Alabama

GREGG RICHARD, *Staff Director*
MARK POWDEN, *Democratic Staff Director*

ELAD ROISMAN, *Chief Counsel*
JOHN O'HARA, *Chief Counsel for National Security Policy*
SIERRA ROBINSON, *Professional Staff Member*

ELISHA TUKU, *Democratic Chief Counsel*
COLIN MCGINNIS, *Democratic Policy Director*

DAWN RATLIFF, *Chief Clerk*
CAMERON RICKER, *Deputy Clerk*
JAMES GUILIANO, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

C O N T E N T S

TUESDAY, JANUARY 9, 2018

	Page
Opening statement of Chairman Crapo	1
Opening statements, comments, or prepared statements of:	
Senator Brown	2

WITNESSES

Greg Baer, President, The Clearing House Association	4
Prepared statement	29
Responses to written questions of:	
Senator Brown	58
Senator Sasse	62
Senator Tillis	70
Senator Warner	75
Senator Cortez Masto	79
Dennis M. Lormel, President and Chief Executive Officer, DML Associates, LLC, and Former Chief, FBI Financial Crimes Program	5
Prepared statement	35
Responses to written questions of:	
Senator Brown	86
Senator Sasse	87
Senator Tillis	96
Senator Warner	100
Senator Cortez Masto	105
Heather A. Lowe, Legal Counsel and Director of Government Affairs, Global Financial Integrity	7
Prepared statement	46
Responses to written questions of:	
Senator Brown	111
Senator Sasse	117
Senator Tillis	124
Senator Warner	130
Senator Cortez Masto	134

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Countering International Money Laundering	145
Letter submitted by the FACT Coalition	174
Statement submitted by the Independent Community Bankers of America	176
Letter submitted by the Credit Union National Association	178

COMBATING MONEY LAUNDERING AND OTHER FORMS OF ILLICIT FINANCE: OPPORTUNITIES TO REFORM AND STRENGTHEN BANK SECRECY ACT ENFORCEMENT

TUESDAY, JANUARY 9, 2018

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

The Committee met at 10:04 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's hearing is the first of two currently planned hearings to explore the difficult issues underlying modernizing a decades-old system designed to combat money laundering, terrorist financing, corruption, weapons proliferation, sanctions evasion, and a host of other threats.

Our Nation's financial industry has long worked on the front lines of preserving the integrity of the United States and international financial systems and in partnership with our Government since at least when the Bank Secrecy Act was first enacted, in 1970, and the phrase "anti–money laundering"—or AML—was coined a few years later.

From its tax and narcotics beginnings, the BSA, its regulations, and other supporting laws have evolved into a mass of counter-threat-finance regulatory requirements designed to focus the industry's attention on an ever-expanding set of domestic and foreign threats to the Nation.

These threats were brought to the forefront of Americans' hearts and minds and have only increased after the terrorist attacks of September 11, 2001, and, in response, the enactment of the PATRIOT Act.

The threats against our Nation, our people, and our financial system are real. Everyone sees these threats. One only needs to turn on a TV or read an article about corruption, drugs, or a terrorist attack and wonder about the money that had to be involved to make it happen or the profits that came as a result.

Illicit money enables bad people to do the worst of things in this world. Where does it come from? Where does it go? And who has it now? These questions will always need to be asked and answered.

In fact, these questions are being answered, whether they always know it or not, by an entire industry of technical and financial professionals dedicated to managing the day-to-day BSA and other threat finance compliance requirements of our financial institutions.

They do the hard work of monitoring hundreds of millions of financial transactions and producing millions of reports so that law enforcement and security professionals can do their jobs of managing an increasingly complex domestic and international threat picture.

But a lot has changed in this nearly 50 years that have passed since the BSA was enacted. Certainly the sophistication, types, and numbers of threats have increased. The regulations that focus the financial industry's attention on suspicious activities have also increased. So, too, have the resources that are expended and paid by industry and Government alike to maintain a constant vigilance over threats to the financial system.

It is incumbent on this Committee to then ensure that all of this work and the resources involved result in a "high degree of usefulness" in protecting this Nation, as intended by the BSA itself.

I welcome each of our witnesses today whose individual expertise in financial regulation, law enforcement, and financial transparency together will help inform the Committee of potential ways to sharpen the focus, sustainability, and enforcement of a modernized, more efficient U.S. counter-threat-finance architecture.

Getting this right saves lives. Period.

This is a bipartisan issue.

This is both an American and a global issue.

I look forward to working with Senator Brown and all Members of the Committee to see that the needs of the stakeholders in this important work are critically examined and addressed in order to modernize a system that benefits so many, at home and abroad.

Senator Brown.

OPENING STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Thank you, Mr. Chairman, for this important hearing, the first of two this month in which the Committee will look at ideas for strengthening and reforming our laws to combat money laundering and illicit financial transactions.

Some of the world's largest banks and their foreign partners have run afoul of these laws. In some cases they had inadequate anti–money laundering oversight and compliance regimes. Other banks willfully and persistently violated U.S. bank secrecy, sanctions, and anti-corruption laws.

In fact, the GAO concluded last year that from 2009 to 2015 about $12 billion was collected in fines and penalties and forfeitures from financial institutions for violations of the Bank Secrecy Act, the Foreign Corrupt Practices Act, and U.S. sanctions requirements.

These laws are all tools that aid the Federal Government in detecting and disrupting and inhibiting financial crimes, terrorist financing, bribery, and corruption.

During that same period, Federal agencies assessed more than $5 billion specifically for Bank Secrecy Act violations. When one

widens the lens and reaches back to 2005, that number grows larger, much larger.

Many of these banks violated U.S. anti–money laundering and sanctions laws by knowingly facilitating financial transactions for rogue jurisdictions like Burma and Iran and Sudan and Libya and Syria.

Some conducted transactions with individuals or entities affiliated with terrorist organizations and drug cartels in violation of U.S. law. Many violated the law for several years. And in some cases, foreign affiliates of banks operating in the U.S. were working actively to circumvent the compliance systems of their own banks.

These are not victimless crimes. For example, money laundering on behalf of drug cartels has a direct line to the opioid epidemic in my State, where more die of opioid overdoses than any State in the country. These drug cartels have a direct line to the opioid epidemic in Ohio, where Sinaloa cartel actors have been active in robbing so many families of sisters and husbands and parents and children.

These types of violations should concern those who argue we should loosen laws or regulations or oversight in this area. These laws have been critical in protecting the integrity of our financial system.

That said, we should assess whether there are ways to responsibly update and strengthen the anti–money laundering framework, including through new measures to require beneficial ownership information when companies are formed in the U.S. Right now the U.S. has the dubious distinction of being a haven for anonymous shell companies. That needs to end so that law enforcement can stanch the flow of money into illegal activity.

Broadening information sharing may make sense, but important questions about privacy protections, of course, must be answered. We should focus on sharpening suspicious activity reporting and bolstering efforts by law enforcement to give banks guidance on what to look for, instead of substantially raising currency reporting thresholds.

There are many tough questions for the Committee to consider on these issues. I welcome our distinguished witnesses, and I look forward to the comments of the panel.

Thanks, Mr. Chairman.

Chairman CRAPO. Thank you very much, Senator Brown.

We appreciate our witnesses' being with us today, and I want to remind the witnesses that we have asked that you each keep your initial presentation to 5 minutes so that we can have time for our questions and answers; also, to remind the Senators that they should keep their questions to a 5-minute period.

Our witnesses today are Mr. Greg Baer, president of The Clearing House Association; Mr. Dennis Lormel, president and CEO of DML Associates and a former Chief of the FBI Financial Crimes Program; and Ms. Heather Lowe, the legal counsel and director of Government affairs of Global Financial Integrity.

Again, we appreciate all of you being with us today, and, Mr. Baer, you may proceed.

STATEMENT OF GREG BAER, PRESIDENT, THE CLEARING HOUSE ASSOCIATION

Mr. BAER. Thank you. Chairman Crapo, Ranking Member Brown, and Members of the Committee, I appreciate the chance to testify before you today.

Over the past year, the Clearing House has convened off-the-record symposia on the AML/CFT system and produced a comprehensive report. We included a wide range of stakeholders from banking, data science, diplomacy, and global development. We emphasized law enforcement input, which included former senior officials at Treasury's Office of Terrorism and Financial Intelligence, former FinCEN Directors, the former Chief of the AML Unit at the SDNY, and numerous former officials from Justice, DEA, IRS, Customs, and Scotland Yard. The consensus, reflected in our report, is that our current AML/CFT system is extraordinarily inefficient, outdated, and driven by perverse incentives.

Collectively, U.S. financial firms act as an intelligence-gathering agency for law enforcement and national security, employing thousands of people and spending billions of dollars. That collective agency currently yields much extremely valuable intelligence, but a fraction of what a modernized, properly targeted regime could achieve.

An effective approach to AML/CFT should be risk-based, devoting the greatest majority of resources to the most dangerous activity. Unfortunately, banks have been pushed away from risk-based approaches because their performance is graded not by law enforcement or national security officials but, rather, by bank examiners, who do not track how the intelligence is actually used. Instead, those auditors focus on what they know: policies, procedures, and quantifiable metrics—for example, the number of computer alerts generated.

So, for example, if a bank were to start a financial intelligence unit focused on the opioid crisis, it would likely receive no examination credit for that activity. It would receive blame if a diversion of resources caused it to fail to file a SAR in another area.

What gets measured gets done, and providing valuable intelligence to law enforcement or national security does not get measured. According to bank analysis, there is little to no governmental analysis. For the average SAR filing, there is a less than 10 percent chance that any law enforcement follow-up will occur. For certain categories of SARs—structuring, insider abuse, and here insider abuse includes teller crimes—the yield is close to 0 percent, and those SARs—insider abuse and structuring—now represent a majority of the SARs filed.

Furthermore, banks know that the fastest way to get in regulatory trouble is failure to file a SAR that an examiner subsequently determined should have been filed. Therefore, they reportedly spend more time documenting decisions not to file SARs, papering the file, than they do following up on the SARs they do file. In other words, they focus on the noise, not on the signal.

To file SARs, in practice, almost all banks hire one of a handful of vendors who construct rules for generating alerts—for example, three cash deposits between $5,000 and $10,000 in a 3-week period, or a wire transfer over $1,000 to a high-risk country, say Mexico.

These crude rules generate numerous alerts, and bank investigators must then decide whether to clear the alert or file a SAR. And examiners will criticize thresholds that do not generate a large number of alerts. Of course, it is widely understood that sophisticated criminals know these rules, as the software is for sale and widely distributed, and its rules do not change much over time.

Consider then the potential for revolutionary change that artificial intelligence and other concepts therefore present. AI does not search for previously identified typologies but, rather, mines data to detect anomalies. It gets progressively smarter, it would not be easily evaded, and it changes as criminal behavior changes.

The current system is not modernizing, however, because there has been no indication from the regulatory agencies or others that dollars can be shifted from the existing, rules-based system to a better one—in other words, that firms will be rewarded, not punished, for innovation.

Perverse incentives also explain a push for banks to eliminate clients in countries or industries that could end up creating political risk, so-called derisking. A recent report in *The Economist* notes, "Derisking chokes off financial flows that parts of the global economy depend on. It undermines development goals such as boosting financial inclusion and strengthening fragile States. And it drives some transactions into informal channels, meaning that regulators become less able to spot suspicious deals. The blame for the damage that derisking causes lies mainly with policymakers and regulators, who overreacted to past money-laundering scandals."

The cause of derisking is clear: Regulators require banks to deem certain accounts "high risk" based on factors such as line of business or country of origin. The cost of maintaining that account thereby rises exponentially as the bank must conduct an independent investigation of each such client, and that does not even include the risk of fines in the event the client actually does something wrong. The safest alternative is always to derisk, that is, fire the client.

Last, one important change to the current system that requires new legislation is ending the use of shell companies with anonymous ownership. The Clearing House strongly urges Congress to adopt such legislation promptly and is pleased to see bipartisan support for it.

I hope this testimony has been helpful, and I look forward to your questions.

Chairman CRAPO. Thank you, Mr. Baer.

Mr. Lormel.

STATEMENT OF DENNIS M. LORMEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, DML ASSOCIATES, LLC, AND FORMER CHIEF, FBI FINANCIAL CRIMES PROGRAM

Mr. LORMEL. Thank you, Chairman, and thank you guys for holding this hearing. I think this is really an important topic. And to your point in your opening statement, when you talked about saving lives, when I was in the FBI, we actually were able to help save lives based on Bank Secrecy Act information and investigations that we conducted.

I have given you a statement for the record, and I am just going to highlight some points on that, and I will look forward to questions afterward and for the discussion. I certainly appreciated Greg's testimony. And as I said, I was in law enforcement, and I have been doing this for 45 years, and in law enforcement I was the direct beneficiary of suspicious activity reports in particular. And I agree that we have a lot of inefficiencies in the system, and they need to be improved, and this is a great starting point. And I believe that the Clearing House report is a good starting point for discussion.

I also think that we need to have a more robust discussion on this, and I would encourage you to include law enforcement more actively in that dialogue, and particularly when we get into SARs, and I will close out my testimony on SARs when we get to that.

I really applaud what you guys did in having the symposiums, and I was not involved in that at all. And one of the things that concerned me was the level of actual participation law enforcement was involved, and I know you mentioned some people that you had spoken to, and certainly that is very helpful. But I spoke, after you issued the report, to current executives in law enforcement, people that sat in the chairs I sat in, and in other chairs in other agencies, and they were not involved in the dialogue. And I think it is really important that going forward that those voices are heard, particularly if you get into the situation where you look at suspicious activity reports and you determine—or currency transaction reports, and you consider changing the reporting thresholds. I think particularly in today's world and environment, where we talk about, you know, the threat of homegrown violent extremists in particular, currency transaction reports will factor into those types of investigations. And I am sure the FBI can provide statistics on that type of thing.

One of the things that I like to do is visualize the flow of funds, and as Mr. Baer pointed out, there are a lot of inefficiencies in the current system, and we really need to look at it and bring those up to date. But from the vantage point where I came from, the information that flows—so law enforcement is the back-end beneficiary of suspicious activity reports and other BSA reports. Financial institutions are really the front-end monitors when it comes to that type of information, and so they provide that information and it flows to law enforcement. And the basic flow, the basic system, and the information that comes to law enforcement on a regular basis is good information. The problem is that as you add filters on top of that—and the regulatory filters is what I am talking about—the more regulatory filters and the more convoluted the flow of information from banks to law enforcement, that is where we run into the inefficiencies and the system being flawed. And that, in my view, is where we need to focus our attention going forward in terms of improving the system.

And then on the subject of SARs, as I said, I was the direct beneficiary of SARs in law enforcement, and one of the things that I would encourage you to look at, if you get into the SARs, is the law enforcement constituents. For instance, I datamined quite a bit at the program level at FBI headquarters. We had the ability to do datamining and a lot of broad analytical work that was very help-

ful. If you talk to people who work with SARs at the street agent level, at the levels of the SAR Review Teams—every U.S. Attorney's Office has a SAR Review Team. They still manually review SARs. So you are going to get two different perspectives on the use of SARs. From where I sat, more was better because we were able to use a lot more information and use it against other data sets. To the SAR Review Teams out in the streets, they have to physically look at every SAR, they are going to say less is better. So I think there is a balance there as to the quality of the SAR information.

And then to the point, again, I was firsthand involved in and a firsthand beneficiary of some very good, innovative projects, and I cite one in my written testimony that JPMorgan Chase did back in 2009, and it came out in 2011, where they worked with Homeland Security, and they had targeted monitoring. It was to the same points that you were making about transaction monitoring, and this was targeted monitoring where they specifically set up certain rule sets. And, consequently, the hit rate in that type of proactive investigations, they have tremendous results. They are tremendously effective, they are very efficient, and we need to encourage more of that type of work. And I agree that there is not the incentive there for banks to conduct those types of investigations. And I also believe—and I do a lot of training with financial institutions, and I am a firm believer, and I look at things, and I try to assess the flows, information flows, and that is how I broke down the flow of SARs or BSA data to law enforcement from financial institutions. And I think that in that regard—and I will stop, sir, on this. I am very passionate about this topic. And I believe that the more we can do to encourage law enforcement and banks to work together as partners and to work together in terms of being proactive, and particularly when we were in a reactive type of environment, the better the outcome.

Chairman CRAPO. Thank you, Mr. Lormel.

Ms. Lowe.

STATEMENT OF HEATHER A. LOWE, LEGAL COUNSEL AND DIRECTOR OF GOVERNMENT AFFAIRS, GLOBAL FINANCIAL INTEGRITY

Ms. LOWE. Thank you, Chairman Crapo, Ranking Member Brown, and Members of the Committee, for the opportunity to testify before you today on this very important topic. I hope that my contributions to today's hearing will help you take measured and informed decisions that are in the public's interest with respect to the U.S.'s anti–money laundering regime.

So my written testimony, of course, is much more lengthy and more detailed, and I hope that you have a chance to read through that. There are additional points in that testimony that I will not be making verbally today.

So some of the key points that I did make in my testimony are, first, that money laundering and the technology that can help us combat it are both evolving. And in light of this, it is appropriate to consider whether changes to our regulatory structure should be made.

Equally, however, it is critical that Congress balance and carefully weigh the potential benefits against the potential negative ramifications before making decisions in this area.

Number two, as you have seen, money-laundering enforcement tends to be through identification of regulatory infractions as opposed to criminal money-laundering cases. The burden of proof is lower. It is far less costly for the Government to pursue regulatory infractions than pursuing criminal money-laundering charges, and yet it still has a very dissuasive effect. Despite this, the hallmarks of serious criminal money laundering are really there in those cases, in those regulatory cases. As a result, decreasing the ability to enforce using the regulatory approach may have serious, negative repercussions on compliance and, ultimately, allow a lot of criminal access to the U.S. banking system.

Number three, it is critical that information about the natural person(s) who own and control companies—otherwise known as "the beneficial owners"—is finally collected either by the States or by the Federal Government and that it be made available to law enforcement and to banks at the very least. Companies with hidden ownership are the number one problem in the anti–money laundering world, and the U.S. cannot continue to allow our failure to act to put the U.S. financial system and the global financial system at risk.

Number four, I strongly oppose one of the Clearing House's proposals, and that is transferring responsibility for setting AML priorities for individual banks from those banks to FinCEN. Banks are best placed to understand their own business, their own systems, the risks that their own client base presents, and what is inherent therein, and to create the systems that work best in their own business models to combat that money-laundering risk. FinCEN and other regulators should review those assessments, but they cannot be responsible for carrying them out. They do not have the information they need to do so.

The Clearing House recommends greater information sharing among banks and with Governments in a number of ways, and we do really support that. It is a really significant impediment to AML enforcement around the world that this information sharing is not happening. However, it really does need to be done with some appropriate safeguards, especially where it may result in somebody being denied banking services. Say a bank in Hong Kong denies services for whatever reason, sends that information to the U.S., and U.S. banks deny services, that person may not be able to get a bank account anywhere, and there may be a good reason for that, which is fine; but they also need an opportunity to disprove whatever information has been collected on them and give them access if they do have legitimate business.

Number six, transferring raw banking data from banks to FinCEN to analyze, with the appropriate privacy safeguards, is not actually a bad idea either. However, it really is essential that we do not absolve banks of the responsibility to carry out their own analysis as well, which they have the ability to review within the context of the additional client information that they are holding and because they are the gatekeepers to the financial system. The Federal Government cannot do that alone.

Number seven, some types of entities and persons should be required to have AML programs in place that currently do not, such as those involved in real estate, lawyers, and others. The banking sector cannot and should not carry the responsibility alone, especially where these persons act as a proxy to open the door to the financial system for criminals and their money.

And, finally, I just wanted to end with an overall concept, that money-laundering and sanctions violation cases over the past few years really relate to willful, knowing, and very egregious violations of U.S. laws and regulations that have resulted in U.S. and foreign banks granting access to the financial system for hundreds of millions of dollars in funds supporting genocide and funds supporting major, violent South American drug cartels, and many other violations. These fines that have resulted from these cases have been seen by the banking industry as heavy, so banks have begun to take AML regulations that have been in place for many years much more seriously. I would, therefore, remind Members of Congress that the regulatory burden here has not actually really been increasing. The threat of being found out is what has actually been increasing.

Thank you very much.

Chairman CRAPO. Thank you very much, Ms. Lowe.

Before I go to my questions, I would like to ask unanimous consent to enter into the record two letters—or a letter and a statement from industry: one from the Credit Union National Association and another from the Independent Community Bankers of America. Without objection, so ordered.

My first question, Mr. Baer, is for you. There has been considerable discussion of the need for improved information sharing between financial institutions and regulators and among the financial institutions themselves. How is information sharing accomplished under the current regime?

Mr. BAER. Sure. Thank you, Mr. Chairman. Right now, under Section 314(b) of the USA PATRIOT Act, information sharing is allowed among firms with regard to two types of offenses: one is terrorist activity, and the other is anti–money laundering. The definition of anti–money laundering can be a little complex because that can include some of the predicate offenses. But there does seem to be room, and not a lot of room, to draw a principal distinction between anti–money laundering and a lot of other Federal crimes to expand the categories of offense for which, you know, information sharing is permitted.

It has multiple benefits. It certainly allows banks to better identify who the true criminals are. It also, in an underrated way, allows banks to identify people who are not criminals. So one bank may be looking at only one piece of the puzzle and see something that looks suspicious and speak to another bank and realize, no, in the broader context, that is actually OK.

So it makes the whole system more efficient both in terms of finding bad guys and not finding good guys.

Chairman CRAPO. So I was going to ask how we could improve that, but I think you just described it, right? Yes, Ms. Lowe, would you like to comment on that?

Ms. LOWE. Sure. I would like just to add some little more of a context to this.

Chairman CRAPO. Turn your mic on.

Ms. LOWE. Oh, sorry. It has a green light.

Just to add a little international context and a little historical context to this particular area, back in 2012, the Financial Action Task Force, which is the international anti–money laundering standard-setting body, was going to update its recommendations, and one of the proposals that they made was that banks be required to share information across borders in this way. And, basically, everyone agreed that that was a really good idea and really important back in 2012, but realized it could not actually be included in the recommendations because, in particular, the EU's privacy laws would actually prevent that information sharing from happening. Since 2012, those privacy rules in the EU have actually only strengthened.

So in looking in this area, if you are looking to make revisions here, something you also need to be looking at are the EU privacy laws as well as the U.S. privacy laws to see, you know, does anything need to change in there, and we may need to be doing international—work across the ocean to really move that forward, because we cannot really do it alone. We can allow it within the U.S., but abroad is going to be much more difficult.

Chairman CRAPO. Well, thank you, Ms. Lowe. That perspective is helpful.

Mr. Lormel, you mentioned yourself the Clearing House report that was put out and indicated that you feel we need some more law enforcement engagement on that. With regard to the report itself, it characterizes the current AML/CFT regime as outdated and in need of redesign to increase the efficiency and effectiveness of it. Are there parts of that report that you agree with? And if so, which are the most critical parts of it that you see?

Mr. LORMEL. Well, I do agree with parts of the report for sure, and I believe that the comments about the system being antiquated is—they are good comments, and I think that we really need to look at the regulatory framework, and I think where they pointed out in the report that the regulators—they have a different perspective, and that is why when I wrote my statement, I talked on the importance of perspectives and understanding perspective. And, quite frankly, if you look at law enforcement and financial institutions and you put them in a triangle, where you have got the financial institutions here, law enforcement and regulators, you will have hard lines between the regulators and law enforcement, and there is a broken line between law enforcement and the regulators. And so I think a lot of the dialogue belongs—should belong there and bringing it—but what we need to do is we need to encourage—and that is the other thing I agreed with in the statement. I am a firm believer in innovation. I think our system is very—it is inherently reactive, and the more we can do to use financial intelligence information from a proactive perspective, the better. So where they encourage innovative and incentivizing innovation, I think that is important.

In my statement I wrote about a bank—and I am not really at liberty to talk about it other than the fact that it is similar to what

I described with the JPMorgan Chase thing. And if you talk to those bankers and they were going to be forthright about it, what they would tell you is that there is no incentive and that the regulators really do not encourage them to do that. And I think that is where I agree and where I think the building block going forward is how do we promote innovation.

Chairman CRAPO. Thank you very much. My time has expired. Senator Brown.

Senator BROWN. Thanks, Mr. Chairman. Before I start, I would like to ask unanimous consent to include a letter and other documents from the FACT Coalition into the record and that the record remain open for 5 days for any other documents that Senators might have.

Chairman CRAPO. Without objection.

Senator BROWN. Mr. Lormel, thank you for your service at the FBI, and thank you for serving as Chief of the Financial Crimes Program. Let me start with you. Give us a sense of how you think law enforcement can better respond to the traditional criticism from banks that it too seldom shares targeted information that is useful to banks in assessing customer risks.

Mr. LORMEL. Yes, sir. I think that law enforcement, really we need to put a feedback mechanism or we need to do more to encourage feedback in working with financial institutions, and I believe that in a lot of instances—and I certainly, when I was in law enforcement, was guilty of this to a degree. Again, it goes to a matter of perspective and almost wearing blinders that I am trying to develop my law enforcement case and in doing that I did not look or I did not consider enough the position of the banks and trying to determine how I could better share information with banks.

One of the things I put in my statement, for instance, on the subject of terrorist finance is the fact that—and I am sorry, sir, I may be drifting from your question. But I think it is important that we put mechanisms in place to provide security clearances to people in banks where we could share classified information and other intelligence information back that they can run into their systems and use for transaction monitoring. If you think about it, the financial institutions are the repository. They have got the financial intelligence, and how do we provide them with more information, and maybe it is the——

Senator BROWN. Is there any evidence—sorry to interrupt. Is there any evidence that that is happening or that there is a mechanism, an effort to make that happen other than your saying you would like that to happen?

Mr. LORMEL. Which, the security clearances?

Senator BROWN. Yeah. Well, the security clearances and then the sharing back of information.

Mr. LORMEL. Yes, there are initiatives. There are one-off initiatives at different agencies. For instance, I started the Terrorist Financing Operations Section at the FBI. TFOS continues to have working groups with a number of the financial institutions. They have major financial institutions they deal with. And to the extent they can permissible, they share information. We were involved with the SWIFT project, for instance, and the sharing of information among agencies and sanitizing some of that information and

being able to share that back to the extent you can with the banks. I do not think we do it as consistently as we can.

Senator BROWN. Thank you.

Ms. Lowe, you have done a lot of work for the Global Financial Integrity on transparency internationally and in the U.S. with FATF and otherwise including beneficial ownership legislation. Describe for the Committee how you think we should be thinking about new beneficial ownership requirements. For example, what are the key elements in the definition that you think are critical?

Ms. LOWE. Sure. So key elements of the definition—and the definition is critical to any legislation. I think we have a problem actually with the current customer due diligence rule that was adopted for banks where the definition is actually not sufficient. It does not meet international requirements. The FATF and the IMF have both said the same, so important to note that that is something we should probably look at. But for beneficial ownership, you want to know the direct or indirect persons who own or control a company or who have control by other means. And there is a recent Kazakh case which involved control by other means. It is a very difficult thing to determine, but you need to be asking the questions to figure out where it exists. So those are really important elements.

I think that the U.S. Treasury has been pushing the idea that one should be able to simply list a senior manager of a company as the beneficial owner. That is not a beneficial owner by any international definition or anybody's idea of who is a beneficial owner of a company. It is the person at the top of the chain or people at the top of the chain who own or control the company.

The other thing that I think the U.S. Treasury has been pushing is the concept that if a company does not have anybody who owns more than 25 percent of that company directly or indirectly at the top, then there is nobody with enough beneficial ownership to actually be listed. So, therefore, if you have or create five people to own 20 percent of a business, you would get away with not listing anybody as your beneficial owner, which is really not acceptable. It is incredibly easy to get around.

I would note that the SEC accepts a 5-percent threshold because they do require beneficial ownership of information for SEC-regulated entities. And, actually, in the FATCA legislation, Congress put that threshold at 10 percent. Treasury, when it actually implemented, implemented at 25 percent. So I would note that difference as well.

Senator BROWN. Why would that be? Why would Treasury implement it that way?

Ms. LOWE. You would have to ask Treasury. I think they think it is easier to comply with. I think it——

Senator BROWN. Which is kind of not the point.

Ms. LOWE. Right, which is kind of not the point to my mind. But I would suggest you ask Treasury that question.

Senator BROWN. Thank you.

Chairman CRAPO. Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman.

I am just curious. The United Kingdom recently established a body known as the "Joint Money Laundering and Intelligence Task Force" that brings together financial institutions, law enforcement,

and trade associations to discuss AML risks and how Government and private industry can work better together. Can you discuss the efficacy of the U.K.'s task force and whether or not there is anything that we can learn from the British system? It kind of comes back down to either a coordinated effort where you eliminate some of the dotted lines and so forth. But I am just curious if any of you have had any contact with or if you are familiar with that system and how that compares with ours. Yes, sir?

Mr. BAER. Yes, Senator, actually we have met with them a couple of times, and, actually, they attended our symposia. We think it is a very good model. It is not an entire anti–money laundering system, but it is the sort of thing you would take for granted that, of course, you would have, you know, law enforcement, intelligence, senior bank folks sit down on a regular basis and basically work cases together. It is the type of informal, now through JMLIT formalized information sharing that we very much support, and it is done in a very thoughtful way there.

Now, that is not a replacement for the broader AML/CFT regime or OFAC or any of the other things. So I would not describe it as a substitute for the current regime, but it is certainly a very useful component potentially of a U.S. regime, and we would very much support a similar endeavor here.

Mr. LORMEL. I certainly agree with that, and some of the training I conduct, I have trained with the former head of terrorist financing for Scotland Yard, and he was an original member of JMLIT, and he really emphasizes the importance of that sharing, and to bring the banks and the intelligence community and law enforcement together under that Government umbrella is a phenomenal thing. And I would really hope we can build on that model and try to replicate it to the extent we can.

Ms. LOWE. And just to add on there, the original country that actually did this was Australia under what they called "Project Wickenby". So that is also something to take a look at.

Something that the U.K. is doing very well is this concept of the FinTech Sandbox, so within this area. They are creating a system—they have created a system where a financial institution can come to them and say, "We would like to try this new technology. We know it is not something that is OK under the regulations at present. Can you take a look at it? Let us know what you think, let us know if we can try it out. And then we will give you feedback on how it is going and you can review." And then over time, the Government can then approve that technology for the larger industry.

So that I think is a really good process that they have put in place that we should be looking at as a model at this point.

Senator ROUNDS. Thank you.

I am just curious, with regard to SARs and the reporting requirements right now, there is one process in which the regulatory processes are set up so that you define, and clearly everybody knows what they are with regard to the reporting requirements for the different monetary transactions that occur. Bad guys know what they are as well, and so you have, first of all, a system set in place today that everybody knows what the rules are, and the real challenge for those that wish to move resources around is how do we

appropriately get around those SARs or the reporting requirements.

Can you talk to me a little bit about our focus on the compliance side of making sure that the financial institutions are appropriately reporting the transactions that are occurring that are suspicious in nature versus our ability using existing resources or the need for new resources to go after the unique ways in which the bad guys can get around those reporting requirements?

Mr. BAER. Sure. It is a great question, Senator. It really gets to sort of the heart of the matter here.

Right now banks are, as I noted, using sort of a rules-based system developed by a set of vendors who are common to all, and those rules are rather crude. They overgenerate alerts. They require huge investigative resources to basically clear away the chaff and whichever is left, the wheat. And that is a fantastically sort of complex and time-consuming and not terribly productive endeavor.

It is also an endeavor that they have to undertake with regard to offenses that no Federal prosecutor would ever prosecute. So our estimate is that approximately 40 percent of SARs filed are structuring, that is, multiple cash deposits that add up to 10 percent—$10,000, but could just as easily in most cases are just simply a small business that does a lot of cash. But that—and the yield on those SARs is close to 0 percent, and yet they are 40 percent of the SARs filed, maybe more.

The same thing with insider abuse where you fire a call center employee for misstating his or her time sheets or fire a teller because the till is short. Those are not crimes that are going to be prosecuted, but that is where the SAR resources are going. Right now the largest focus of the AML system is filing sales practices SARs on low-level employees, unfortunately.

So it gets to what I think Dennis was talking about, which is, yeah, we can—and I think what the Ranking Member was talking about, we could say, law enforcement could say let us prioritize opioids, let us prioritize human trafficking, let us prioritize other things. That is what any rational intelligence community would do, any rational law enforcement or national security organization would do. And you can tell the banks that. But the banks are in no way absolved by the bank examiners of having to file those SARs on teller abuse. So they cannot shift the resources out of that to the more serious crimes to more innovative and thoughtful artificial intelligence and other means of catching bad guys. They are sort of stuck in the mud in an old rules-based system that does not work very well.

Senator ROUNDS. Thank you.

Chairman CRAPO. Senator Reed.

Mr. LORMEL. If I can just add one comment, sir, just on that.

Chairman CRAPO. Briefly.

Mr. LORMEL. I believe, though, that—I mean, and I agree with that statement. But at the same token, we still see a good number of SARs that come through that are very meaningful and they continue to come through. So there is a fine balance here that we really have to try to achieve.

Senator ROUNDS. Thank you, Mr. Chairman.

Chairman CRAPO. Senator Reed.

Senator REED. Well, thank you very much, Mr. Chairman. Let me thank all the witnesses for their excellent testimony. I have reviewed it, and I particularly thank you, Mr. Lormel, for your service in the FBI. Thank you, sir.

One of the issues that has been raised in your testimony and in your written statements is beneficial ownership and shell companies, and one of the disturbing things, we are getting the reputation around the world as a place to go if you want to hide money, and we used to think, at least when I was younger, that that was un-American, that, you know, it was these little exotic lands overseas, et cetera.

So beginning with Mr. Baer, given the context that most of this is a function of State law because unless you are publicly traded company, the SEC does not have a lot to do—few exceptions, but not a lot to do. So how do we get our arms around this when there is a new industry for attracting questionable money because of beneficial ownership rules and limited or shell companies?

Mr. BAER. Right. It just really gets down to what is the need to form a company with anonymous ownership in the United States, and the United States, as I think some have noted, is a magnet for this because we and I think Kenya are the two worst in the world on this.

There is certainly a legitimate desire, I believe, that you may not want the whole world to know who owns your company. Everybody uses the example of, you know, when the Disney Corporation was buying up half of Orlando, they did not want to have to pay exorbitant rates for the last piece of land. And there may be valid privacy reasons where you do not want people to know who owns your company. But we cannot think of any valid reason you would not want law enforcement to know who owns your company, or if there is a bank that, pursuant to Federal law, is required to know who owns your company, well, they should get to peek behind and see who that is as well.

So, you know, I think as Heather noted, there are difficult issues around how to define beneficial ownership. We actually support the FinCEN final customer due diligence rule on that. But there are certainly other ways to look at that. But I think the general notion that you should not be able to have a company with anonymous ownership from law enforcement and banks who are required to know who owns you is a pretty simple concept, and I think that is why it has gotten good bipartisan support.

Senator REED. Just a follow-up, and then I will go to Mr. Lormel. One, you could either do it through changes of State law requiring the acknowledgment of real ownership, or you could do it through the banking laws in terms of banking relationships, even deposits that the entity would have to disclose who was, so we have a Federal avenue if we have to deal with this.

Mr. BAER. Yes, Senator, I think a couple of alternatives have been proposed. One is just to have the States do it when you file your articles of incorporation, you file your ownership.

Senator REED. Right.

Mr. BAER. Some have suggested that—and I do not know if that is right or not—that might be a burden on the States or they may choose not to do that, so the alternative has been——

Senator REED. Well, I think there are about 45 States at least that require that.

Mr. BAER. Yes. So for those, I think at least one of the bills I have seen has the sort of fail-safe that if the State does not want to do it, FinCEN can gather that information and hold it the way it holds a lot of confidential information currently. I think others have suggested the IRS. I think FinCEN is probably the right place if the State does not want to do it.

Senator REED. I only have about 2 minutes, but, Mr. Lormel, your comments? You are a law enforcement officer.

Mr. LORMEL. Well, certainly having been in law enforcement, I dealt with the challenge of trying to identify beneficial ownership. That was always a challenge, and it was always problematic. And in today's world, when we need to get things more urgently, that is problematic. I look at this and I look at the good-case scenario in a sense, and I agree with Greg that FinCEN may be the better alternative. I am a believer going back that the information should be collected at the States at the point of incorporation. To me, that makes the most sense. And trying to make that uniform I am sure would be a bit of a challenge.

Alternatively, FinCEN would be, I think, a good alternative. The IRS is not a good alternative in the sense that that information for me as an FBI agent, when I was an FBI agent, I would have to get a court order, or I would not have access to that information. So it is not relevant then for my investigative purposes. So the FinCEN alternative would be a decent alternative.

Senator REED. Thank you.

Ma'am, your final comments?

Ms. LOWE. Sure. You know, I am happy with States collecting it. I am happy with FinCEN collecting it. I would note, you know, one of the things people raise is the privacy issue. First of all, on the Disney example, I would point out that you have two parties in that; you have Disney and you have a farmer. And that money—I am sorry, that land is worth whatever they can get for it, right? You have two parties in a transaction. One party should not have more information than the other party has. That is not good economics. So there is that.

I would say that we are talking about making information on beneficial ownership available to law enforcement and to the banks, which is fine, and I think it is where we need to go next. But I would note that the entire European Union, 28 countries have now decided to make beneficial ownership information on companies public information, and that is despite their very, very strong, you know, individual privacy laws that are in place. Other countries around the world are doing the same. Afghanistan is working to make public registration of beneficial ownership information. Ghana is doing that. Nigeria is doing that. And we are just grappling with can we give it to FinCEN. So a little context there.

Senator REED. Thank you very much.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Tillis.

Senator TILLIS. Thank you, Mr. Chairman. Thank you all for being here.

Mr. Baer, in your written testimony there was a footnote that I found very striking in terms of the regulatory burden and whether or not we are putting our resources to their best use. It is on page 6. It says, "The over 800 employees in Global Financial Crimes Compliance at Bank of America is greater than the combined authorized full-time employees in Treasury's Office of Terrorism and Financial Intelligence and the Financial Crimes Enforcement Network." And that does not include other bank employees in anti–money laundering, economic sanctions compliance, business operations, and technology.

It seems like if you see that with a large bank of the scale of Bank of America, which happens to be down in my neck of the woods, I wonder what the small banks and medium banks are doing in terms of the regulatory burden on them. Are we spending that money for its best purposes? Are we spending that money on innovative concepts that could be worked back into the financial—to a broader benefit for the financial services industry? So I know that a part of what I think we have to do is go back and look at the practices that seem like they add cost and not value, either as they are currently implemented or—can you give me some sense, if you were to go through and just do it quick, when we come into committees like this, we tend to have a "Solve World Hunger" sort of scope to our discussion. And if we were just going to cook a good meal and make some progress, what sorts of quick hits, immediate obvious things that there seems to be consensus on but no action in terms of congressional action? And I would open that up to anybody, starting with Mr. Baer.

Mr. BAER. Sure. Thank you, Senator. And I would just say we highlight those numbers—I mean, not to complain about the cost but just to emphasize how important it is that those resources are being misallocated.

Senator TILLIS. Well, I think it is very important for that purpose.

Mr. BAER. Right, because, again, you are talking about a very large intelligence community that has been created under the PATRIOT Act and the BSA, and so it actually really matters whether they are well led and they are incentivized to do the right things, and the stakes are very high. So it is not, "Oh, we do not want to spend the money anymore." It is, "We are spending it on the wrong things."

And I should note, you know, I testified last year with a community banker who had, I think it was, a $100 million bank with three branches. He had seven AML compliance officers and four lending officers. AML was 15 percent of the budget of his bank. So this is not just a problem for large banks. It is a very large problem for small banks. He also described how he was pressured to dramatically increase the number of high-risk customers they designated and on which they had to do more and more investigations. I actually wrote down the number. His system, they generate 7,100 alerts a year and file 15 SARs. And they do not even know if any of those SARs are of any use.

So I think I am sort of dodging your question, which is what is the easy——

Senator TILLIS. But how do we use some of those metrics, some of those outcomes to be instructive to what we should first start looking at to improve the system? Look, I am not against money laundering—I think it is a bad thing. What I want to do is make sure as much lead can be put on the target as possible, and right now it does not—it seems like we are shooting a lot, but not necessarily hitting the target near as much as we could, and it is costing us a lot of money.

So, again, I want to move—we are going to submit several questions for the record. This is an area that is very important to me and of personal interest, but if we are going to do the best that we can, let us say harden our domestic banking system, we obviously have a lot of international depositors, and we do a good job here, and we do not have strong global cooperation, we do not work through some of the privacy differences between the EU, what have we done except move the snakes somewhere—I mean, what we are trying to do here is not limit our portfolio of banking clients. We are trying to identify bad actors and take their money away. And so what sort of global initiatives are really leading us down that path to say, OK, everything is great here, but the money is still flowing through other international banking entities? Ms. Lowe, I would be happy to have you answer that one and give me the secret sauce.

Ms. LOWE. Well, organizations like mine are working internationally on these issues, so, you know——

Senator TILLIS. Yeah, but what progress are we making?

Ms. LOWE. You know, I think actually we are making quite a lot of progress. In a lot of the world, the FATF recommendations, the sort of framework, if you will, of what we consider to be an anti–money laundering regime, has only recently in the past 2 or 3 years been put in place in many, many different countries. And so, you know, as it goes, you put laws in place, and then you give some time for the industry to get used to them, to understand how to implement them, et cetera, and then you start enforcing, et cetera. So in many parts of the world, this is still very nascent, but the regime and the framework is in place.

The U.S. FinCEN is our financial intelligence unit, or FIU, and we are part of what is called the "Egmont Group", which is the network of financial intelligence units around the world that have methods and ways of sharing information among financial intelligence units or between financial intelligence units. And right now there are over 135 Egmont FIUs, which tells you that we are making progress.

I spent a lot of time in Africa last year actually meeting with heads of FIUs, and, you know, it is actually inspiring to have those meetings because these are people that really want to make a difference and they are trying.

Senator TILLIS. I am going to submit several questions for the record.

Ms. LOWE. Sure.

Senator TILLIS. But I would also like you to come back and just think about as I would do when I go in any organization, what are

the things that we should clearly be making consensus on—or making progress on? Because there is consensus, you just need action.

Ms. LOWE. There is no question on the beneficial ownership. Absolutely no question there.

Senator TILLIS. So we will look forward to your feedback so that we can work with the Chair and the Committee.

Ms. LOWE. Sure. No problem.

Senator TILLIS. Thank you.

Chairman CRAPO. Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you. Thank you all for this discussion. Mr. Chairman and Ranking Member, I appreciate the conversation. And let me follow up with what my colleague Senator Tillis has just been talking about. I agree. I think there has to be some balance absolutely on this. I hear from Nevada, from the gaming industry, the same thing that I am hearing from the banking industry, some of the concerns. They are absolutely open to looking at how we address the security necessary to attack money laundering, but at the same time streamlining some of the forms, making sure they want to be cooperative with Government, and so I am really curious about how we find this balance now.

The first question I have is you have been talking about—and let me just focus on the law enforcement piece of this—this risk-based approach. And I am curious, Ms. Lowe, is this something that you would support and how would you identify what this looks like?

Ms. LOWE. The risk-based approach is actually fundamental to the entire international anti–money laundering regime. It is not a question for me of how does this look. It actually exists. It is a framework, and it has a look, right? A casino, for example, or a bank looks at what are its financial products or what is its business line. Who are its clientele, and what risks do they pose? What countries am I bringing money to and from? And what risks does that pose based on whether or not those are high or low risk for money laundering, et cetera? And they create a profile. A casino will do this, a bank will do this. And then they will craft their anti–money laundering regime to reflect what they consider to be their highest risks, OK? So that is the basics and the basis of the risk-based analysis.

I think a lot of the concern that you are hearing is that when examiners are going in, they are not really open to that risk base that the financial institution has put in place. They are looking at checking their boxes that are on their forms.

Senator CORTEZ MASTO. When you say the examiners, that is the Federal Government, the regulatory oversight.

Ms. LOWE. Yes.

Senator CORTEZ MASTO. They are coming, and they are not recognizing——

Ms. LOWE. Right. I understand that that is the concern, and I think Greg can probably tell you a little bit more about that. But as far as the risk-based approach goes, I absolutely 100 percent support that. I think it is incredibly important, actually, in order to actually address the problem.

Senator CORTEZ MASTO. And that is something the industry is actually doing now, Mr. Baer.

Ms. LOWE. Yes.

Senator CORTEZ MASTO. Is that right?

Mr. LORMEL. If I can add a comment to that.

Senator CORTEZ MASTO. Please.

Mr. LORMEL. Yes, it is one of the fundamentals in an AML program to have a risk-based approach, and fundamentally and the way conceptually it is supposed to work then is you identify that risk and to what Greg has been complaining about or pointing out is the inefficiency. And what has happened is that the regulators now have put the banks in a position where they are not necessarily going after that risk or putting metrics in place or procedures in place to deal with that high risk, but they are more into the check-box mentality. And I have done a lot of training, and I was on the quarter point and monitor team for Western Union, and one of the problems they had—and they used that as an example—was their investigative process was such that it was really a check-the-box mentality, and we had to break them from that and say, you know, you need to go out and you have got to have an investigative mind-set. And it is a similar thing when you come over to the banks, and I think that is where I talked earlier about law enforcement being that beneficiary and the banks being the monitor, is the process from getting information from the bank to law enforcement has become so convoluted, and it gets detoured because of the regulatory concern or the perceived concerns.

Senator CORTEZ MASTO. And so can you address your targeted monitoring? How do you—is that the same thing or is it something different?

Mr. LORMEL. OK. Well, it is similar in the sense that all financial institutions conduct transaction monitoring, and they will have vendors or whatever are involved in that. And they have a baseline monitoring system, and they identify and they alert to certain rules, because you establish the rules and you alert them, and that is where one of the problems we have is there are too many false positives in the system. So if you are going to do targeted monitoring—and I will use the human smuggling or the human trafficking. We understand these are the scenarios that we know that smugglers are going to follow, and this is where, to the question earlier from Mr. Reed about how we can help, is to provide the financial institutions, the compliance people, with those scenarios, and for them then to build into their systems targeted monitoring where you are specifically on top of your regular transaction monitoring, you have a targeted monitoring for a specific crime problem, you know, and I would like to see us carry that over to terrorist financing if we can—I think the area of human smuggling, you have got more defined and identifiable patterns of activity so that it is more workable there.

Senator CORTEZ MASTO. Right. And I know my time is up, and thank you, Mr. Chair, but this is something, I agree, the technology gives us the ability now to be targeted to also focus on the risk-based, and we do need law enforcement at the table when we are having this conversation. So I appreciate the dialogue today. Thank you all.

Chairman CRAPO. Thank you.

Senator Warren.

Senator WARREN. Thank you, Mr. Chairman, and thank you all for being here today.

Money laundering is a massive problem. The United Nations estimates that between 2 and 5 percent of global GDP—that is about $800 billion to $2 trillion—is laundered through the international banking system every single year. That money funds terrorists. It funds human traffickers. It funds crime syndicates. So everything we can do to try to crack down on that is good, and that is what we should be doing.

But it seems to me we need to rethink a lot of our money-laundering laws, some of which, as you noted, were written back in the 1970s and are badly out of date, because that makes it hard for law enforcement that is trying to stop money laundering and bad for financial institutions that are trying to comply with these laws.

So my colleagues have probed some areas, but I want to ask about some other areas where we might be able to update our rules and help both law enforcement and financial institutions. So let me start with reporting requirements.

Mr. Baer, I have heard from a lot of community banks and credit unions that anti–money laundering reporting requirements are a big part of their overall compliance costs, so let us probe that a bit. They have pointed out that the threshold that triggers a currency transaction report to the Treasury Department has been at $10,000 since 1972. So let me ask, do you support raising that number?

Mr. BAER. Thank you, Senator. I think here—I mean, obviously, our organization is slightly larger, somewhat larger banks. I think for them that number is not as big a burden in the sense that they have the capability to file whatever the number is. Those systems are built, and it is at least a clear rule. You know the number, right?

Senator WARREN. Right.

Mr. BAER. The larger problem for them has been questions like: How do you decide whether it is $10,000? If you own with someone else a company and you make a cash deposit, the company makes a cash deposit, and the other owner makes a cash deposit, do you add all those up? So those are the tougher issues. But certainly for community banks, I agree with you it is a large burden.

Senator WARREN. OK, that it is large burden. All right. And we should at least talk about where the number should appropriately be set. But community banks also, when they come in and talk, and other small financial institutions, often mention the costs associated with filing the suspicious activity reports with the Treasury Department. You know, the banks are filing more and more of these reports every year. I note that there was a 50-percent increase in filings just from 2012 to 2017 over this 5-year period. At the same time, the banks are submitting this information through a reporting process that, as I understand it, makes it actually harder for law enforcement to use.

So, Mr. Baer, let me ask, the Clearing House has proposed letting banks directly share data with the Treasury Department with proper guardrails to protect customers' privacy. This sounds like it would make it easier for the banks, but can you say a word about how it would impact Treasury's ability to catch criminals that are laundering money?

Mr. BAER. Yes, Senator. I think it would have both those effects. A lot of times what law enforcement really wants is just the underlying data. They do not need a carefully calibrated paragraph written by a bank compliance officer about that information. So with regard to certain types of activities, it would certainly be much more efficient to avoid—you know, you have the alert, and then you have to conduct an investigation to decide whether to file a SAR, and you have to document why you did not file a SAR if you decide not to file a SAR, and that is a massive resource drain. And it would be much simpler just to file the data with law enforcement and let them datamine it to the heart's content.

Senator WARREN. OK.

Mr. BAER. And that would be a very efficient——

Senator WARREN. So I hope we keep digging into this because we might be able to reduce costs for the banks and at the same time help law enforcement do this more efficiently.

I have got two more questions I want to hit, if I can very quickly. Another one is anonymous shell corporations that make money laundering easier. You know, there are a variety of proposals out there to deal with the so-called beneficial ownership legislation at the Federal level that would require companies to disclose their owners. Just setting aside the details, which we could go into for a long time, can I just ask, do all of you support the idea in principle? Can I just have an on-the-record yes?

Ms. LOWE. Yes.

Mr. LORMEL. Yes.

Mr. BAER. Yes.

Senator WARREN. Good. OK. So we have got three yeses on that, Mr. Chairman. I support this as well.

Let me ask one more question. Ms. Lowe, in your estimation, if we did that, if we revealed the beneficial ownership, would that increase or decrease the costs of anti–money laundering compliance for small financial institutions?

Ms. LOWE. It should certainly decrease it. If they have access to that information as a place to start their customer due diligence, you know, a lot of people equate customer due diligence and just beneficial ownership, and that is not correct. You also need to know the source and use of the funds coming in for that account and many other things. But that is the start. And if a bank has someplace to start, I think it really reduces their costs significantly.

Senator WARREN. Good. And I take it that both of you would agree with that.

I just want to say I introduced a bill with Senator Rubio to increase oversight of money laundering used by human-trafficking networks, and I was very glad when we were able to adopt that at the Committee and get it into the language on the North Korea sanctions bill. But we need to do a lot more with our money-laundering laws, and I think we can make some changes to reporting requirements and beneficial ownership disclosure that would make life easier both for law enforcement and for our smaller banks. And I look forward to working with the Committee to be able to do exactly that.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Schatz.

Senator SCHATZ. Thank you, Mr. Chairman.

I want to ask a question about AI. I think, you know, in challenging spaces, especially challenging spaces that include data, there is a tendency to think of this as sort of a magical solution where you just sort of throw big data, throw AI at the problem, and I want to get your sense—in the intelligence community, there is a conversation about the sort of overabundance of data and the overreliance on data points and an underutilization of human intelligence and instincts. And I am wondering what you think about the balance between utilizing new data analytics, big data AI in terms of fighting money laundering, but also how do we balance that with the fact that we probably still need human beings who have instincts, who have experience? I think we should move in this direction. I just think we should not overcorrect and abandon the sort of institutional knowledge of people. I will start with Mr. Baer.

Mr. BAER. Senator, I think that was very well put. I think those, like us, who believe there is great potential here do not believe that you would eliminate the human element. Really what you would use the AI for is—we have talked a lot about alert SAR filing. So you would use AI in order to generate fewer alerts but much smarter alerts, and you would then still need to have an investigator come in and decide whether or not that was truly a suspicious activity that needed to be reported to law enforcement.

The true great advantage of the AI approach, though, is you get rid of what we have discussed earlier, which is a rules-based approach. If X, then alert. If Y, then alert. But there is a whole other alphabet that you are not even looking at. And what AI is able to do is look for anomalies. So instead of typologies, it is anomalies. And it gets smarter and smarter and it learns.

So particularly in the world we would hope to get to is where, you know, banks could share that information. A friend of mine uses the example of a food truck, which is a great way to launder money, but it is also a great way to feed people in D.C. So one bank may only have three food truck clients, so they do not know what is anomalous. But if that bank could share information with a bank that has 300 food truck clients say in San Francisco, that bank would get smarter.

Senator SCHATZ. And isn't that the Square model, on the private sector side, isn't that what Square does? They just sort of presumptively give you the device, and then if you look different than the thousands of other florists or food trucks, then you get scrutiny as opposed to sort of preapproval?

Mr. BAER. I think it is a very similar approach.

Senator SCHATZ. Mr. Lormel.

Mr. LORMEL. I agree. I think we definitely need to keep human intelligence in the mix. It is very important. And certainly you hit the word of "instincts," and, again, I do a lot of training, and I always talk about trusting your instincts, because even with the best technology, you need to rely on human experience. And I think that is important. But I also think we need to leverage newer technologies to improve our efficiencies and certainly our capabilities. And I will look at it from the law enforcement perspective. The

more that we could use analytical tools, certainly the better and the more sharply we can focus our attention, and I think the more timely we can act.

Senator SCHATZ. Ms. Lowe.

Ms. LOWE. I do not think I have anything to add as far as the AI element of it, but just to go back to some of the things that were being discussed a little earlier. So a bank is concerned that they are spending too much time filing SARs about structuring transactions under a $10,000 threshold. I understand that. But if they do not do that, then law enforcement does not see that that same client is doing that at six different banks, right? And all of a sudden, what would have been, well, a problem but probably something that would not be investigated if it was only at that one bank will be investigated if it is at six different banks, right? So I think we need to also bear that in mind when we are talking about what do we file SARs on and what don't we.

Senator SCHATZ. One final question. I will start with you, Ms. Lowe. It appears to me that I do not think we are going to settle the sort of technical aspect of these questions and these system improvements, process improvements, and rule changes and all the rest of it. And so I know Senator Tillis mentioned the U.K. model, the working group. There has been some discussion about a sort of FinTech, FinCEN Sandbox. I am wondering what you think about establishing a public–private either task force or working group to kind of work the technical details, because as much wisdom as is possessed on this dais, I am not sure we can settle this in statutory law or that that is where this belongs. So I am just wondering, very quickly, if you like the idea of some sort of working group in statute.

Ms. LOWE. Sure, I think that that is an important thing, I think at least for a limited time period. I do not think it would have to go on forever. I would note, though, that the people that are really innovating in the FinTech area are actually mainly Nordic. So a lot of the companies are based in Sweden and Denmark and Norway, and not actually in the U.S. So I would be concerned about limiting it just to sort of U.S. involvement. I think you actually need to be looking further.

Senator SCHATZ. Fair enough. But, listen, in the Defense Department, you have the Defense Policy Advisory Board. You can have sort of standing committees without authority to actually establish policy, but who are highly influential and can help agencies to iterate. Do either of you have anything to add on this as my time runs out?

Mr. LORMEL. Well, just if I may, in terms of a working group, the Association of Certified Anti–Money Laundering Specialists has a FinTech working group that is exploring some of these issues now.

Mr. BAER. I guess maybe I will end with a discouraging note.

Senator SCHATZ. Thanks.

[Laughter.]

Mr. BAER. To what I was saying earlier, I mean, I think before this can really be realized, there are a lot of great vendors out there with great AI approaches and other types of approaches, but there really is a break on the system in the sense that there is no sense from the bank regulatory agencies that banks are going to

be allowed to shift from the old rules-based system where they file thousands and thousands of SARs to a new smarter system. And so what you are effectively telling them is you have to double your budget. You are not going to get any——

Senator SCHATZ. You have got to do both.

Mr. BAER. Yeah. And so somebody in charge—and that is really our core recommendation for all this. Somebody has got to step up and say, "I am in charge, and we want you to stop filing SARs where the yield is effectively 0 percent for law enforcement and start filing higher"——

Senator SCHATZ. Got it. Thank you.

Chairman CRAPO. Senator Warner.

Senator WARNER. Thank you, Mr. Chairman, and I appreciate you having this. This is something I need to learn more about, and we have got a lot of intersection with it on the Intelligence Committee side. And I was really disappointed when Senator Schatz came in and jumped the line again, but he actually asked really good questions.

[Laughter.]

Senator SCHATZ. You seem so surprised.

Senator WARNER. I know.

One, I am glad to see the consensus around beneficial ownership and the need for new rules. I thought I was also hearing, similar to what Mr. Baer has said, that, you know, we need to move from this rules-based approach to a more collaborative approach, and actually perhaps with some of the smaller institutions shift some of the—shift more of the data to some central point and allow that to be analyzed.

Ms. Lowe, I think earlier on didn't you push back on that and felt that—I thought you made some comments that you thought this responsibility ought to stay with the bank examiners. Could you explain, if I heard it right?

Ms. LOWE. Sure. I actually think it is important to shift that information, you know, to, for example, FinCEN because I think they need to be looking at that intelligence across different banks. What are they seeing as far as trends? Where do you have certain—again, you will have clients that have accounts at many different banks in order to not raise suspicion, for example. So I think that that is a really important shift, and I think it is important that FinCEN do that.

But what is also important is the banks not be absolved of their responsibility of doing their own analysis as well because they have so much more information about the client and, you know, the risks that that client may pose and what they should expect——

Senator WARNER. But how would you get at the problem of the $100 million bank that has got seven AML individuals and only four lenders? There has got to be some way we can move this from the rules-based, check-the-box approach.

Ms. LOWE. Right, and I think that that has a lot to do with the examinations. I go back to the examinations. And, you know, it is more work for the regulators to actually accept that they cannot do a one-size-fits-all, check-the-box approach when you have an entirely risk-based system. And so that shift needs to happen, and it will be a big one.

Senator WARNER. Let me move to two other areas, if I can. I may ask for an extra minute since I waited so long.

One, we are seeing all the problems with the existing system and how we need to change and modernize machine learning and AI. I also see that back in August of 2015, FinCEN talked about extending this type of anti–money laundering activities toward registered investment advisers, and then back in 2017 there was some motion, some need to look at bringing real estate into the fold as well.

As these proposals around registered investment advisers, around real estate move forward, are they being moved forward with kind of more modern forward thinking? Or how can we avoid, if we were to take in these two industries, simply going back to a check-the-box type approach? If I could get each of you to quickly address that.

Mr. BAER. Actually, I am glad you mentioned real estate because I think one of the major reasons to support beneficial ownership legislation is most of these companies do not establish bank accounts so it is not really that much about the banks. What they do is they put real estate in, or jewelry or art or whatever. So there is clearly a need to expand the scope of potential money laundering. You know, cryptocurrencies right now——

Senator WARNER. That is what I was going to come to next.

Mr. BAER. ——is certainly going to be an area of great concern, and there are a lot of other financial institution types that are not necessarily subject to the customer due diligence rule, or if they are subject to it, are not examined for it. So there clearly is a sense that a lot of this is being pushed out of the largest banks and the banks that are best able to detect bad behavior to places where it is a little less——

Senator WARNER. And how do we get that right? Having seen a great deal of Russian activity in terms of using real estate, wearing my other hats, how do we get that right? What is the regime that we ought to be looking at? Since, clearly, I would think that the real estate industry and the financial investment advisory industry would say, oh, my gosh, look at the burden this has put on us on the banking side, we want nothing about that. Who is doing the best thinking, Ms. Lowe, on real estate and investment advisers?

Ms. LOWE. So on the real estate end of things, FinCEN has had geographic targeting orders in place in Florida, California, Texas, and New York in specific counties to have title insurers—which are part of that industry, right?—determine the beneficial owners of any entity that is purchasing high-value real estate and then provide that information to FinCEN.

FinCEN found that they had crossover where 30 percent of the beneficial owners identified by those title companies, title insurance companies, had SARs filed on them already by banks. So it tells you just the sort of saturation of what we are talking about here.

Apart from investment advisers, there is a list of what are called "designated nonfinancial businesses and professions," or DNFBPs, that FinCEN has identified as sort of nonbanks that play a role in access to the financial system and should have money-laundering regimes in place that essentially require them——

Senator WARNER. But are those industries fighting back against—I would think they do not——

Ms. LOWE. Many of them are, yes.

Senator WARNER. Let me also, since my time has expired, have you also address—and, Mr. Baer, you raised this. You know, we are seeing how we try to move from a rules-based system to a more collaborative system, but, you know, we are about to be overwhelmed with bitcoin and other kind of cryptocurrencies. How are we preparing—how is the system preparing for this whole new movement? And I would love to hear briefly from each of you? With that, I——

Mr. BAER. I think we are all looking at each other on that one. I will admit to a certain amount of bank myopia. Actually, I do not know how this system is preparing for cryptocurrencies. I am not sure there is a way to prepare.

Ms. LOWE. I can say——

Mr. BAER. Go ahead.

Ms. LOWE. So FinCEN—I am sorry, not FinCEN. FATF has actually been looking at this quite closely. The last two private sector meetings that I attended, there were breakout sessions specifically on this and how do we regulate in this area. You know, FinCEN has done some regulation, and we are the first country to actually have put some regulation with respect to cryptocurrencies in one part of the transaction. And I think that that is a good discussion to have with FinCEN about how effective that has been. I really could not tell you. I think, again, I would discuss that with FinCEN.

There have been moves to make the cryptocurrencies or the technology, et cetera, actually more anonymous. The biggest problem with it is that you are talking about movement of funds in a very anonymous way.

So the underlying technology of blockchain has a lot of different potential positive uses, and because it is a closed system, that does not allow you to go back and amend something. So you can only amend going forward, and you have to sort of explain why you are doing that, right?

So a lot of financial institutions are adopting the underlying technology of blockchain for various applications, and I think that that would actually be a really good hearing to have to understand the difference between what is the cryptocurrencies and dangers posed versus the technology, the underlying technology itself, and, you know, how do we draw the line and how do we regulate in a way that allows that technology to be used in a really positive way—I think it can be really used in a positive way in anticorruption as well—versus the dangers of the anonymity of the actual currencies that are traded using that technology.

Senator WARNER. I would hope, Mr. Chairman, that we could take a look at this and maybe get ahead of it rather than chasing the issue after the fact.

Chairman CRAPO. Definitely, and we should.

Well, that concludes our questioning. I want to thank our witnesses again for coming. Both your written and your oral testimony has been very helpful. As you can see, there is a lot of very serious interest in this issue on this Committee, and we will be working

to try to find a way to improve and strengthen and make our approach to this more efficient, both in terms of the burden that is carried by those who engage in our anti–money laundering efforts and in terms of the results that we get in terms of achieving the objectives.

I have a couple of quick announcements. For those Senators who want to ask questions following the hearing, those will be due by January 16th, Tuesday. And to the witnesses, you will probably get some follow-on questions. I ask you to respond to them very promptly.

With that, the hearing is adjourned. Thank you.

[Whereupon, at 11:25 a.m., the hearing was adjourned.]

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

PREPARED STATEMENT OF GREG BAER

PRESIDENT, THE CLEARING HOUSE ASSOCIATION

JANUARY 9, 2018

Chairman Crapo, Ranking Member Brown, and Members of the Committee, my name is Greg Baer and I am the President of the Clearing House Association and General Counsel of the Clearing House Payments Company. Established in 1853 and owned by 25 large commercial banks, we are the oldest banking payments company in the United States, and our Association is a nonpartisan advocacy organization dedicated to contributing quality research, analysis and data to the public policy debate.

The Clearing House is grateful that the Senate Banking Committee is holding this hearing to review our Nation's anti–money laundering and countering the financing of terrorism (AML/CFT) regime.

Introduction

Our AML/CFT system is broken. It is extraordinarily inefficient, outdated, and driven by perverse incentives. A core problem is that 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. Fundamental change is required to make this system an effective law enforcement and national security tool, and reduce its collateral damage.

The U.S. AML/CFT regulatory regime, circa 2017, is a system in which banks have been deputized to act as quasi law-enforcement agencies and where the largest firms collectively spend billions of dollars each year, amounting to an annual budget somewhere between that of the ATF and the FBI.[1] One large bank may employ more individuals dedicated to BSA/AML/OFAC compliance than the combined staffs of Treasury's Office of Terrorism and Financial Intelligence, OFAC, and FinCEN. However, in talking to senior executives at banks large and small, their primary concern is not how much they spend, but how much they waste. And that waste derives from a series of perverse incentives embedded in the current system.

As an analogy, think of the collective resources of the banks as a law enforcement agency where officers are evaluated solely based on the number of tickets they write and arrests they make, with no consideration of the seriousness of the underlying crimes or whether those arrests lead to convictions. Imagine further that suspension or firing is most likely in the event that a ticket is not written or an arrest not made, or if a resulting report is not filed in a timely manner.

To appreciate how misdirected the system has become, it's helpful to first consider what kind of incentives should be at its heart. From a public policy perspective, any rational approach to AML/CFT would be risk-based, devoting the greatest majority of resources to the most dangerous financial crimes and illicit activity. For example, law enforcement and national security officials would prefer that banks allocate significant resources to so-called financial intelligence units (FIUs)—basically, in-house think tanks devoted to finding innovative ways to detect and prevent serious criminal misconduct or terrorist financing—or to following up on high-value suspicious activity reports; or SARs.

Unfortunately, our AML/CFT regulatory system is focused elsewhere. Large banks have been pushed away from risk-based approaches, because their performance is not graded by law enforcement or national security officials, but rather by bank examiners, who do not know of or consider their successes.[2] Instead, those examiners focus on what they know and control: policies, procedures, and quantifiable metrics—for example, the number of computer alerts generated, the number of SARs filed, and the number of compliance employees hired. This means that a firm can have a program that is technically compliant, but is not effective at identifying suspicious activity, or is producing adverse collateral consequences. The converse is also true (and frequently true in practice).

---

[1] See PwC Global Anti–Money Laundering available at *http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/anti-money-laundering.html* ("According to new figures from WealthInsight, global spending on AML compliance is set to grow to more than $8 billion by 2017"); FBI FY2017 Budget Request at a Glance available at *https://www.justice.gov/jmd/file/822286/download*; ATF FY2017 Budget Request at a Glance available at *https://www.justice.gov/jmd/file/822101/download.*

[2] See article by Bob Werner and Sabreen Dogar, "Strengthening the Risk-Based Approach", in TCH Q3 2016 *Banking Perspectives* issue; available at: *https://www.theclearinghouse.org/research/banking-perspectives/2016/2016-q3-banking-perspectives/strengthening-the-rba.*

As a result, we have banks filing SARs that are in less than 10 percent of cases followed up on in any way. For certain categories of SARs, the yield is close to 0 percent. Meanwhile, given the draconian consequences of missteps and prohibitively high cost of compliance, banks are exiting regions or businesses categorized by regulators as high risk.

Specific Problems With the Status Quo

Background. The BSA/AML regime is primarily codified in the Bank Secrecy Act (BSA), enacted in 1970 and amended periodically since then. The Act requires financial institutions to keep certain records and make certain reports to the Government, including reports on cash transactions greater than $10,000. In the 1990s, the law was amended to require financial institutions to detect and report their customers' "suspicious" transactions. Finally, in 2001, the USA PATRIOT Act amended the BSA and imposed additional requirements on financial institutions to, among other things, verify and record information relating to the identity of their customers; and conduct enhanced due diligence on correspondent banks, private banking clients and foreign senior political figures.

Congress granted authority to implement the BSA to the Secretary of the Treasury, thereby designating an agency with both financial and law enforcement expertise as its administrator.[3] The Secretary in turn delegated most of these functions to FinCEN. The Secretary was also given authority to examine financial institutions for BSA compliance, which Treasury then delegated to various regulators according to institution type.[4] This has resulted in a regime where banking agency examiners, with their safety-and-soundness focus, evaluate the BSA/AML policies, procedures, and processes at the institutions they supervise, while Treasury and law enforcement officials use the information supplied by financial institutions to mitigate domestic and international illicit finance threats.[5]

SAR Filings. A key obligation of banks under the current BSA reporting regime—and the key area of focus by bank examiners—is the filing of SARs. The current SAR reporting regime went into effect in April 1996 as a way for banks to provide leads to law enforcement. The process typically begins with an alert generated by a bank's monitoring system, with a SAR filed in the event that investigation determines that the activity is suspicious. For example, negative media reports on an existing bank customer could trigger an alert, prompt an investigation by a bank compliance department, and result in a SAR filing.

In the current regulatory and enforcement climate, bank compliance officers have powerful incentives to trigger as many alerts and file as many SARs as possible, because those metrics demonstrate a quantifiable culture of compliance. (There appears to be no case of a bank being sanctioned for filing spurious SARs.) And even where no grounds for a SAR filing are found, financial institutions can also spend a significant amount of time documenting, for review by their examiners, why they closed an alert without filing a SAR.

What gets measured gets done, and providing valuable intelligence to law enforcement or national security agencies does not get measured; writing policies and procedures and filing SARs does. So, almost two million SARs are filed per year.[6] Worse yet, SAR filing rules and metrics fail to consider the relative severity of the offense. SAR dollar thresholds have not changed in 21 years, and there is no dollar threshold for so-called insider abuse (say, a teller stealing a small amount of money).[7] No Federal law enforcement agency would ever prosecute the large and

---

[3] See 31 U.S.C. 5318(a)(2) and (h)(2). As recently as 2014, the Secretary delegated that authority to FinCEN. See Treasury Order 108-01 (July 1, 2014).

[4] See 31 CFR §1010.810(b).

[5] As in other areas, regulators have imposed requirements through guidance or manuals that are not published for comment, and can conflict with valid FinCEN rules. See TCH letter to the Federal banking agencies, "Appropriate Implementation of FinCEN's Customer Due Diligence Rule", (December 14, 2017); available at *https://www.theclearinghouse.org//media/TCH/Documents/TCH%20WEEKLY/2017/%2020171214_TCH_Letter_CDD_Rule_Implementation.pdf.* See also The Clearing House Letter to FinCEN, Re: RIN 1506-AB15—Advance Notice of Proposed Rulemaking on Customer Due Diligence Requirements for Financial Institutions (June 11, 2012); available at *https://www.theclearinghouse.org/-/media/files/association%20documents%202/20120611%20tch%20comments%20on%20customer%20due%20diligence.pdf.*

[6] See "SAR Stats", available at *https://www.fincen.gov/fcn/Reports/SARStats.* The total number of SARs filed in 2017 was 1,867,269.

[7] See 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System) (Federal Reserve) 12 CFR 353 (Federal Deposit Insurance Corporation) (FDIC) 12 CFR 748 (National Credit Union Administration) (NCUA) 12 CFR 21.11 and 12 CFR 163.180 (Office of the Comptroller of the Currency) (OCC) and 31 CFR 1020.320 (FinCEN) for Federal

growing majority of offenses to which SAR filings relate, and this is one reason the "yield" on SARs is generally reported to be well under 10 percent, and close to 0 percent for many types of SARs.

In practice, almost all banks hire one of a handful of vendors who construct rules for generating alerts: for example, three cash deposits between $5,000 and $10,000 in a 3-week period, or a wire transfer over $1,000 to a high-risk country (Mexico, for example). These crude rules generate numerous alerts, and bank investigators must then clear the alert or file a SAR. And examiners will be critical if the thresholds for a given bank are set at a level that does not generate a large number of alerts; so, in the event that a $1,000 threshold is not generating many alerts, the bank may be told to lower the threshold to $250, or even $0. Of course, it is widely understood that sophisticated criminals know these rules, as the software is for sale and widely distributed, and its rules do not change much over time.

Consider the potential for revolutionary change that artificial intelligence therefore presents. AI does not search for typologies but rather mines data to detect anomalies. It gets progressively smarter; it would not be easily evaded; and different banks with different profiles would end up producing different outcomes. The current system is not progressing from typology to anomaly, however, because there has been no signal whatsoever from the regulatory agencies that dollars can be shifted from the existing, rules-based system to a better one.

To be clear, this is not a criticism of bank examiners, but rather of the role the current system forces them to play. From a political and personal risk perspective, they are in a no-win situation. On the one hand, they are excluded when the bank they examine is pursuing real cases with law enforcement, national security or intelligence community officials, and therefore receive no credit when those cases are successful. But if something goes wrong—if a corrupt official or organization turns out to be a client of the bank they examine—the examiner faces blame. Thus, from an examiner and banking agency perspective, the only possible safe harbor is to demand more policies and procedures, ensure that a lot of alerts are generated and SARs filed, and encourage the bank to investigate exhaustively any client deemed high risk. While all other aspects of banking—for example, credit risk management—have risk appetites and tolerances, for AML/CFT, there is none. And because banks know that the easiest way to get in trouble is to fail to file a SAR when examiners subsequently determine they should have, they probably spend more time documenting decisions not to file SARs—papering the file—than they do following up on SARs they do file. In other words, they are incentivized to follow the noise, not the signal.

Enforcement trends have only served to exacerbate the impact of the perverse incentives underlying our system; AML/CFT-related fines on U.S. banks have increased exponentially over the past 5 years. Certainly, there have been some egregious cases where enforcement action was warranted, but many enforcement actions taken involve no actual money laundering. Rather, they are based on a banking agency finding that an insufficient number of alerts were being generated by bank systems or that not enough SARs were filed. But the primary problem with this enforcement history is not the size and number of fines that are imposed periodically, but rather how those fines and accompanying consent orders incentivize financial firms to allocate their AML/CFT resources. Such orders uniformly result in the hiring of more compliance personnel, the retention of consultants, the drafting of more policies and procedures, and the direct involvement of the board of directors, with resources reallocated to those functions, and away from more proactive ones.

Derisking. Nowhere is this set of perverse incentives more clear than in the push for banks to eliminate clients in countries or industries that could end up creating political risk to examining agencies. A recent set of articles in *The Economist* details the unfortunate consequences that the misalignment in AML/CFT expectations and standards has created as financial institutions have worked to balance fear of enforcement and supervisory expectations with the AML compliance costs of maintaining a global business. As the writers note, "[d]erisking chokes off financial flows that parts of the global economy depend on. It undermines development goals such as boosting financial inclusion and strengthening fragile States. And it drives some transactions into informal channels, meaning that regulators become less able to spot suspicious deals. The blame for the damage that derisking causes lies mainly

---

SAR regulations. The SAR requirement became effective April 1, 1996, and dollar thresholds have not been raised since.

with policymakers and regulators, who overreacted to past money-laundering scandals."[8]

The causes of derisking are clear: the systems, processes, and people required to manage examiner expectations for clients deemed to be of "higher risk", are extremely costly. For example, a bank may prepare a lengthy report on a customer only to be criticized for not further documenting the grounds on which it decided to retain the customer. Institutions are therefore required to make difficult decisions, because it is often times too expensive to build out this infrastructure to support higher risk accounts. And this does not even include the risk of massive fines and reputational damage in the event a customer designated high-risk actually commits a criminal act.

Similarly, domestically, banks of all sizes report that customer due diligence (CDD) requirements have dramatically increased the cost of opening new accounts, and now represent a majority of those costs. Of course, disproportionate and heightened account opening requirements make low-dollar accounts for low- to moderate-income people much more difficult to offer and price. While the connection is not immediately apparent, AML/CFT expense now is clearly an obstacle to banking the unbanked, and a reason that check cashers and other forms of high-cost, unregulated finance continue to prosper. The problem, of course, is that bank examiners and Federal prosecutors seeking record fines do not internalize those costs. And those in the Government who do internalize those costs play no role in examining the performance of financial institutions.

To put some numbers to the issue, one AML director recently testified that his firm employs 800 individuals worldwide fully dedicated to AML/CFT compliance, detection and investigation work, as well as economic sanctions compliance.[9] Today, a little over half of these people are dedicated to finding customers or activity that is suspicious. The remainder—and the vast majority of employees dedicated to these efforts in the business and operations teams that support the firm's AML program—are devoted to perfecting policies and procedures; conducting quality assurance over data and processes; documenting, explaining and governing decisions taken relating to their compliance program; and managing the testing, auditing, and examinations of their program and systems.

The Great Opportunity Being Lost

This lack of focus on the goals of the system is especially disheartening in an age in which emerging technology has the potential to make the AML/CFT regime dramatically more effective and efficient. One of the most pressing needs in enhancing the U.S. regime is to enable financial institutions to innovate their anti–money laundering programs and coordinate that innovation with their peers. As noted above, artificial intelligence (AI) and machine learning could revolutionize this area, and banks continue to discuss various concepts for greater sharing of information. When the SAR requirement (and its predecessor the criminal referral form) was first implemented, relatively few reports were filed, and each SAR was read by someone in law enforcement. Now, with banks and other financial institutions employing tens of thousands of people and using computer monitoring to flag potentially suspicious activity, almost two million SARs are filed per year.[10] Law enforcement generally reads SARs only if they are specifically flagged by the institution, or if a word search identifies it as relevant to an existing investigation.

Thus, the role of a SAR in law enforcement has changed completely, which is not necessarily a bad development. Because so much more data is available, there is extraordinary potential for the use of AI and machine learning to improve the system, as previously described. But there are obstacles. AI strategies require feedback loops, which do not exist in the current system. In addition, there are barriers to cross-border information sharing of suspicious activity for global financial institu-

---

[8] See "The Great Unbanking: Swingeing Fines Have Made Banks Too Risk-Averse", *The Economist*, July 6, 2017, available at *https://www.economist.com/news/leaders/21724813-it-time-rethink-anti-money-laundering-rules-swingeing-fines-have-made-banks-too-risk-averse*. See also "A Crackdown on Financial Crime Means Global Banks Are Derisking", *The Economist*, July 8, 2017, available at *https://www.economist.com/news/international/21724803-charities-and-poor-migrants-are-among-hardest-hit-crackdown-financial-crime-means.*

[9] This number does not include other employees dedicated to anti–money laundering or economic sanctions compliance in Bank of America's lines of businesses, operations or technology teams. The over 800 employees in Global Financial Crimes Compliance at Bank of America is greater than the combined authorized full-time employees in Treasury's Office of Terrorism and Financial Intelligence (TFI) and the Financial Crimes Enforcement Network (FinCEN).

[10] SAR Stats, supra n. 6.

tions.[11] As noted above, resources are trapped elsewhere and several AML executives have reported that efforts to construct novel approaches to detecting illegal behavior have resulted in examiner criticism. Examiners have now also begun applying to bank AML models the same model risk governance rules they adopted for capital measurement, even though models are much more dynamic and have no financial reporting consequence; as a result, it now takes months, as opposed to weeks, to change an AML model to capture new behaviors, which serves as a major disincentive to innovation.[12]

In sum, banks will be reluctant to invest in systems unless someone in the Government can tell them that such systems will meet the banking examiners' expectations, and can replace old, outdated methods—in other words, that they will be rewarded, not punished, for innovation. Until then, we have a database created for one purpose and being used for another.

To get a sense of the potential for improvement, note that one bank has publicly reported that it receives follow-up requests from law enforcement on approximately 7 percent of the SARs it files, which is consistent with other reports we have received. More importantly, for some categories of SARs—structuring, insider abuse—that number is far lower, approaching 0 percent. But no one can afford to stop filing SARs in any category, because examination focuses on the SAR that was not filed, not the quality or importance of the SAR that was filed.

Furthermore, in resolving this issue, we also must deal with the "last piece of the puzzle" problem. Law enforcement will report anecdotally that it sometimes finds a low-dollar SAR of use as part of a larger investigation—not as a lead but as the last piece in a large puzzle. However, it is important to consider the opportunity cost of that SAR—the resources necessary to produce it, and whether those resources, if allocated elsewhere, would produce the first piece in a more important puzzle. As an analogy, if law enforcement rigorously enforced jaywalking rules, it would occasionally capture a wanted fugitive, but no one would consider that a good use of finite law enforcement resources. Again, a core problem with the current regime is that there is an absence of leadership making choices like these.

The Beginning of a Solution

In early 2017, TCH issued a report offering recommendations on redesigning the U.S. AML/CFT regime to make it more effective and efficient. This report reflects input from a wide range of stakeholders, including foreign policy, development and technology experts.[13]

The most important recommendation in the report is for the Department of the Treasury to accept—or, better yet, claim—responsibility for the system. That includes convening on a regular basis the end users of SAR data—law enforcement, national security and others affected by the AML/CFT regime including the State Department—and setting goals and priorities for the system. Treasury is uniquely positioned to balance the sometimes conflicting interests relating to national security, the transparency and efficacy of the global financial system, the provision of highly valuable information to regulatory, tax and law enforcement authorities, financial privacy, financial inclusion, and international development.

Such a process has a clear precedent. The National Security Strategy (NSS) is a document prepared periodically by the National Security Council (NSC) for submission to Congress which outlines the major national security concerns of the United States and how the Administration plans to deal with them. The strategy is developed by the NSC through an iterative, interagency process to help resolve internal differences in foreign policy/national security agendas and effectively communicate priorities to a number of different audiences. There's also the National Intelligence Priorities Framework (NIPF), which is used to establish national priorities for the

---

[11] See TCH and FSR letter to the Treasury on its "Review of Regulations", ("2017 Joint Trades Letter to Treasury on Review of Regulations") July 31, 2017, available at *https://www.theclearinghouse.org/sitecore/content/tch/home/issues/articles/2017/07/20170731%20tch%20and%20fsr%20comment%20on%20fincen%20and%20ofac%20regulations.*

[12] Id.

[13] See *The Clearing House*, "A New Paradigm: Redesigning the U.S. AML/CFT Framework To Protect National Security and Aid Law Enforcement", (TCH AML/CFT Report) (February 2017), available at *https://www.theclearinghouse.org//media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.* See also TCH press release "The Clearing House Publishes New Anti–Money Laundering Report", (February 16, 2017), available at *https://www.theclearinghouse.org/press-room/in-the-news/29170216%20tch%20aml%20cft%20report.*

intelligence community.[14] We believe that measurable outcomes or goals should be clearly and specifically defined for each component of our Nation's AML/CFT regime (including the anti–money laundering programs in financial institutions), and then agreed upon ways to measure the achievement of those outcomes or goals should be set and reported. From these outcomes or goals, priorities should be set regularly for the AML/CFT regime and promptly revisited when new risks emerge. We believe this is the best way to build a regime that is ultimately effective in achieving the desired outcome of a robust and dynamic national AML/CFT regime that can efficiently and quickly adapt to address new and emerging risks. For financial institutions, we believe that such an exercise would change the focus from technical compliance with regulations or guidance, to building anti–money laundering programs that achieve the clearly articulated desired and measurable outcomes or goals of the regime. And we believe that setting measurable outcomes or goals, and then tracking progress to the achievement of these goals, is the best way to build anti–money laundering programs and a national AML/CFT regime that are both effective and efficient.

Reform must also recognize that of the roughly one million SARs filed annually by depository institutions (banks and credit unions), approximately half are filed by only four banks. Whereas a small to mid-sized bank might file a handful of SARs per year, the largest banks file roughly one SAR per minute. These are the same banks that are internationally active, and therefore present almost all of the most difficult policy questions with respect to derisking. Certainly, reform is warranted for smaller firms, where the cost of filing that handful of SARs is wildly disproportionate to its benefit. But if the goal is to catch dangerous criminals, identify terrorist activity, and reduce collateral damage to U.S. interests abroad, FinCEN need focus its examination energy on only a very few firms. This creates an extraordinary opportunity.

We estimate that an examination team of only 25–30 people at FinCEN could replicate the existing work of the Federal banking agencies and the IRS (for the largest MSBs) at the largest, most internationally active institutions. More importantly, a dedicated FinCEN exam team for this small subset of large institutions could receive appropriate security clearances, meet regularly with end users and other affected parties, receive training in big data and work with other experts in Government. They in turn would be supervised by Treasury officials with law enforcement, national security, and diplomatic perspectives on what is needed from an AML/CFT program—not bank examiners with no experience in any of those disciplines. And when FinCEN turned to writing rules in this area, it would do so informed by its experience in the field. It would see the whole battlefield, and promote innovative and imaginative conduct that advanced law enforcement and national security interests, rather than auditable processes and box checking.

Remarkably, this arrangement is exactly what Congress intended and authorized. In the Bank Secrecy Act, Congress granted FinCEN, not the banking agencies, authority to examine for compliance. However, over 20 years ago, FinCEN delegated its supervisory authority to the Federal banking agencies, while retaining enforcement authority. At the time the delegation was made, FinCEN's decision was logical, even inevitable. The agency had few resources, and insufficient knowledge of the banking system. Furthermore, the Nation had over 10,000 banks, and those banks were more alike than different.[15] Restrictions on interstate banking meant that there were no truly national banks, and U.S. banks generally were not internationally active. As a result, there was no real basis by which FinCEN could have distinguished among banks. Given the choice between supervising 10,000 banks or none, it logically chose none, effectively sub-contracting its statutory duties in this area to the banking agencies.[16]

Importantly, the benefits of a FinCEN examination function would extend well beyond the handful of banks it examined. Priorities set and knowledge learned could be transferred to regulators for the remaining financial institutions. And innovation started at the largest firms, with encouragement from FinCEN, would inevitably

---

[14] See Intelligence Community Directive Number 204—"Roles and Responsibility for the National Intelligence Priorities Framework", (September 13, 2007); available at *https://www.dni.gov/files/documents/ICD/ICD_204.pdf.*

[15] See "Commercial Banks in the U.S., Economic Research of the Federal Reserve Bank of St. Louis" available at *https://fred.stlouisfed.org/series/USNUM.*

[16] In addition, in 1986, Congress granted the Federal banking agencies authority to prescribe regulations requiring banks to comply with the Bank Secrecy Act, and examine for such compliance. See 31 CFR §1010.810. As the rule notes "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter, is delegated to the Director, FinCEN." Id. §1010.810(a). See also 12 U.S.C. §1818(s).

benefit smaller firms. The result of FinCEN assuming some supervisory authority would be a massive cultural change, as the focus shifted to the real-world effectiveness of each institution's AML/CFT program, rather than the number of SARs filed or number of policies written. That change would start with those banks under sole FinCEN supervision, but would eventually spread to all institutions.

(In that regard, I testified last year alongside a community banker who reported that his three-branch bank has four lending officers—and six AML compliance officers.[17] While my testimony has focused on challenges faced by the largest banks, the AML/CFT regime is no more rational when imposed on the smallest.)

Relatedly, TCH recommends that Treasury undertake a review of the BSA/AML reporting regime to ensure information of a high degree of utility is reported to law enforcement as well as encourage the exchange of AML/CFT information between the Government and the private sector as well as between and among financial institutions. We applaud FinCEN's recently announced "Exchange" program which aims to strengthen public–private sector AML/CFT information sharing by convening regular briefings between FinCEN, law enforcement and institutions. Such sharing not only makes financial institutions' programs more effective and efficient, it assists in focusing their resources on important matters.

Finally, one important change to the current system that requires new legislation is ending the use of shell companies with anonymous ownership. Here, the United States trails the rest of the world, and has been criticized by the Financial Action Task Force for being a shelter for criminals or kleptocrats seeking to launder money by adopting the corporate form and cloaking their ownership.[18] There may be valid reasons why corporate owners would want to keep their ownership secret from the broader public; however, it is difficult to imagine a valid reason why corporate owners would want to keep their ownership secret from the State incorporating them, law enforcement, and a financial institution that is legally obligated to determine that ownership in the exercise of its BSA/AML obligations. The Clearing House strongly urges Congress to adopt such legislation promptly, and is pleased to see bicameral, bipartisan support for it.

In conclusion, I thank you for inviting me today and focusing Congressional attention on such an important topic. I look forward to your questions.

PREPARED STATEMENT OF DENNIS M. LORMEL

PRESIDENT AND CHIEF EXECUTIVE OFFICER, DML ASSOCIATES, LLC, AND FORMER CHIEF, FBI FINANCIAL CRIMES PROGRAM

JANUARY 9, 2018

Good morning Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee. Thank you for the opportunity to testify before you today. My name is Dennis M. Lormel. I have been engaged in the fight against money laundering, financial crimes, terrorist financing and other forms of illicit finance for 45 years. I served in the U.S. Government for 31 years, 28 of which I served as a Special Agent in the Federal Bureau of Investigation (FBI). I amassed extensive investigative experience in complex and labor intensive financial investigations as a street agent, first line supervisor, middle manager, and senior executive. In 2000, I was promoted to Chief of the Financial Crimes Section, in the FBI's Criminal Division. Following the terrorist attacks of September 11, 2001, I formulated, established and led the Terrorist Financing Operations Section (TFOS) within the FBI's Counterterrorism Division. During my FBI career, I was the direct beneficiary of Bank Secrecy Act (BSA) data to include currency transaction reports (CTRs) and suspicious activity reports (SARs). I experienced firsthand the value BSA data brought to investigations. This was especially true after 9/11. One of our important initiatives was a datamining project which included SAR reporting. For the past 14 years, I have been a consultant, primarily working in the financial services industry, in the anti–money laundering (AML), terrorist financing and financial crimes prevention community. In this capacity, I have worked with private sector clients to improve the effectiveness and efficiency of BSA reporting.

My Government investigative and private sector consulting experience has provided me a unique opportunity to understand and appreciate two very distinct per-

---

[17] See Testimony of Lloyd DeVaux before the House Financial Services Committee Subcommittee on Financial Institutions and Consumer Credit, June 28, 2017, available at *https://financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-ldevaux-20170628.pdf*.

[18] See FATF Anti–money laundering and counterterrorist financing measures, Mutual Evaluation of the United States (December 2016) at 18 available at *http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016*.

spectives regarding the BSA. Two of the principal stakeholders of the BSA are law enforcement and financial institutions. Putting this in the context of the flow and utilization of financial information, law enforcement is the back end user and beneficiary of BSA data. Financial institutions serve as the front end repository and custodian of financial intelligence. Financial institutions also serve the critical function of being the monitor for identifying and reporting suspicious activity and other BSA data to law enforcement. Simply put, law enforcement uses BSA data to predicate or enhance investigations from a tactical standpoint. Law enforcement also uses BSA data for strategic purposes. From a simplistic standpoint, the flow of BSA data that is continuously filtered to law enforcement is invaluable. When you layer the complexities of regulatory compliance requirements over the monitoring and filtering process financial institutions must follow, the effectiveness and efficiency of BSA reporting from the front end monitor to the back end beneficiary, becomes flawed.

My point is that the BSA system is not broken. The system is fraught with many inefficiencies but it works. Law enforcement consistently receives valuable intelligence from BSA data. The challenge is that the BSA system can and should be much more effective and efficient. In this context, I applaud the Committee for dedicating the time to assess the effectiveness and efficiency of BSA enforcement and considering reform measures to strengthen BSA reporting requirements.

I'd like to take the opportunity to commend the Clearing House for having issued their report in February 2017 "A New Paradigm: Redesigning the U.S. AML/CTF Framework to Protect National Security and Aid Law Enforcement". I believe the report is a good point of reference to initiate discussion for reform consideration. I laud the Clearing House for recognizing the importance of including all stakeholders in the discussion. I was not involved in the two symposiums held to formulate the report. One concern I have about the report is the actual extent to which law enforcement was included as a contributing stakeholder. In my view, law enforcement is the most important stakeholder because the BSA was intended to assist law enforcement. When the report was issued, I contacted then current law enforcement executives in positions like I held and none were included in the deliberations. I encourage the Committee to include a variety of active and former law enforcement executives in your ongoing dialogue and efforts to strengthen the BSA.

The BSA was passed in 1970 with the legislative purpose of generating reports and records that would assist law enforcement in following the money and developing prosecutable criminal cases. Since passage of the BSA, additional legislation has periodically been enacted to enhance regulations. Most notably, passage of the USA PATRIOT Act established a host of new measures to prevent, detect, and prosecute those involved in money laundering and terrorist financing. Going forward, deliberations to enhance the BSA should focus on systemic vulnerabilities, evolving technology, emerging trends and opportunities to leverage public and private partnerships and information sharing with an eye on continuing to enhance law enforcements investigative ability.

As noted in the introduction of the BSA, "the implementing regulations under the BSA were originally intended to aid investigations into an array of criminal activities, from income tax evasion to money laundering. In recent years, the reports and records prescribed by the BSA have also been utilized as tools for investigating individuals suspected of engaging in illegal drug and terrorist financing activities. Law enforcement agencies have found CTRs to be extremely valuable in tracking the huge amounts of cash generated by individuals and entities for illicit purposes. SARs, used by financial institutions to report identified or suspected illicit or unusual activities are likewise extremely valuable to law enforcement agencies". This statement is a true reflection of BSA reporting. However, there is a troubling back story about perceived regulatory expectations that have resulted in systemic inefficiencies.

Regardless of the extent or effectiveness of BSA regulations, criminals and terrorists must use the financial system to raise, move, store and spend money in order to sustain their illicit operations and enterprises. The reality is that no matter how robust an anti–money laundering (AML) program is, it cannot detect all suspicious activity. The BSA standard is that financial institutions maintain AML programs that are reasonably designed to detect and report suspicious activity. One of the regulatory challenges confronting financial institutions today is the question: What constitutes a reasonably designed AML program? Regulatory expectations, either real or perceived, have caused financial institutions to lose sight of the purpose of BSA reporting and have consequently led to many of the systemic inefficiencies of BSA reporting.

In using the financial system, criminals and terrorists are confronted with distinct contrasts. On one hand, the financial system serves as a facilitation tool enabling

bad actors to have continuous access to funding. On the other hand, the financial system serves as a detection mechanism. Illicit funds can be identified and interdicted through monitoring and investigation. Financing is the lifeblood of criminal and terrorist organizations. At the same time, financing is one of their major vulnerabilities. At the basic core level of the front end and back end data process flow, BSA reporting works and is more apt to serve as the intended detection mechanism. The more convoluted and distracting the regulatory process becomes, the greater the likelihood that the financial system serves as a facilitation tool for criminals and terrorists.

There are a number of vulnerabilities or high risk areas in the financial system that criminals and terrorists exploit. I categorize them as criminal activity and facilitation tools bad actors use to exploit their ill-gotten gains derived from their criminal activity. The biggest crime problems we encounter include fraud and money laundering. Most criminal activity, other than select violent crimes, includes elements of fraud and money laundering. Drug trafficking, human trafficking, corruption, and other crimes contain elements of fraud and require money laundering. Some of the more significant facilitation tools include wire transfers, correspondent banking, shell companies (beneficial ownership), illegal money remitters (informal value transfer systems), non-Government organizations, credit and debit cards, and electronic mechanisms. In my experience, one of the biggest areas of vulnerability in the financial system is identifying illegal money remitters.

One facilitation tool that consistently garners Congressional attention is the issue of beneficial ownership. Year after year, potential bills are introduced regarding beneficial ownership. I strongly encourage the Committee to consider beneficial ownership legislation as an enhancement to the BSA. Throughout my law enforcement career, I dealt with the challenge of shell companies and identifying true beneficial owners. Based on my experience, I believe beneficial ownership should be required by Secretaries of States, at the point of incorporation. On May 11, 2016, the Financial Crimes Enforcement Network (FinCEN) issued Customer Due Diligence Requirements for Financial Institutions (the COD Rule). The rule strengthens existing customer due diligence (CDD) requirements and requires banks to identify and verify the beneficial owners of legal entity customers. Financial institutions are in the process of implementing COD requirements. If identification of beneficial ownership were required at point of incorporation, the burden on financial institutions would be lessened.

Regarding the BSA, it is important that all stakeholders be engaged in the discussion and deliberation to improve the effectiveness and efficiency of BSA reporting and enforcement. More importantly, all stakeholders should be involved in breaking down real or perceived regulatory impediments. In each of our areas of responsibility, all BSA stakeholders should strive to exploit the financial vulnerability of criminals and terrorists by ensuring the financial system serves as a detection mechanism disrupting illicit funding flows. Although the BSA system works, it is flawed and lacks the effectiveness and efficiency it was intended to achieve.

The starting point toward improving the effectiveness and efficiency of BSA reporting is to improve the current system through building meaningful and sustainable public and private sector partnerships beginning with BSA stakeholders, including the financial services industry, regulators, policy makers, sanctioning authorities, intelligence experts, law enforcement, legislatures and other stakeholders. We need to start by improving the efficiencies of our current system by breaking down impediments. We then need to determine what enhancements to regulations should be considered.

Building meaningful and sustainable partnerships begins with understanding perspectives. Each stakeholder partner possesses a perspective based on their professional responsibilities and experience. Each of our perspectives will be somewhat unique. Understanding and blending the perspectives of our partners will enable us to establish a middle ground to improve or build efficiencies upon. As this process evolves, we can leverage the capabilities and capacity of our partners. This type of evolution sets the stage for developing innovative ideas and proactive measures.

One of the inherent disadvantages we have in our financial system and AML environment is that we are reactive. Criminals and terrorists have the advantage of being proactive. Our ability to add innovative ideas and proactive measures to an otherwise reactive system can achieve impactful investigative results. In fact, there have been recurring innovative and proactive law enforcement investigations. I speak from firsthand experience when I talk about developing proactive techniques. I can point to specific proactive law enforcement initiatives following 9/11 that were the direct result of innovative public and private sector partnerships. My emphasis here is we can be innovative within the current framework. We can also improve the current landscape through enhancements to encourage and/or incentivize inno-

vation. For example, financial institutions conduct baseline transaction monitoring to alert to anomalies that can lead to identification of suspicious activity. By developing rule sets and scenarios that are targeted to specific transactions or financial activity, we are more likely to identify specific or targeted suspicious activity regarding specific crime problems such as human trafficking. Financial institutions are reluctant to employ targeted monitoring initiatives because of concern for the potential regulatory expectations or other perceived impediments such innovative thinking could incur.

Included as an attachment to my testimony is an article I wrote in 2011 for publication by the Association of Certified Anti–Money Laundering Specialists (ACAMS) titled "Perspectives. Partnerships and Innovation". As an example of innovative and proactive targeted monitoring, the article details the public and private partnership of a special AML investigative team at JPMorgan Chase (JPMC) in 2009, with Homeland Security Investigations (HSI), Immigration and Customs Enforcement (ICE). I provide extensive training to the financial services industry regarding AML, terrorist financing, fraud, investigations, suspicious activity reporting and related topics. I frequently site the JPMC and ICE collaboration as one of the best models for partnerships and innovation. One of the accomplishments of this collaboration was the effective and efficient use of BSA data based on targeted monitoring against human trafficking. The attached article also provides a sense of leveraging perspective and, the regulatory and collateral challenges financial institutions face by endeavoring to be innovative.

As an extension of public and private partnerships, we should consider how to improve information sharing. The PATRIOT Act provided us with information sharing vehicles such as Section 314(a) where financial institutions can share financial information with law enforcement and Section 314(b) where financial institutions can share information with each other. Efforts should be made to enhance Section 314 information sharing in the current environment. In addition, any proposed enhancements to the BSA should consider additional information sharing mechanisms. The more we can do to enhance information sharing, the more meaningful information will be for law enforcement and the more detrimental to criminals and terrorists. During their plenary session in June 2017, the Financial Action Task Force (FATF) stressed the importance of information sharing to effectively address terrorist financing. I have always been a huge proponent of information sharing to the extent legally allowable.

One of the most productive examples of public and private sector partnership, and information sharing, is the Joint Money Laundering Intelligence Task Force (JMLIT) in the United Kingdom (U.K.). JMLIT was formed by the Government National Crimes Agency (NCA) in partnership with the financial sector to combat high end money laundering. JMLIT was established as a business-as-usual function in May 2016. It has been developed with partners in Government, the British Bankers Association, law enforcement and more than 40 major U.K. and international banks. I'm hopeful that the U.S. can assess and work through information sharing and privacy concerns in order to replicate the U.K. JMLIT model.

With respect to terrorist financing, any legislative enhancement to the BSA should consider facilitating obtaining security clearances for select financial institution personnel. In most instances, law enforcement is precluded from sharing classified information with financial institutions. If financial institutions had select personnel with a security clearance and they could gain access to select classified information, they would be able to either search for specific financial information or establish targeted monitoring initiatives to identify specific financial intelligence that would be meaningful to classified or otherwise sensitive counterterrorism investigations.

Throughout my career, I have worked closely with financial institution AML and fraud compliance professionals. I have the utmost respect for their dedication and commitment to protecting the integrity of their financial institutions and for identifying the misuse of the financial system by bad actors. Next to my former law enforcement colleagues, I hold my friends in AML and fraud compliance in the highest regard. It is important to note that the BSA shortcomings we face are systemic problems caused by multiple factors and not by groups of individuals. One of the positive trends evolving within financial institutions, in part, founded on the dedication factor of AML professionals that I complimented, is the formation of financial intelligence units and/or special investigations teams established to deal with terrorist financing and emergency response situations such as the Panama Papers, the FIFA scandal and human trafficking. In addition to developing proactive mechanisms, like targeted monitoring, these teams have developed "urgently" reactive capabilities to respond to terrorist and emergency situations requiring immediate response. As I mentioned earlier, AML programs are inherently reactive. One of the

best reactive mechanisms we possess is negative news reporting. For example, when terrorist incidents like the attacks in New York in October and December 2017 occurred, as soon as the names of the perpetrators are announced, these special investigations teams immediately run the perpetrator names through their systems and should they identify accounts or transactional activity involving those individuals, they immediately contact law enforcement.

Like the JPMC and ICE human trafficking targeted monitoring program I mentioned, I'm aware of a major bank that has formed a special investigative team to similarly search for human trafficking that could be related to a forthcoming major sporting event. I' m not at liberty to further identify the financial institution or circumstances. However, it is important to note that financial institutions and law enforcement do participate in targeted monitoring projects and when they are able to do so, BSA data flows from the front end monitor (a financial institution) to the back end beneficiary (law enforcement) in a timely and, effective and efficient manner.

I encourage all financial institutions to establish special investigations or critical incident response teams. I teach and view these teams analogous to law enforcement Special Weapons and Tactics (SWAT) teams. SWAT officers receive regular intensive training to deal with dangerous emergency response situations. Most SWAT officers have other primary law enforcement assignments, and SWAT is a collateral duty. Financial institution SWAT or critical incident response or special investigations teams should also receive special training for dealing with emergency response and targeted proactive investigative situations. Regardless of the size of a financial institution, all financial institutions should establish special investigative teams to identify and report targeted suspicious activity. Whether the team is a unit or one investigator, all financial institutions should develop emergency response capabilities.

In my training programs regarding money laundering, fraud and terrorist financing, I stress the importance of situational awareness. Situational awareness is being aware of and responsible for your physical surroundings regarding your personal safety and security. If you see something, say something. The same principles apply to money laundering, fraud and terrorist financing. You need to be situationally aware of and understand the flow of funds for illicit purposes. Much the same, we all need to be situationally aware of the vulnerabilities to the financial system and ensure the BSA is as effective and efficient as it can be.

The most important BSA report is a SAR. In most instances, the biggest regulatory compliance breakdown resulting in some sort of enforcement or regulatory action is the failure to file SARs or to adequately file SARs. I cannot underscore enough that law enforcement is the direct beneficiary of SARs. Regardless of systemic inefficiencies, law enforcement consistently benefits from SAR filings.

SARs are used tactically to predicate and/or enhance criminal investigations. SARs are also used strategically for analytical purposes. When attempting to measure effectiveness and efficiency of SAR filing, we cannot solely rely on the percentage of SARs filed versus the number of SARs used to predicate or enhance an investigation. We must also factor in how SARs are used strategically for trend analysis and analytical purposes. Finding accurate metrics to determine the effectiveness and efficiency of SAR filing is extremely difficult.

When I was in law enforcement, I used SARs for both strategic and tactical purposes. When I was Chief of TFOS at the FBI, we established a financial intelligence unit. I wanted to know on a recurring basis what were the emerging threat trends, as well as emerging crime problems. SARs were one of the data sets we used for such trend analysis. We also used SARs for tactical purposes in furtherance of investigations. We used financial intelligence, some of which was derived from BSA data, to include SARs and CTRs, for tactical proactive investigations and for tactical reactive or more traditional "books and records" "follow the money" investigations. We used datamining technology for both strategic and tactical initiatives. I believe that the FBI continues to use BSA data for strategic and tactical investigative purposes.

I developed a flow chart I use for training purposes describing the "lifecycle" of a SAR. It tracks a SAR from the point of origin when it's filed with FinCEN through both regulatory and law enforcement review and investigative tracks. During their lifecycle, some SARs go directly to support investigations and some remain in the SAR database. A number of SARs that go into the SAR database will be used to support investigations at later times. Regardless of whether SARs are used to support investigations, they will be used in datamining initiatives to develop trend analysis or other strategic analyses.

Following my retirement from the FBI and as I have gained more of a financial institution perspective, based on my experience as a consultant, I have become more

sensitive to the perceived lack of feedback to financial institutions from FinCEN and law enforcement regarding the value of SARs and how SARs should be written to get law enforcements attention. FinCEN has done a good job of discussing the value of SARs in their SAR Activity Review publications. In recent years, FinCEN has recognized financial institution personnel as the front end provider and law enforcement agents as the back end consumer for outstanding investigations involving BSA data.

When I was Chief of Financial Crimes, and subsequently TFOS, I had frequent meetings with Jim Sloan. During that time period, Mr. Sloan was Director of FinCEN. We often discussed developing a SAR feedback mechanism from law enforcement through FinCEN to financial institutions. There were many impediments that existed at the time, much as they continue to exist today, that precluded us from developing a consistent feedback mechanism. Some impediments include the ongoing nature and secrecy of Federal grand jury investigations, the time lapse from when a SAR was filed and an investigation completed, resource constraints and other factors. Feedback regarding SARs warrants further consideration. This is an area where the Committee should consider dialogue with FinCEN and senior law enforcement executives.

The law enforcement utilization of SARs, as I have described how I used SARs as an FBI executive, was more at a program level than at the grass roots investigations level. At the program level there is a greater use of datamining and advanced analytics. At the grass roots field level, SARs are dealt with more in the form of individual manual reviews where each SAR is physically reviewed. For example, every U.S. Attorney's Office has a SAR review team. Even though the SAR review teams use excel spreadsheets and other analytics, they review SARs by hand. The reason this is important for the Committee is at the program level, I was more inclined to want to see more SARs filed. For our datamining purpose, more was better. At the grass roots level, SAR review teams would prefer to see less numbers of SARs filed. In this context, less is better. As a field agent and middle manager, I reviewed SARs manually, and I understand the grass roots perspective as well as the program perspective. Therefore, it is incumbent that as the Committee proceeds, you speak to a variety of law enforcement stakeholders to gain the best context available.

One final issue where law enforcement should be the primary stakeholder to potential legislation is the issue of CTR and SAR reporting thresholds. Since SARs were first implemented, the reporting thresholds have been the same. Periodically, banking associations and financial institutions have recommended that reporting thresholds be adjusted to account for inflation. I strongly believe that CTR and SAR reporting thresholds should remain as they are. Law enforcement would lose valuable financial intelligence if thresholds are raised. This is especially true for terrorist financing, where our primary threat is from homegrown violent extremists. My sense is that when we identify homegrown violent extremists and financial institutions run their names, a high percentage of them will have transactional activity involving CTRs.

As I've stated, at the core level, the flow of BSA data from the front end provider (financial institutions) to the back end consumer (law enforcement) is good. When financial institutions can be proactive and more targeted in their monitoring and reporting, the BSA data they provide is more effective and efficient. When the data flow becomes convoluted and more constrained, the system becomes more flawed and ineffective and inefficient.

Thank you again for affording me the opportunity to testify today. I look forward to responding to any questions you have.

19309 Winmeade Drive, #110 • Lansdowne, Virginia 20176

571.333.0300 • www.dmlassociatesllc.com

Getting to the root of the matter.

DML
ASSOCIATES, LLC

Perspectives, Partnerships and Innovation

By Dennis M. Lormel 1/18/2011

I have been blessed throughout my 38-year professional career to be associated with truly outstanding professionals. I spent 31 years in government service, 28 with the Federal Bureau of Investigation. The integrity and dedication I encountered among my law enforcement peers was noteworthy. I was extremely proud of my friendships and associations. Over the last seven years as a consultant working with compliance and fraud specialists, I have had the privilege of observing the same levels of integrity and dedication. I have likewise been proud of the friendships and associations I've developed in the private sector.

The primary difference between my law enforcement and private sector colleagues is perspective. Not many people recognize this important fact. Both my law enforcement and private sector contemporaries understand the importance of partnering with each other. Unfortunately, successful partnerships have been on a one-off basis and not systemic and sustainable. One reason for this is the difference in perspectives.

Many of the individuals I have had the honor to associate with in law enforcement and the private sector are innovative thinkers. However, in most instances, they have been unable to affect institutional innovation. Law enforcement and private sector institutions tend to operate in their safety zones, and frequently, innovation falls outside the institutional safety zone. As a result, there is little incentive to develop innovative techniques to fight fraud and money laundering.

This brings me to the point of this article: perspectives, partnerships and innovation.

Introduction

When it comes to fraud and money laundering, the bad guys are not constrained by boundaries. This affords them the opportunity to be proactive and imaginative in furtherance of their illicit activities. In fact, the more proactive and innovative the bad guys become, the more incentive they derive. Conversely, law enforcement and the financial services sector are frequently constrained by red tape and reluctance to implement change. Regulations, privacy considerations, policies, procedures, budgetary constraints and a myriad of other factors often serve as impediments to proactive measures and forward thinking. Regulations are such that reactive transaction monitoring and fraud detection in the financial services sector is the accepted norm. There is little incentive for innovation. Consequently, the bad guys have a considerable advantage.

As we've witnessed in the last few years, corporate frauds, investment frauds and mortgage frauds have devastated our economy. Add to that the continuous stream of check fraud, loan fraud and credit card fraud, not to mention health care fraud, and other crimes, and our economic problems are significantly compounded. The one constant in the various fraud schemes we have experienced is the ongoing need to launder these criminal proceeds. The intersection of fraud and money laundering should be the focal point for prevention and deterrence.

The time has come to take the advantage away from the bad guys in a sustainable and meaningful way. To achieve this, law enforcement and the financial services sector must first truly understand, embrace and act upon three words: perspectives, partnerships and innovation.

Perspectives

In many of the training presentations I have given since I retired from the FBI, I have commented that when I retired and became a consultant, I thought I knew everything I needed to know about bank anti-money laundering (AML) and fraud compliance and investigations. What I came to realize in a heartbeat was how little I actually understood about the AML compliance and investigative function. It was not a matter of not knowing, it was a matter of not understanding the financial institution compliance and fraud perspective. That was a humbling and educational experience. Over the last seven years, I have worked hard to understand and appreciate the financial institution perspective. For the benefit of my law enforcement friends, if I knew then (when I was in law enforcement) what I know now, I would have been dangerous. I encourage my law enforcement colleagues to learn from my experience and look beyond your perspectives when dealing with the private sector.

The reality is that many law enforcement officers do not understand the perspective of the bank compliance or fraud specialist. Likewise, many bank compliance and fraud specialists do not understand the perspective of the law enforcement officer. The first step in progressing to sustainable and meaningful partnerships is for the two sides to understand and respect the differences in perspectives.

The fundamental difference in perspectives is that law enforcement is driven by criminal investigations. They must focus on developing evidence to support criminal prosecutions. Bank investigators focus on identifying and reporting suspicious activity. These two focuses would appear compatible; however, in between law enforcement and the banks sit the regulators. Without assessing blame to anyone, the regulatory system is such that the banks have to satisfy the regulators before supporting law enforcement. This is where the greatest strain on understanding perspective exists. Law enforcement is focused on their criminal case. They generally do not understand the banks' dilemma in having to satisfy regulators when there are bad guys to put in jail. In the meantime, banks are not necessarily concerned about whether the bad guys go to jail. They are concerned about getting the bad guys out of their banks and how the regulators will respond. Exacerbating the problem is the fact that although regulations and laws are written in black and white, their implementation and interpretation are gray and subjective.

Law enforcement and financial institutions need to address the conflict in their respective perspectives and understand that each possesses information that would greatly benefit the other. Law enforcement

has investigative and intelligence information regarding schemes and trends. I frequently hear complaints and frustrations expressed by bank compliance and investigative specialists that law enforcement does not share such information. Conversely, banks contain an incredible repository of financial information and intelligence that would greatly enhance criminal investigations if law enforcement was aware of its existence or where to obtain it.

Law enforcement and financial institutions must come to terms with perspectives. Once that is achieved, the foundation will be set for more productive partnerships. Such partnerships will be better positioned to be sustainable and meaningful.

Partnerships

There have been a number of public and private partnerships that have achieved success. Most of these have been at the local or grass roots level. We need to develop more robust partnerships at both the grass roots and, more specifically, at the national level. The starting point should be with the realization that both law enforcement and financial institutions share the mutual responsibility to safeguard our financial system and their customers from fraud and money laundering.

One way to accomplish this is to develop crime problem specific partnerships. In doing so, law enforcement should develop case typologies specific to the crime problem and how the finances of the criminal activity flow through financial institutions. By sharing these case typologies and trend analysis information with the private sector, law enforcement will enable the private sector to more effectively and efficiently identify and report suspicious activity. By doing so, both sides benefit. Law enforcement develops evidence to support criminal prosecutions and/or, asset forfeiture and recovery. Financial institutions in turn will reduce institutional risk.

There is a great example of a public-private partnership that is crime problem specific and typologies driven. It was initiated by JPMorgan Chase (JPMC) under the leadership of William Langford. In 2009, JPMC Corporate AML founded a team dedicated to identifying and assessing immediate and strategic risks to JPMC. This outstanding team enthusiastically developed an issue-based approach by which they identified specific crime problems that presented them with significant risk. In 2010, JPMC identified human trafficking as a significant crime problem and a vehicle for institutional risk. Overall, the project developed typology-based surveillance models and investigator training to better enable the identification of potential human trafficking. JPMC's team of dedicated compliance and investigative professionals meticulously developed typologies which enabled them to identify transactional activity associated with human trafficking.

The next step was to develop active channels for coordination with relevant law enforcement agencies, especially those specifically focused on human trafficking. William and his team formed an outstanding working partnership with Immigration and Customs Enforcement (ICE), which has a dedicated group of agents assigned to investigate human trafficking. Through two way information sharing, JPMC was able to identify additional typologies while ICE was able to develop evidence to sustain criminal prosecutions.

Human trafficking is a heinous crime problem. The meaningful partnership formed by JPMC and ICE has begun to grow. In September 2010, during the annual ACAMS Conference, ACAMS executive vice president John Byrne hosted an informal, off the record, meeting between law enforcement and members of the ACAMS Advisory Board to discuss how ACAMS could facilitate partnerships between law enforcement and the financial services sector. Among some promising takeaways from that meeting came a subsequent meeting in Washington, D.C., between Byrne, advisory board chairman Rick Small, board member William Langford and senior executives at ICE. One of the topics was human trafficking.

Because of the devastating impact of this crime problem on its victims, ACAMS has formed a Human Trafficking Task Force, which Langford will chair. This initiative will provide a platform for the public-private partnership started by JPMC with ICE to grow and become more sustainable. In furtherance of this effort, on January 13, 2011, ACAMS hosted a free webinar training session on human trafficking. Byrne served as moderator along with ICE agent Angie Salazar, who provided a compelling training session. Education and training promote awareness, which frequently leads to action.

In establishing the issues based approach, JPMC did not settle for a traditional or reactive transaction monitoring framework. Langford and his team took an innovative and proactive approach to dealing with challenging crime problems. It should be noted that JPMC is not alone in developing innovative approaches to identifying and reporting suspicious activity. JPMC represents but one example of how certain financial institutions are gravitating toward the use of more proactive mechanisms.

Innovation

Langford's team conducted extensive research to develop typologies. They relied on data mining and proactive targeted model development. By being proactive and focused, JPMC more effectively and efficiently identified suspicious activity consistent with human trafficking. The methodology developed by JPMC should serve as a model for future transaction monitoring models.

The industry needs to be less predictable in transactional monitoring and more targeted and proactive. There needs to be a balance between traditional reactive transaction monitoring and crime problem specific proactive targeted monitoring. A balanced approach between reactive and proactive monitoring would keep the bad guys off balance in their efforts to exploit areas of vulnerability.

A challenge going forward with this approach is incentive. The incentive for JPMC was doing the right thing. In terms of tangible incentives for financial institutions to implement similar typologies and methodologies, there is little. This is where the regulators could be a factor. If there was a regulatory incentive to develop crime problem specific monitoring typologies and proactive techniques, more financial institutions would be inclined to develop programs similar to JPMC's. This would significantly increase the generation of more consequential suspicious activity reports.

JPMC has applied the issues based approach to other significant crime problems. Hopefully, as they reach out to the relevant law enforcement agencies to form partnerships, those agencies will respond as

well as ICE did regarding human trafficking. Building meaningful and sustainable public-private partnerships is the best way to take the advantage away from the bad guys.

Conclusion

Since the bad guys are not constrained by boundaries when it comes to fraud and money laundering, it is incumbent that law enforcement and the financial services sector share the responsibility to contain and disrupt criminal activity. The more proactive and coordinated law enforcement and industry are the more likely they are to deter the bad guys. The combination of perspectives, partnerships and innovation will provide the framework needed to stem the tide of fraud and money laundering.

PREPARED STATEMENT OF HEATHER A. LOWE

LEGAL COUNSEL AND DIRECTOR OF GOVERNMENT AFFAIRS, GLOBAL FINANCIAL INTEGRITY

JANUARY 9, 2018

Thank you for the opportunity to testify before you today on the subject of Combating Money Laundering and Other Forms of Illicit Finance and the Opportunities to Reform and Strengthen BSA Enforcement. I hope that my contributions to today's hearing will help you take measured and informed decisions that are in the public's interest with respect to the U.S.'s anti–money laundering (AML) regime as set forth in the Bank Secrecy Act (BSA).

Money laundering is a vast subject and there are many different facets that it would be worthwhile for this Committee to examine. I will discuss some of those areas in my testimony today but, as I am sure you will discover as we delve deeper into the topic, there may be a great deal more that you wish to explore moving forward. I am happy to assist to the extent that I can.

In my testimony, I will provide information and opinions regarding the following: Trends in compliance, Suspicious Activity Reports (SARs), Know Your Customer (KYC)/Customer Due Diligence (CDD), and the balance of activity and obligations between the Financial Crimes Enforcement Network (FinCEN) and the private sector. Some of my remarks will directly address recent proposals by The Clearing House in their publication "A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement", as I am sure that you are giving consideration to those proposals. (CFT refers to countering the financing of terrorism.)

Some of the key points that I will be making in my testimony are:

1. Money laundering and the technology that can help us combat it are both evolving and, in light of this, it is appropriate to consider whether changes to our regulatory structure should be made. Equally, however, it is critical that Congress consider and carefully weigh the potential benefits against potential negative ramifications before making decisions in this area.
2. Enforcement against money laundering is primarily through identification of regulatory infractions as opposed to through criminal charges of actual money laundering. This may be because it is much easier to find evidence of regulatory infractions, the burden of proof is lower, and it is far less costly for the Government than pursuing a criminal money laundering charge, and there is a clear dissuasive effect. Despite this, when we look at the cases where enforcement was merely through identification of deficiencies of AML systems and filing requirements, the hallmarks of serious criminal money laundering are there in the cases. As a result, decreasing the ability to enforce using the regulatory approach may have serious, negative repercussions on compliance and, ultimately, criminal access to the U.S. banking system.
3. It is critical that information about the natural person(s) who own or control companies (the beneficial owners) is finally collected by either the State or Federal Government and is made available to law enforcement and to financial institutions. Companies with unknown or hidden ownership are the number one problem in the AML world and the U.S. cannot continue to allow our failure to act to put the U.S. and global financial system at risk.
4. I would strongly caution against transferring responsibility for setting AML priorities for individual banks from those banks to FinCEN. Banks are best placed to understand their business and their systems and the money laundering risks inherent therein, and create the systems that work best in their business models to combat money laundering. FinCEN and/or other regulators should review those assessments but cannot be responsible for carrying them out.
5. The Clearing House recommends greater information sharing among banks and with the Government in a number of ways. While we generally support greater sharing of information in the AML area, it must be done with appropriate privacy safeguards. Where it may result in a person being denied banking services at all, there must be a system for redress for people to be able to restore that access if they can demonstrate that they are involved in legitimate activity.
6. Transferring raw banking data from banks to FinCEN to analyze (with appropriate privacy safeguards) is not a bad idea. However, it is essential that we do not absolve banks of the responsibility to carry out their own analysis as well, which they have the ability to review within the context of the additional

client information that they have, because they are the gatekeepers to the financial system. The Federal Government cannot do this alone.

7. AML compliance and reporting is undertaken by a wide range of entities and persons, going far beyond the banking sector. Any proposed changes should consider the implications for all of these types of entities and persons.
8. Some types of entities and persons should be required to have AML programs in place that currently do not, such as those involved in real estate closings, lawyers, and others. The banking sector cannot and should not carry this responsibility alone, especially where these persons act as a proxy to open the door to the financial system for criminals and their money.
9. Suspicious Activity Reports are meant to be just that, reports of "suspicious" activity. Requiring bank employees to determine if activity is in fact illegal before filing a SAR would be counterproductive for a number of reasons, including increasing the burden on bankers who would consequently have to make a new, legal determination.
10. Congress should request from the various regulators data regarding formal and informal enforcement actions pertaining to AML/BSA violations and deficiencies so that they are able to independently asses the appropriateness of the enforcement regime currently in place.
11. Both small banks and large banks have been the subject of major money laundering cases.
12. Money laundering and sanctions violation cases over the past few years relate to willful, knowing, and egregious violations of U.S. laws and regulations that have resulted in U.S. and foreign banks granting access to hundreds of millions of dollars in funds supporting genocide and funds supporting major, violent South American drug cartels into our system, to name a few examples. The fines that have resulted from these cases have been seen by the banking industry as heavy and so banks have begun to take AML regulations that have been in place for many years more seriously as the possibility and repercussions of enforcement have increased. I would therefore remind Members of Congress that the regulatory "burden" has not actually been increasing, the threat of being found out is what has actually increased.

Preface: Who Has AML Compliance Responsibilities?

One thing to keep in mind for the purposes of AML is that the term "financial institution" (FI) is defined very broadly and encompasses a much wider range of types of entities than most people realize. Being classified as a financial institution means that an entity must generally have some sort of AML compliance in place, with the main types of FIs [1] being required to have an AML compliance program, conduct customer due diligence and know your customer checks, monitor accounts, and file suspicious activity reports and currency transaction reports. I have included the definition of "financial institutions" at the end of this testimony for information. Today you have before you representatives from three banking associations, but it is important to consider that any changes to the AML/CFT regime will affect a much wider range of entities and persons, such as currency exchanges, casinos, dealers in precious metals, stones or jewels, pawn brokers, and insurance companies, which you should also factor into your decision making.

There are also a few persons that ought to have U.S. AML obligations but currently do not. Although banks serve as an immediate gateway into the U.S. financial system and must therefore bear significant responsibility for preventing criminals and other wrongdoers from finding safe haven here, they shouldn't bear that responsibility alone. Other actors that handle large sums of money, such as persons involved in real estate transactions, escrow agents, investment advisors, lawyers, corporate service providers, and accountants must also take responsibility for knowing with whom they are doing business and guard against their services being used to launder dirty money. Excluding these nonbank sectors renders the U.S. financial system vulnerable to serious, ongoing money laundering threats as shown by multiple media reports about how, for example, anonymous ownership of high-value real

[1] This includes insured banks, commercial banks, agencies or branches of a foreign bank in the U.S., credit unions, savings associations, corporations acting under section 25A of the Federal Reserve Act 12 U.S.C. 611, trust companies, securities broker-dealers, futures commission merchants (FCMs), introducing brokers in commodities (IBs), and mutual funds. FATF Mutual Evaluation Report of the United States, December 2016, available at *http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.*

estate facilitates money laundering,[2] a *60 Minutes* segment showing how lawyers facilitate money laundering by corrupt foreign Government officials,[3] and of course the Panama Papers which disclosed how corporate formation agents and lawyers help wrongdoers hide and launder criminal proceeds.

Technically, persons involved in real estate closings are already classified as FIs per the definition established by the USA PATRIOT Act in 2001, but they were given a "temporary exemption" (which had no sunset clause) from AML compliance requirements in 2002. Despite Treasury conducting a comment period with respect to AML compliance in the real estate sector in 2003, they have not removed that temporary exemption. Congress should consider doing so.

Addressing the money laundering risks posed by these nonbank sectors and actors would finally bring us in line with international anti–money laundering standards—agreed to by the U.S., as a leading member of the Financial Action Task Force (FATF), the international anti–money laundering standard-setting body. In FATF parlance, most of these persons are referred to as "Designated Non-Financial Businesses and Professions". Members of FATF, including the U.S., are supposed to require most of these persons to have AML compliance programs, and many of its member countries have already done so.

I. Trends in Compliance

A. Understanding Regulatory Enforcement Data

As you know, the money laundering realm is governed by statutes which both criminalize the act of laundering money[4] and impose civil and criminal penalties for the failure of a financial institution to have an effective AML program.[5] Under Federal law, the type, nature, and scope of a financial institution's AML systems and controls depend upon the institution's risk profile, which differs significantly for banks that, for example, serve a local, rural community versus a global institution that operates in high-risk foreign environments. A financial institution's risk profile depends upon its assessment of the types of risks it faces, which are a function of where it operates, what products and services it offers, and what clients it takes on, among other variables.

Developing accurate risk assessments and AML compliance regimes is therefore an art and not a science, and requires a great deal of judgment. It is the job of the regulators to determine if a financial institution has gotten it right—whether the FI's risk assessment is comprehensive and reasonable, whether its AML systems and controls are appropriately responsive to those risks, and whether those systems and controls are effective. The examination reports that result from regulators' reviews are highly confidential and exempt from public records requests,[6] although this Committee has the authority to review those examination reports should it want to review their content and reasonableness.[7]

My organization was hired by a third party in 2015 to undertake a confidential study of AML enforcement in the U.S. and the U.K. between 2001 and 2015. That study was carried out by myself and our Policy Counsel Elizabeth Confalone. I have permission to share some of our observations from that report with you today, but unfortunately I am unable to share the entire report.

One of our primary observations was that, apart from the rather small number of publicly available deferred prosecution agreements (DPAs) and nonprosecution agreements (NPAs) that financial institutions have entered into with respect to AML-related activity, it is extremely difficult to determine the number and nature of the formal and informal enforcement actions taken by regulators in response to BSA/AML deficiencies because (i) very little information about informal actions is available to Congress or the public, (ii) information about formal actions is not in a machine-readable format—meaning that one must open and read every file to know what the infraction(s) was, and (iii) "actions" taken by regulators do not always indicate misconduct—an "action" for the FDIC terminating deposit insurance for a banking unit whose deposits were transferred to another bank within the

---

[2] See, e.g., The *New York Times* series "Towers of Secrecy" available at *https://www.nytimes.com/news-event/shell-company-towers-of-secrecy-real-estate.*

[3] Can be accessed at *http://www.cbsnews.com/news/anonymous-inc-60-minutes-steve-kroft-investigation/.*

[4] 18 U.S.C. §§1956–1957.

[5] The Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C. §5311 et seq. (regulations at 31 CFR Ch. X).

[6] Exemption of examination reports from public availability. See 12 CFR §261.14 (Federal Reserve Board); 12 CFR §309.5(g)(8) (FDIC); 12 CFR §4.12(b)(8) (OCC).

[7] Prohibition on banks disclosing information from their examination reports. See 12 CFR §261.20(g), 12 CFR §261.2(c)(1) (Federal Reserve Board); 12 CFR §350.9 (FDIC); 12 CFR §18.9 (OCC).

group is lumped together with an "action" for the systemic violation of U.S. sanctions laws.

A second observation was that, based upon a review of the enforcement actions that could be identified as related to AML deficiencies, the Federal Government rarely charged a financial institution with the criminal offense of money laundering, favoring instead a finding that the institution had violated Federal requirements to have an effective AML program and report suspicious activity to law enforcement. This was the approach even when the hallmarks of criminal money laundering seemed clearly present in the cases. This may be because it is easier to prove deficiencies in AML compliance than it is to meet the criminal standard of proof for money laundering. In light of this, it is important to carefully consider how, for example, shifting responsibility for AML risk analysis for FIs and aggregate data analysis from the private sector to FinCEN (as has been proposed in different ways by The Clearing House) could hamper the Government's use of civil enforcement actions to combat money laundering, which uses far less time and fewer Government resources than criminal prosecution would entail, with important dissuasive results.

B. What Does an Overview of Selected Enforcement Tell Us?

The best source of data on AML/BSA-specific enforcement actions providing sufficient detail for adequate analysis are (i) nonprosecution agreements (NPAs) and deferred-prosecution agreements (DPAs), and (ii) FinCEN data. My organization, Global Financial Integrity, reviewed those data sets in order to conduct a more detailed analysis of AML/BSA-specific violations and trends in enforcement. I will discuss each of these in turn.

FinCEN Enforcement Actions

Unlike bank regulatory agencies that tend to be more concerned with ensuring the general health and stability of our financial system, FinCEN's specific mission is to "safeguard the financial system from illicit use and combat money laundering and promote national security."[8] As a result, FinCEN's enforcement actions relate solely to issues involving money laundering and illicit finance.

Given the available data, we analyzed 61 separate actions[9] against 52 different banks.[10] There were 26 American banks subject to FinCEN actions, and 26 foreign banks and U.S. branches and offices of foreign banks that were subject to FinCEN actions. Each case involved multiple failings over a period of years, making categorization of the violations challenging.

Within the FinCEN actions, the most common thread was a failure to file suspicious activity reports, however the violations were usually accompanied by a large range of other AML system violations such as a failure to carry out customer due diligence, failure to verify the source and use of funds, failure to identify red flag activity, failure to have an adequate AML program, failure to have enough compliance staff, and failure to train staff, among other deficiencies.

Among the full body of 61 cases, 13 of the actions included problems relating to money service businesses (MSBs) (mainly foreign) and the processing of the cash and monetary instruments by those MSBs, including issues with the identification and risk-rating of MSB clients. Ten of the actions involved problems with the management of foreign correspondent accounts and the processing of the cash and monetary instruments for correspondent accounts, including the identification and risk-rating of the clients. Several banks had violations relating to their failure to file required currency transaction reports, and there were a hodge-podge of other specific violations as well, such as fraud and problematic trade finance activity. Five of the actions involved banks that had foreign Politically Exposed Person (PEP) clients, some coupled with failures to carry out adequate customer due diligence on those PEPs, to verify the source and use of funds, or monitor the client accounts appropriately.

The FinCEN actions contained damning details illustrating the banks' failures, but were always drafted to focus on the civil law violations as opposed to the activity that might, in fact, be criminal. For example, The Foster Bank, based in Chicago, was sanctioned by FinCEN for violations relating to having an ineffective money laundering program in place. Illustrating the types of activity that Foster's AML deficiencies permitted to occur, the FinCEN action states:

---

[8] Financial Crimes Enforcement Network, Mission Statement, available at *http://www.fincen.gov/about_fincen/wwd/mission.html.*

[9] Technically, the DPAs and NPAs are "cases" and the FinCEN notices are "actions," however for ease of reference we will use the term "actions" here.

[10] In a few instances there was both a FinCEN action, as well as a DPA or NPA relating to the same bank activity, and we have counted those as one case each because they cover the same bank activity.

> For example, from April 1999 through August 2002, one customer who operated a sportswear business purchased approximately $674,390 in cashier's checks, all individually purchased below the $3,000 Bank Secrecy Act record-keeping threshold for monetary instrument transactions. Concurrently, from April 1999 through August 2002, the same customer engaged in a pattern of structured transactions involving over $6,199,616 in cash deposits in amounts under $10,000 per deposit. Ultimately, in December 2002, the Bank discovered that this customer had conducted nearly $10 million in cash transactions between April 1999 and November 2002.
>
> Another Foster customer routinely made cash deposits in the amounts of $9,900 up to four times daily. The Bank retained no documentation in its file to support a legitimate business reason for these deposits.
>
> Other customers engaged in large aggregate cash transactions, totaling an average of $300,000 to $600,000 per month, at least some of which appeared to be designed to avoid currency transaction reporting. Foster did not have documentation supporting the legitimacy of the customers' banking activities and failed to file timely suspicious activity reports for these customers.[11]

This description indicates that that these customers were engaging in activities that were likely illegal, given the lengths that they went to in order to the avoid money laundering reporting requirement that deposits of $10,000 or more be reported to FinCEN on a Currency Transaction Report (CTR). The FinCEN action is concerned with Foster's failure to identify these avoidance techniques, but we can find no corresponding case in Illinois where the bank is actually charged with the criminal act of laundering money for its clients. At the time we conducted this research, we did not find any records relating to prosecution of persons in Illinois who used the accounts at Foster Bank, although a case against an individual might not mention the bank's name. Therefore, while this case has multiple hallmarks of money laundering activity, there was no prosecution for the laundering that we could find. Further, we were unable to find evidence that these clients' activities were even investigated by Illinois State or Federal authorities.

Having reviewed the FinCEN actions, we are under the impression that the vast majority of the sanctioned banks knew or should have known (as is the standard) that their services were being used to launder proceeds of some sort of illegal activity (although they may not have known precisely what kind of illegal activity), and that some of the banks may have either been established for that specific purpose, or the banks' business was somehow taken over by those clients. This misconduct is most evident in the cases relating to small banks, where in several cases the clients that were engaging in activity that should have raised red flags and caused the banks to file SARs were a large percentage of the small bank's business.

For example, North Dade Community Development Federal Credit Union was a nonprofit community development bank based in North Dade County, Florida, with $4.1 million in assets. As a community development bank, its clients were supposed to be limited to people who live, work or worship in the North Dade County area. North Dade had only one branch and only five employees. Despite its small, local focus, North Dade was servicing multiple money service businesses that were located outside of its geographic field of membership and that were engaging in high-risk activities. For example, records showed "(1) deposits in excess of $14 million in U.S. cash that was physically imported into the United States on behalf of nearly 40 Mexican currency exchangers, and (2) hundreds of millions of dollars in wire transfers to foreign bank accounts of MSBs located in Mexico and Israel."[12] It is difficult to believe that the bank's five staff members were unaware of the likelihood that the bank was being used to launder money via their MSB clients, and it is wholly possible that the bank was either established to carry out illegal activity or was overtaken by criminal clientele.

DPAs and NPAs

We also reviewed deferred prosecution agreement and nonprosecution agreements (DPAs and NPAs) related to BSA/AML violations, which we drew from the University of Virginia School of Law's Federal Organizational Prosecution Agreements col-

---

[11] FinCEN, "Assessment of Civil Money Penalty Against the Foster Bank", Case No. 2006-8, at 5, *http://www.fincen.gov/news_room/ea/files/foster.pdf.*

[12] FinCEN, "In the Matter of North Dade Community Development Federal Credit Union", Number 2014-07, at 7, 8, 9, Nov. 25, 2014 (hereinafter, "FinCEN North Dade Enforcement Action"), *http://www.fincen.gov/news_room/ea/files/NorthDade_Assessment.pdf.*

lection.[13] As you know, NPAs and DPAs represent a step beyond agency enforcement actions. They represent settlements of criminal and civil cases brought by the Government against corporations where the corporation generally admits to certain facts, agrees to take certain remedial measures, and often pays a fine in exchange for the Government deferring or discharging the prosecution. In the case of NPAs, the matter is settled once the Government has signed the agreement. In the case of DPAs, the Government has the option of renewing the prosecution if the company does not implement the required remedial measures or continues to otherwise act unlawfully.

The DPAs and NPAs we reviewed settled actual cases against banks brought by the U.S. Department of Justice. We reviewed 36 DPAs and NPAs involving banks. Eleven of those did not involve AML/BSA-related infractions. Eight of the agreements related to sanctions-busting violations, where the banks were stripping wires of key information, re-routing the wires, or taking other actions to evade U.S. sanctions laws. Fourteen cases involved money laundering violations, ten of which were also the subject of FinCEN actions, and therefore included in the analysis above. Only four banks were the subject of money laundering-related DPAs/NPAs that did not have a corresponding FinCEN action. Five of the cases were against large, international banks for aiding and abetting large-scale tax evasion by Americans. Several cases were included in the count of both the sanction violations and money-laundering categories because their conduct and the terms of their agreements included both types of violations.

Several of the money laundering cases involved funds being moved from developing or middle income countries into the U.S. via money service businesses or correspondent banking activities. The majority of the countries involved were South or Central American (mainly focusing on the Black Market Peso Exchange) or Middle Eastern. One case involved a bank in Nigeria and one case involved Russian banks. The countries that arise in these cases are not surprising in light of the American political priorities of fighting drug crime and terrorist financing.

Some Useful Perspective

Lastly in this section, I'd like to remind Members of the Committee that although the headline-grabbing figures relating to BSA/AML enforcement for FIs' may seem large, they pale in comparison to some of the egregious, willful violations taking place. Two examples:

HSBC USA was fined a mere $1.9 billion in 2012 for:

- Failing to have required money laundering controls applied to over $200 trillion in wire transfers it received over a 3-year period (that's about 3x global GDP),
- Of which $670 billion came from Mexico, which it had classified as a low risk country for money laundering although the U.S. Department of State and many, many others classify it as high risk, and
- Of which $881 million was determined to be proceeds of drug trafficking by the Mexican Sinaloa Cartel and the Columbian Norte de Valle Cartel.
- Bear in mind that we have no idea what other percentage of that $200 trillion was dirty money flowing through HSBC USA because the AML controls were turned off.
- Failing to have the required money laundering controls in place with respect to the purchase of $9.4 billion in cash from its Mexican subsidiary.
- Processing wire transfers with inadequate information that were the result of other HSBC subsidiaries' efforts to ensure that U.S. dollar transactions from sanctioned countries like Iran and Libya were cleared in the U.S.

BNP Paribas, France's largest bank, was fined $8.9 billion in 2014 for:

- Processing over $190 billion in transactions through its New York office for clients in the sanctioned countries of Sudan, Iran, and Cuba,
- at one point providing over half of the banking services in use by the Sudanese Government, enabling this Government, sanctioned by the U.S. for perpetrating genocide, to process its oil money (denominated in dollars) and continue to purchase the weapons it needed and pay its soldiers to continue to engage in mass-murder, and
- knowingly providing banking services in U.S. dollars for people subject to individual and specific sanctions.

---

[13] Brandon L. Garrett and Jon Ashley, "Federal Organizational Prosecution Agreements", University of Virginia School of Law, at *http://lib.law.virginia.edu/Garrett/prosecution_agreements/*.

C. Conclusion of Analysis and Recommendation

Our analysis of the AML enforcement data showed that small banks, even local banks, can be and are used to move illicit funds in the same way that large, international banks are used. In addition, our analysis of the DPAs, NPAs, and FinCEN actions establishes that banks of all sizes knowingly and intentionally facilitate the movement of illicit funds. In none of the cases reviewed does it appear that the bank was unwittingly involved in the movement of illicit money, many of which appeared to have been the subject of previous regulatory warnings. SAR filing violations were a factor in almost every single one of these cases, but they were far from the most serious violations.

Due to the limitations on access to data, our analysis is incomplete. Additional analysis should be undertaken prior to making major alterations to the existing U.S. AML regime. We therefore recommend that the Members of the Committee undertake a more in-depth review of the AML enforcement data prior to making any policy changes. This review could include requesting each regulator to identify which of their formal and informal enforcement actions over the last 10 years relate to AML/BSA or sanctions violations and to include information in the searchable/sortable data fields indicating the type of infraction involved and the laws or regulations that were violated. In addition, we recommend that the Committee obtain the documents related to a sample of the formal and informal enforcement actions taken by each agency to get a better sense of the misconduct involved and the quality of enforcement actions taken. Finally, it would be ideal if all the regulators adopted the same fields and display format on their website. This will allow for more effective and efficient Congressional oversight moving forward, and make it easier for FIs to search the data to identify evolving criminal methods and trends.

II. Suspicious Activity Reports (SARs)

The Nature of SARs. Suspicious Activity Reports (SARs) are an important part of the BSA/AML framework, but the nature of SAR filing has changed over time and could be reviewed. It is important for the Committee to understand that SARs were intended to be just that, reports of suspicion of criminal activity. They are not called illegal activity reports, because FI employees are not required to determine if the activity they are seeing is actually illegal. Instead, FI employees are supposed to file reports where they see something out of the ordinary and simply have a suspicion that there is a problem. Requiring bank employees to go further and make a determination that an activity is actually illegal would be an unrealistic and unwarranted expectation. There is no "bright line" test for when a SAR should be filed because that is contrary to the intended nature of a SAR.

The Clearing House has nevertheless proposed that further guidance be provided by FinCEN to "relieve financial institutions of the need to file SARs on activity that is merely suspicious without an indication that such activity is illicit." That recommendation would fundamentally change the nature of SAR reports and would actually make bank employees' tasks much more difficult and risky. After all, it clearly requires a greater amount of effort and legal analysis to determine whether an activity is, in fact, illicit rather than merely suspicious.

One source of tension in this area appears to be that law enforcement wants SARs to include as much information as possible, in as standard a format as possible, and that their demands for greater detail and specificity have grown over time. FI employees may not have the desired level of detail that law enforcement would like, but that is simply a reality of money laundering cases which often involve hidden conduct and individuals. The SAR instructions properly allow FI employees to indicate on the form that the information is "unknown"; that option should be honored by law enforcement rather than trying to require FI employees to become detectives uncovering illegal conduct.

The Sharing of SARs. The Clearing House has proposed that new regulations allow FIs to share SAR information among foreign affiliates and branches. GFI supports this recommendation; its importance was made clear in the HSBC case. A related issue, however, is what actions FI's affiliates and branches are required or permitted to take in response to receiving this information. I understand that there have been cases where a person's accounts have been closed by a bank because it received information that another bank identified the person as suspicious, making it difficult for that person to establish banking relationships elsewhere. If FIs are permitted to close accounts based upon suspicions communicated to them by other banks, Congress should ensure that there is some mechanism for appeal or redress for individuals wishing to establish their bona fides. Such closure of accounts may also serve to "tip off" the account holder that they are the subject of a SAR, contrary to the SAR confidentiality requirements.

Integrating New Technology. I am in favor of exploring the ways in which today's (and tomorrow's) technology can be used to innovate in the AML compliance sphere and believe that the Government should be supporting such innovation (usually referred to as "FinTech"). Northern Europe seems to be leading in this space, and it would be helpful to create a better environment for such innovation in the U.S. I therefore support the creation of a technological "sandbox", as has been proposed by The Clearing House and has been implemented in the U.K. The U.K. structure appears to have some specific safeguards to protect consumers, however, which they consider to be an integral part of their system. I have not had an in-depth look at the U.K. program, however regulators presented it at a recent FATF industry consultation meeting I attended. They stressed the importance of ensuring that consumers were protected at all times as innovative approaches were being tested, and the U.S. should do the same. It is important to note that, in the House of Representatives, Members are discussing legislative language that does not require any of the safeguards present in the U.K. system, potentially giving FIs an unlimited safe harbor for the use of any new technology with no Government oversight. This is a significant danger because if an FI spends the money to integrate new technology that, it turns out, isn't as effective as alternative methods, they would have no incentive to change their approach. They would incur some unwelcome cost for doing so and they'd have the security of an unlimited safe harbor, so there would be no incentive to act.

III. Know Your Customer (KYC)/Customer Due Diligence (CDD)

As part of their customer due diligence, or CDD, procedures, FIs are supposed to know their customers by engaging in Know Your Customer, or KYC, procedures. In banking terms, knowing your customer is more than just knowing who the owners or controllers of the company are (known as "beneficial ownership" information), it is also understanding how that legal or natural person will be using the account so that the account can be appropriately monitored for possible money laundering activity. Establishing the expected normal use of the account is imperative if the FI is to effectively monitor for suspicious activity going forward. Moreover, characteristics of the beneficial owner of the account (such as nationality/residence, whether a politically exposed person (PEP), etc.), the type of business using the account, whether that business is cash intensive, and many other factors all contribute to an account's risk profile, and that risk profile determines what type and level of monitoring the account will be subject to.

Beneficial Ownership Information. Knowledge of the beneficial owner(s) of a company holding an account is a critical question in KYC, however. Therefore, one Clearing House proposal that GFI wholeheartedly supports is its proposal that information about the beneficial owners of U.S. companies—the actual individuals who own or control those companies—should be collected at the time that companies are incorporated in the U.S. and that this information should be made available to law enforcement and financial institutions. This is an issue that has been gaining visibility and urgency on a global level. This is because anonymous companies, or companies with hidden owners, are the most frequently used vehicle for money laundering. That's why identifying who owns or controls a company is a fundamental step necessary to combat the problem.

In response to the global movement towards greater corporate ownership transparency, in May 2016, the U.S. Treasury Department adopted a regulation which more explicitly requires banks to obtain beneficial ownership information beginning in May 2018. Unfortunately, that regulation includes some significant loopholes and so has not been deemed compliant with international AML standards in the most recent evaluation of the U.S. AML system by the IMF. Hopefully, Treasury will be making improving that regulation a priority in order to bring the U.S. into compliance with international AML standards and ensure that true beneficial ownership information is being collected.

But whether or not the U.S. improves its regulation, U.S. banks that operate in other countries are already subject to strong corporate transparency standards that are only getting stronger. As a result, the multinational banks that belong to The Clearing House want beneficial ownership information for U.S.-formed entities to be collected by either those who incorporate the companies or by an appropriate Government entity so that they can use the information as a key data point in their customer due diligence process. While we do not support banks being allowed to rely exclusively on this information in their customer due diligence procedures, the information could and should be an extremely helpful starting point in the "know your customer" process and as a tool to verify information supplied by the client. Accordingly, we strongly support The Clearing House beneficial ownership proposal, which is soon to be the subject of bipartisan legislation in the House and Senate.

I wanted to note that in discussions of relevant legislative text in the House of Representatives, some Members have been pushing the idea that law enforcement should only have access to information about the beneficial owners of companies if they can produce a summons or subpoena, while at the same time not discussing any limitations on availability of the information to the banks. As a fundamental principle, U.S. law enforcement should have free access to beneficial ownership information because it is critical information they have been requesting for years, as evidenced by their many letters of support for beneficial ownership bills introduced over the past 10 years. We should not, under any circumstances, have a situation in which the banks have easy access to this information and our law enforcement does not. I would also note that last month, the European Union adopted legislation which requires all 28 EU Member States to create registers of beneficial ownership information and for that information to be made available to the public, including law enforcement and financial institutions. The U.K. already has such a public registry in place, and countries such at Ghana, the Ukraine, Afghanistan, Kenya, and Nigeria are all actively working on putting the same in place. At this point, free access by law enforcement and banks must be seen as a minimum standard.

IV. The Balance of Activity and Obligations Between FinCEN and the Private Sector

The Clearing House has proposed that (i) for the large multinational FIs, all enforcement power should be consolidated within FinCEN, (ii) data collection and analysis should be shifted from the private sector to FinCEN, and (iii) for the large multinational FIs, FinCEN/Treasury should establish priorities for each FI on an annual basis, review progress with each FI every 3 months, and oversee any examination of an FI. I'll address each in turn.

Consolidation of AML Enforcement Power. While the proposal to consolidate AML enforcement power in FinCEN has surface appeal, it would also be at odds with a major principle in Federal law regulating FIs. Federal law now authorizes different functional regulators to regulate different FI activities in order to make use of their specialized expertise. For example, the SEC is given primacy over securities activities at FIs because it understands the securities markets and their inherent risks. Similarly, the Commodity Futures Exchange Commission oversees AML issues affecting commodity trading, and State insurance regulators examine AML issues affecting FI insurance activities, again because each regulator is expert in their own field. If AML enforcement power were instead consolidated in FinCEN, the sector-specific AML experts now working at the individual regulators would have to be transferred to FinCEN, swelling its ranks and reach. There are strengths and weaknesses to continuing the current disaggregated AML oversight system versus concentrating AML oversight at FinCEN, and the issues and tradeoffs would need to be carefully thought through.

Data Collection and Analysis Transferral to FinCEN. The suggestion that FinCEN be given access to bulk data transfers from FIs to enable it to analyze AML trends and patterns across institutions is another potentially useful idea. But questions about the effectiveness and cost of this proposal include whether FinCEN currently has the technological capability and personnel needed to perform that type of data analysis or whether it would need to be built, which could be a significant expense. In addition, charging FinCEN with industrywide data collection and analysis should not be seen as a way for banks to absolve themselves of their AML obligations. The banks would retain their position as the primary gateway into the U.S. financial system, so the first level of responsibility to safeguard the system against money laundering abuses must remain with the individual banks who open their accounts to individuals and entities around the world.

Requiring FinCEN To Establish AML Priorities. The third proposal, to essentially charge FinCEN with establishing annual AML priorities for every large multinational bank and monitoring every bank's progress every 3 months, is extremely ill-advised. The FI understands its own business and products better than anyone else. It is therefore best-placed to determine what its AML risks are and how best to address those risks within the systems that it has created. We support the idea of an FI working with FinCEN/Treasury to discuss those risks in the context of national and global trends observed by FinCEN, and whether adjustments might be made as a result, however. In addition, reviewing each FI's progress in AML every 3 months seems like far too short a time frame to observe how an FI is progressing in this respect, however, and entirely impractical from a Government resource allocation perspective.

Creates Bigger Government. Overall, it is critical that the Committee understand that changes of the magnitude suggested by The Clearing House would require a significant appropriation from the Federal budget to pay for, among other things,

a very large staff increase and procedural and technological improvements at FinCEN. In addition, many new regulations would have to be drafted to give effect to these changes. The result would be a much bigger Government agency and a bigger FinCEN impact on AML activities. Careful analysis is needed to determine whether the benefits of each of these changes would outweigh the costs.

V. Conclusion

In conclusion, positive changes can be made to the AML regulatory structure, but they must be made carefully, with good data, and only after thinking through as many of the potential ramifications as possible.

Unfortunately for the banking community, many of the high profile, incredibly egregious cases that involve the biggest banks in the world have eroded public trust that banks will indeed act in a manner that is law-abiding and actively try to turn away proceeds of crime. Even many bankers lack faith in their institutions. The Members of this Committee may find a 2015 study by the University of Notre Dame and the law firm of Labaton Sucharow, entitled "The Street, the Bull, and the Crisis", to be of interest. The researchers surveyed more than 1,200 U.S. and U.K.-based financial services professionals to examine views on workplace ethics, the nexus between principles and profits, the state of industry leadership and confidence in financial regulators. As the report states, "The answers are not pretty. Despite the headline-making consequences of corporate misconduct, our survey reveals that attitudes toward corruption within the industry have not changed for the better." [14]

Some of the banks that have been the subject of these high-profile, egregious cases are members of The Clearing House, whose proposals for regulatory change are before this Committee. That does not necessarily mean that the proposed changes are unwarranted, but it is the responsibility of Congress to make informed decisions about the extent to which each of these proposals is also in the public interest. Deregulation for the sake of deregulation in the AML area is most certainly not in the public's interest. Making it easier for banks, knowingly or unknowingly, to take in greater inflows of drug money, the proceeds of human trafficking, the ill-gotten gains of foreign dictators, and terror financiers is not in the best interest of anyone.

Thank you for the opportunity to share my views on such an important topic.

[14] "The Street, the Bull, and the Crisis" is available at *https://www.secwhistleblowerradvocate.com/pdf/Labaton-2015-Survey-report__12.pdf.*

Definition of Financial Institution (31 U.S.C. §5312(a)(2))

(2) "financial institution" means—

(A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813(h)));
(B) a commercial bank or trust company;
(C) a private banker;
(D) an agency or branch of a foreign bank in the United States;
(E) any credit union;
(F) a thrift institution;
(G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.);
(H) a broker or dealer in securities or commodities;
(I) an investment banker or investment company;
(J) a currency exchange;
(K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments;
(L) an operator of a credit card system;
(M) an insurance company;
(N) a dealer in precious metals, stones, or jewels;
(O) a pawnbroker;
(P) a loan or finance company;
(Q) a travel agency;
(R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;
(S) a telegraph company;
(T) a business engaged in vehicle sales, including automobile, airplane, and boat sales;
(U) persons involved in real estate closings and settlements;
(V) the United States Postal Service;
(W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph;
(X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which—
(i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or
(ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act);
(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or

(Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

Exempted anti-money laundering programs for certain financial institutions. 31 C.F.R 1010.205(b)(1)

(b)Temporary exemption for certain financial institutions. [no sunset clause]

(1) Subject to the provisions of paragraphs (c) and (d) of this section, the following financial institutions (as defined in 31 U.S.C. 5312(a)(2) or (c)(1)) are exempt from the requirement in 31 U.S.C. 5318(h)(1) concerning the establishment of anti-money laundering programs:
(i) Pawnbroker;
(ii) Travel agency;
(iii) Telegraph company;
(iv) Seller of vehicles, including automobiles, airplanes, and boats;
(v) Person involved in real estate closings and settlements;
(vi) Private banker;
(vii) Commodity pool operator;
(viii) Commodity trading advisor; or
(ix) Investment company.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM GREG BAER

Q.1. *Shifting BSA Oversight Back to FinCEN*—One Clearing House recommendation is to have FinCEN's BSA oversight authority over large banks—originally delegated to Federal banking agencies over 20 years ago—returned to FinCEN. But it seems clear FinCEN does not have the bandwidth to make such a radical change.

Can you describe your organization's effort to assess what this change would require, in terms of additional Federal funding and personnel, or new assessments on big banks? Why should we redo wholesale a system that has been working reasonably well, and put in place the kind of centralized examination teams you suggest, when examiners have expertise and experience with these large entities, and have been doing this job successfully for many years?

A.1. While it would be a significant undertaking for FinCEN to examine all financial institutions subject to the BSA, we instead recommend that FinCEN retake exam authority for large international financial institutions that present complex cross-border issues and file a majority of SARs. We estimate that an examination team of only 25–30 people at FinCEN could replicate the existing work of the Federal banking agencies and the IRS (for the largest MSBs) at these institutions. More importantly, a dedicated FinCEN exam team for this small subset of large institutions could receive appropriate security clearances, meet regularly with law enforcement and other end users, receive training in big data analytics and work with other experts in Government. They, in turn, would be supervised by Treasury officials with law enforcement, national security, and diplomatic perspectives on what is needed from an AML/CFT program—not bank examiners who frequently bring no experience in any of those disciplines. Furthermore, when FinCEN turned to writing rules in this area, it would do so informed by its experience in the field. It would see the whole field, and promote innovative and imaginative conduct that advanced law enforcement and national security interests, rather than auditable processes and box checking. Funding such an exam team could be accomplished many ways, including: (i) assessing financial institutions for examinations costs;[1] or (ii) establishing a centralized team funded pro rata by each of the affected agencies but reporting directly and solely to the FinCEN Director.

This recommendation aims to address one of the fundamental drivers of the inefficiency in the U.S. AML/CFT regime—the fact that the end users of the information generated by banks (e.g., law enforcement and national security officials) have no say in how banks allocate their resources and provide financial intelligence to them. Therefore, examiners do not have insight into the utility of the material provided by banks, law enforcement AML/CFT priorities, or the degree to which banks can innovate their compliance

[1] Existing statutory authority appears to allow for such an assessment and affected institutions should see a corresponding reduction in the assessment they currently pay to prudential regulators for supervision of this function. The Independent Offices Appropriation Act provides general authority for a Government agency to assess user fees or charges by administrative regulation, based on the value of the service to the recipient. See 31 U.S.C. §9701. OMB Circular No A-25 provides further guidance regarding "user fees" ("A user charge . . . will be assessed against each identifiable recipient for special benefits derived from Federal activities beyond those received by the general public."). See OMB Circular No. A-25 Revised.

programs in order to provide better leads to law enforcement. Instead they focus on auditable policies, procedures, and metrics.

From a political and personal risk perspective, examiners are in a no-win situation. On the one hand, they are excluded when the bank they examine is pursuing real cases with law enforcement, national security or intelligence community officials, and therefore receive no credit when those cases are successful. But if something goes wrong—if a corrupt official or organization turns out to be a client of the bank they examine—the examiner faces blame. Thus, from an examiner and banking agency perspective, the only possible safe harbor is to demand more policies and procedures, ensure that a lot of alerts are generated and SARs filed, and encourage the bank to investigate exhaustively any client deemed high risk. Given that banks have been complying with AML/CFT requirements for decades, examiners are also fairly comfortable with the current technological and programmatic aspects of the regime, so rather than encourage institutions to make innovative programmatic changes to detect high-risk financial crimes, the examiner focuses on auditing processes like the number of computer alerts generated, SARs filed and compliance employees hired. As a result, banks of all sizes generate a lot of SARs that are of little to no use to law enforcement.

Importantly, the benefits of a FinCEN examination function would extend well beyond the handful of banks it examined. Priorities set and knowledge learned could be transferred to regulators for the remaining financial institutions. And innovation started at the largest firms, with encouragement from FinCEN, would inevitably benefit smaller firms. The result of FinCEN assuming some supervisory authority would be a massive cultural change, as the focus of exams shifted to the real-world effectiveness of each institution's AML/CFT program, rather than the number of SARs filed or number of policies written. That change would start with those banks under sole FinCEN supervision, but would eventually spread to all institutions.

Q.2. *Protecting Information Shared Among Banks*—With any increase in information sharing between financial institutions beyond that allowed under current law would come an increased responsibility for those institutions to protect consumer and commercial data.

What additional steps are needed to ensure that expanding information sharing among banks doesn't put customers at greater risk of data theft, or of unjustified exclusion from the financial system because of inaccurate information being shared? Should we consider a more formal redress mechanism for persons debanked as a result of increased information sharing? Has the Clearing House surveyed its members to assess, over the last 5 years or so, how many 314b inquiries were made, and how many responded to, by member banks? If not, could you do such an informal survey and provide to the Committee that data?

A.2. Financial institutions work very hard to ensure that their customers can conduct their financial transactions in a safe and secure manner, while protecting their privacy. U.S. banks are subject to a host of regulatory and other requirements and devote substantial

time and investment to safeguarding customer data—and have every incentive to do so. We believe that greater information sharing is fully consistent with the important privacy risks of bank customers. If a customer has an account at multiple banks, each of those banks is already monitoring those accounts for suspicious activity. Allowing a bank that believes that it has detected suspicious activity to consult the other relevant banks would allow it to develop a more complete picture of the customer's financial activity, and in many cases would result in a SAR not being filed. (For example, one bank might see suspicious wire transfers to another country, while a second bank might explain that it banks a company owned by that customer in that country, so the transfers are entirely appropriate.) Of course, in some cases, a more complete picture might confirm initial suspicions, and lead to a higher quality SAR filing.

We do not believe there should be concerns about information sharing on SARs leading to customers becoming unbanked. Sharing would only occur if there was already cause for suspicion, and would occur only among those banks that currently share the customer. Even in the event that all those banks, as a result of the sharing, decide to close the customer's accounts, this fact will not be disclosed to other banks or to the public. Thus, this case is not akin to credit reporting, where a customer's experience with one bank affects his or her credit score, and thereby the ability to obtain credit from any bank.

In order to be covered by the 314(b) safe harbor, financial institutions or an association of financial institutions must comply with a number of requirements, including: (i) annually registering with FinCEN and providing a point of contact for requests; (ii) taking reasonable steps to verify that the recipient institution is also registered with FinCEN; and (iii) ensuring that the information shared is adequately protected, secure and confidential.[2] In particular, FinCEN's 314(b) regulation states that institutions who share under this program are to "maintain adequate procedures to protect the security and confidentiality of such information . . . [which] shall be deemed satisfied to the extent that a financial institution applies to such information procedures that the institution has established to satisfy the requirements of section 501 of the Gramm–Leach–Bliley Act (15 U.S.C. 6801), and applicable regulations issued thereunder, with regard to the protection of its customers' nonpublic personal information."[3] As a general matter, FinCEN notes that sharing under 314(b) must only be done to "[i]dentify[] and, where appropriate, report[] on activities that may involve terrorist financing or money laundering; [d]etermine[] whether to establish or maintain an account, or to engage in a transaction; or [a]ssist[] in compliance with anti–money laundering requirements."[4]

While it would be difficult to provide you with data on the frequency of requests and responses as requests carry varying degrees of urgency and significance—some are critical and merit an institu-

[2] See FinCEN "Section 314(b) Fact Sheet", (314(b) Fact Sheet) November 2016, available at *www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.*

[3] See 31 CFR 1010.540(b)(4)(ii).

[4] See 314(b) Fact Sheet, supra n. 2.

tion's immediate attention while others are more routine and can function as alerts—we note that FinCEN guidance suggests that financial institutions reference 314(b) in SAR narratives when it has assisted institutions in determining whether information is suspicious, so the agency may be able to provide you with a comprehensive assessment of the relative effectiveness of the program. Relatedly, our members have been told anecdotally by law enforcement that their investigative work, using 314(b) and other tools, has resulted in the production of highly useful information.[5]

Finally, when dealing with financial inclusion concerns, we note that the present regulatory framework lends itself to overly conservative evaluations of risk. This is why TCH recommends that Treasury lead the regime as it is uniquely positioned to balance the sometimes conflicting interests relating to national security, the transparency and efficacy of the global financial system, the provision of highly valuable information to regulatory, tax and law enforcement authorities, financial privacy, financial inclusion, and international development.

Q.3. *SAR Filings*—You noted in your testimony that currently the largest number of SARs being filed against banks are for insider threats and abuses such as deceptive and fraudulent sales practices, and seemed to suggest that was inappropriately high. But I note that in cases like Wells Fargo, which has recently been forced to pay out hundreds of millions in fines, penalties, and a class action settlement, the filing of SARs is often a useful tool to identify such patterns of misconduct among employees, and throughout a bank and its branches.

Are there specific types of insider threats, deceptive or fraudulent practices, or other types of illicit conduct that you think should NOT be subject to SAR filings?

A.3. We are aware of no case, including Wells Fargo, where SAR filings served as a "useful tool to identify . . . patterns of misconduct among employees, and throughout a bank and its branches." Rather, our strong presumption is that SAR filings with respect to minor offenses in small dollar amounts are rarely if ever investigated by law enforcement. We do not know but strongly suspect that any post hoc SAR filings made by Wells Fargo have not resulted in any prosecution of employees subject to those filings, and that law enforcement, if it were interested in prosecuting or interviewing those employees, did not require a SAR filing to identify them. Again, this is only speculation, so we would strongly urge the Committee to ask FinCEN for data on the yield on SARs filed on insider abuse, and for examples of where such filings initiated or advanced a prosecution.

None of this is to minimize the importance of enforcing the law against banks and their employees. We do question strongly whether resources deployed to filing SARs on insider abuse could be better deployed to innovative approaches to detecting more serious crimes. As a general matter, the current BSA/AML reporting re-

[5] See Testimony of William J. Fox before the U.S. House Financial Services Subcommittees on Financial Institutions and Consumer Credit and Terrorism and Illicit Finance, November 29, 2017, available at *financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-wfox-20171129.pdf.*

gime should be reviewed and the investigation and reporting of activity of limited law enforcement or national security consequence should be deprioritized, while increasing law enforcement feedback, to allow financial institutions to re-allocate resources to higher value AML/CFT efforts. This effort corresponds with the statutory purpose of the BSA, which is to provide the Government with AML/CFT information that is of a "high degree of usefulness."[6]

TCH believes that the SAR regime should be modernized through the tailoring of various requirements and facilitation of the submission of raw data from financial institutions to law enforcement. This could be done in part by (i) providing guidance further clarifying that a SAR is not required simply because a transaction appears to have no economic, business, or lawful purpose; (ii) eliminating requirements to file SARs when there are single instances of structuring activity and under the 90-day continuing activity review requirements; (iii) reducing the number of fields deemed "critical" and "optional" to SAR and CTR filings, as each one imposes associated regulatory expectations and burdens with varying benefits; and (iv) reviewing, revising or retracting as necessary all existing SAR guidance to ensure it aligns with the priorities of law enforcement and the regime more broadly and clearly communicates expectations to institutions. CTR expectations should also be streamlined as, when coupled with the SAR regime, many may be of low law enforcement or national security value.[7]

To get a sense of the potential for improvement, note that one bank has publicly reported that it receives follow-up requests from law enforcement on approximately 7 percent of the SARs it files, which is consistent with other reports we have received. More importantly, for some categories of SARs—structuring, insider abuse—that number is far lower, approaching 0 percent. However, no one can afford to stop filing SARs in any category because examiners focus on the SAR that was not filed, not the quality or importance of the SAR that was filed. A core problem with the current regime is that there is an absence of leadership making choices like these—therefore we also recommend that Treasury set priorities for the AML/CFT regime and allow financial institutions to deploy their resources in support of those priorities.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR SASSE FROM GREG BAER

Q.1. Our current money laundering regulatory regime evaluates financial institutions based on how they meet process-based metrics such as the filing of suspicious activity reports. As this hearing discussed, the drawback to this is that financial institutions end up focusing on meeting these metrics instead of developing innovations that will better catch the bad guys. One proposed way to en-

[6] See 31 U.S.C. §5311, which states that "[i]t is the purpose of this subchapter [the BSA] to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism." Note that the last clause was added by the USA PATRIOT Act in 2001.

[7] See *The Clearing House*, "Re: Request for Comments Regarding Suspicious Activity Report and Currency Transaction Report Requirements", (April 10, 2018), available at *www.theclearinghouse.org/-/media/tch/documents/tch-weekly/2018/20180410_tch_comment_letter_to_fincen_on_sar_and_ctr_requirements.pdf.*

courage innovation that focuses on results is to find ways to allow financial institutions to experiment with new anti–money laundering technologies without facing regulatory liability. For example, some have proposed a no-action letter system which would allow financial institutions to gain guidance from FinCEN and other regulators about the legality of proposed actions. How would such a system function and how could it encourage innovation? Would FinCEN need legislative authorization to implement a no-action letter process, either to issue no-action letters themselves or to have the authority to exempt financial institutions from any particular reporting requirements?

A.1. TCH supports efforts to institute a no-action letter like process that resembles the Securities and Exchange Commission's.[1] While rulemaking and the issuance of guidance are cumbersome processes that do not always promote innovation or dialogue with the industry, a no-action letter system could be more effective. It would allow individual financial institutions to ask particular questions about actions they plan to take, thereby spurring innovation; provide quick answers, thereby nurturing innovation; and increase the flow of information from industry to FinCEN. As with other areas of reform, Congressional efforts to encourage the establishment of a no-action letter process for Bank Secrecy Act-related issues would be helpful.[2] We note that the Bank Secrecy Act grants Treasury broad interpretive authority including to "prescribe an appropriate exemption from a requirement under this subchapter and regulations prescribed under this subchapter."[3]

More broadly, a cultural change is necessary in how banks are examined for compliance, and assessed for potential enforcement action. The current focus of examination is reviewing a sample of alerts and attempting to demonstrate that a SAR should have been filed in some of those cases. There is little to no focus on the value of the SARs the bank filed. There is little to no contact between examiners and the law enforcement and national security officials who use those SARs. We believe that any assessment of a firm's AML/CFT program should include all that information, and that any examination criticisms (in the form of Matters Requiring Attention) or formal enforcement action should come only after a holistic review of the program, and not perceived compliance lapses in a particular area, particularly where there was no attempt to actually assist (as opposed to failure to detect) money laundering. We have proposed achieving that result for the largest, internationally active banks—which file the majority of SARs and present global derisking issues—by having FinCEN reclaim the examination au-

---

[1] See *The Clearing House*, "A New Paradigm: Redesigning the U.S. AML/CFT Framework To Protect National Security and Aid Law Enforcement", (TCH AML/CFT Report), February 2017, available at *www.theclearinghouse.org//media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.*

[2] While legislative authorization would be helpful, we note that the Securities and Exchange Commission's no-action letter regime appears to be established under broad authorities. See Nagy, Donna M., "Judicial Reliance on Regulatory Interpretations in SEC No-Action Letters: Current Problems and a Proposed Framework", *Cornell Law Review*, Vol. 83: 921, p. 931 which says "[i]n addition to rulemaking and adjudicatory powers of statutory origin, the SEC possesses inherent power to issue interpretations of the Federal securities laws and the SEC rules it has promulgated thereunder. This authority to make interpretive statements derives from Congress's charge to the SEC to administer and enforce the Federal securities laws." Available at *www.lawschool.cornell.edu/research/cornell-law-review/upload/Nagy.pdf.*

[3] See 31 U.S.C. §5318(a)(7).

thority that Congress assigned it, rather than continuing to delegate it. For other banks, we believe FinCEN needs to set priorities and assist in reviewing the value of a firm's program.

Q.2. What should our risk tolerance be for the fact that the U.S. financial system facilitates crimes like human trafficking? Should we strive to have zero incidence of money laundering in our financial system?

A.2. Financial institutions around the globe are proactively working among themselves and with the public sector to disrupt human trafficking networks. In a 2016 *Financial Times* op-ed, Standard Chartered's Group General Counsel discussed the need for enhanced public–private sector sharing, noting that presentations from NGOs and Government agencies "have improved banks' ability to detect potentially [human trafficking] related financial transactions. In turn, they have helped law enforcement disrupt trafficking networks."[4] Such movements are also underway in the United States.[5]

However, a core problem with the current regime is that it does not prioritize the allocation of financial institution resources to generate leads that are of a "high degree of usefulness" as required by the BSA.[6] Therefore, TCH recommends that Treasury set AML/CFT priorities for the regime to assist financial institutions as they work to fulfill their statutorily mandated reporting obligations—including for potential human trafficking.[7] Furthermore, we encourage the development and improvement of public–private sector AML/CFT information sharing partnerships. The authorized and appropriate sharing of information between the Government and the private sector as well as the sharing of information between and among financial institutions is critical to efforts to address illicit finance. We note that the USA Patriot Act's Section 314(b) private sector information sharing provisions have reportedly been useful in addressing human trafficking and other crimes.[8]

Q.3. I'd like to understand better how technological innovation is transforming the fight against money laundering and how Government policy can help or hurt these efforts.

---

[4] See *Financial Times* op-ed by David Fein, "How To Beat the Money Launderers: Banks Must Work With Governments To Combat This Scourge", November 22, 2016, available at *www.ft.com/content/569c2e26-adb9-11e6-ba7d-76378e4fef24.*

[5] See *TCH Banking Perspectives* article by Juan C. Zarate and Chip Poncy, "Designing a New AML System", Q3 2016, available at *www.theclearinghouse.org/research/banking-perspectives/2016/2016-q3-banking-perspectives/a-new-aml-system.*

[6] See 31 U.S.C. §5311, which states that "[i]t is the purpose of this subchapter [the BSA] to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism." Note that the last clause was added by the USA PATRIOT Act in 2001.

[7] We note that the U.K.'s Joint Money Laundering Intelligence Taskforce (JMLIT) has established the following operational priorities for its public–private sector information sharing partnership: (i) understanding and disrupting the funding flows linked to bribery and corruption; (ii) understanding and disrupting trade based money laundering; (iii) understanding and disrupting the funding flows linked to organized immigration crime, human trafficking and modern slavery; (iv) understanding and disrupting money laundering through capital markets; and (v) understanding key terrorist financing methodologies. See JMLIT website at *www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit.*

[8] See Testimony of William J. Fox before the U.S. House Financial Services Subcommittees on Financial Institutions and Consumer Credit and Terrorism and Illicit Finance, November 29, 2017, available at *financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-wfox-20171129.pdf.*

In the health care context, I hear about how researchers have used machine learning and artificial intelligence to identify diseases and predict when they will occur, using data points that humans would have never put together. How have financial institutions or law enforcement officials been able to use of similar techniques to identify money laundering and how much more progress can be made in this front?

Outside of AI and machine learning, how can recent FinTech innovations such as blockchain fight money laundering?

What regulatory requirement or requirements—if any—most hinders the adoption of technological innovations?

A.3. Financial institutions are in the early stages of exploring various ways to apply technological innovations to AML/CFT efforts. In particular, artificial intelligence has the potential to improve the way that banks identify suspicious activity. AI does not search for typologies but rather mines data to detect anomalies. It gets progressively smarter; it won't be easily evaded; and different banks with different profiles would end up producing different outcomes.

Our banks report that they are working to pilot AI solutions in this area, yet the experts that they need to work on these initiatives are instead required to validate their current programmatic processes to examiners.[9] Financial institutions need to be able to innovate their AML programs and coordinate that innovation with their peers. Yet, the most consequential impediment to innovation is the current regulatory structure as examiners focus on auditing banks' policies, processes, and metrics versus encouraging financial institutions to shift their resources to developing innovative methods of detecting financial crime.

Furthermore, some firms have expressed concerns that if they adopt new and more effective methods, and actually identify more illicit activity, they will be sanctioned by the banking agencies for failing to detect that conduct earlier. It is a reflection of the current dysfunction that this is an actual concern.

This is why TCH believes that Treasury should take a more prominent role in coordinating AML/CFT policy and examinations across the Government and conduct a robust and inclusive annual or biennial process to establish AML/CFT priorities and provide an overarching purpose for the regime. Furthermore, we believe that FinCEN should retake exam authority for multinational, complex financial institutions. A dedicated FinCEN exam team for this small subset of large institutions could receive appropriate security clearances, meet regularly with law enforcement and other end users, receive training in big data analytics and work with other experts in Government. They, in turn, would be supervised by Treasury officials with law enforcement, national security, and diplomatic perspectives on what is needed from an AML/CFT program. This change would promote innovative and imaginative conduct that advanced law enforcement and national security interests, rather than auditable processes and box checking. Importantly, the benefits of a FinCEN examination function would extend well beyond the handful of banks it examined. Priorities set and knowledge learned could be transferred to regulators for the remaining

[9] Id.

financial institutions. And innovation started at the largest firms, with encouragement from FinCEN, would inevitably benefit smaller firms. The result of FinCEN assuming some supervisory authority would be a massive cultural change, as the focus of exams shifted to the real-world effectiveness of each institution's AML/CFT program, rather than the number of SARs filed or number of policies written. That change would start with those banks under sole FinCEN supervision, but would eventually spread to all institutions.

Q.4. How much does bitcoin, blockchain, and other cryptocurrencies facilitate money laundering? How—if at all—should this impact our approach to combating money laundering in traditional banks? How can law enforcement officials best stop this newer form of money laundering?

A.4. As a general matter, customers are using various tools to conduct transactions around the globe with bank and nonbank financial institutions. In 2013, FinCEN issued guidance indicating that a cryptocurrency "administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person." [10] We also note that in the past few years, FinCEN has levied enforcement actions against cryptocurrency exchangers. While TCH is not privy to data on the extent of money laundering within virtual currencies, we note that others are beginning to look into this issue. [11]

Any review of the BSA/AML regime and its effectiveness should investigate the changing ways in which customers interact with financial institutions and ensure that statutory authorities are adequately tailored to address the evolving nature of illicit finance threats.

Q.5. I'd like to discuss Suspicious Activity Reports (SARs). Today, around 2 million SARs are filed each year. While every SAR used to be read by law enforcement officials, that is no longer the case today. Financial institutions often complain that they rarely, if ever, receive feedback from law enforcement officials on the utility of any particular suspicious activity report that they file. This lack of feedback loops increases the burdens on financial institutions, who continue to file SARs that are of little utility to law enforcement officials. It also prevents financial institutions from developing better analytical tools to more precisely discern between the signal and the noise.

What percentage of SARs are actually read by someone in law enforcement?

How often do financial institutions receive feedback from law enforcement officials as to the utility of their SAR filing?

While some have proposed reducing the number of SARs and CRT filings because they are often superfluous and are never read,

---

[10] See FIN-2013-G001 "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", March 18, 2013, available at *www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.*

[11] For example, in January 2018, Yaya J. Fanusie and Tom Robinson published a memorandum on "Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services". Available at: *www.defend democracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.*

others argue that this poses risks, because investigating minor infractions may still lead to significant law enforcement successes. How should policymakers resolve this conflict?

A.5. TCH members report that they receive follow-up requests for additional information from law enforcement on their SAR filings in less than 10 percent of cases. For certain categories of SARs, the number of requests is close to 0 percent. It should be noted that a follow-up request does not mean that the SAR led to an arrest or conviction; it means only that someone in law enforcement wanted to learn more about the case. Our understanding is that FinCEN does not routinely research how SARs are used and what their yield is. Obviously, a more modern system would be more data-driven.

While law enforcement is best placed to provide data on how many reports are read, we note that they are generally used by FinCEN and law enforcement for data searches and mining. While one BSA report may be the "last piece of the puzzle," it's important to consider the resources deployed for the production of that report and whether they would be better spent if redirected to produce the first piece in a more important puzzle. As an analogy, if law enforcement rigorously enforced jaywalking rules, it would occasionally capture a wanted fugitive, but no one would consider that a good use of finite law enforcement resources. Again, a core problem with the current regime is that there is an absence of leadership making choices like these.

This is why TCH recommends that Treasury lead the regime by coordinating AML/CFT policy and examinations across the Government and conduct a robust and inclusive annual or biennial process to establish AML/CFT priorities that would form the basis for the deployment of financial institution resources. Relatedly, Treasury should undertake a review of BSA/AML reporting requirements to ensure information of a high degree of utility is reported to law enforcement, which conforms with financial institutions' obligations under the BSA. [12]

Q.6. How could regulators (1) set up better feedback loops between financial institutions and law enforcement officials that could help financial institutions better identify money laundering; and (2) empower financial institutions to act upon their improved ability to distinguish between useful and superfluous reports, including by filing fewer unnecessary SARs, without fearing regulatory consequences for doing so?

Would a better feedback loop system exist if financial institutions employed more people with security clearances? If so, what, if anything, can the Federal Government do to facilitate this?

A.6. There are substantial benefits to developing additional pathways, both formally and informally, for AML/CFT information sharing between various stakeholders in the public and private sector. Granting law enforcement and national security authorities opportunities to provide general feedback on the reports filed, and in-

[12] See 31 U.S.C. §5311, which states that "[i]t is the purpose of this subchapter [the BSA] to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism." Note that the last clause was added by the USA PATRIOT Act in 2001.

corporating this feedback into supervisory evaluations of firms' compliance, could assist financial institutions in targeting their resources to efforts that provide information that is of the greatest use in preventing illicit financing. We note that under the current regime, many large financial institutions operate financial intelligence units (FIUs) that employ former law enforcement or national security officials, yet still receive little to no useful feedback.

It would also be helpful if a pathway for sharing information was established to allow financial institutions to efficiently share raw data with law enforcement, under a safe harbor, and with reforms made to current reporting requirements. The current regime is built on individual, bilateral reporting mechanisms grounded in the analog technology of the 1980s, rather than the more interconnected and technologically advanced world of the 21st century.[13] Therefore, providing such data in bulk would modernize the current regime and allow institutions to provide law enforcement with information in a timelier manner. Furthermore, it would allow law enforcement, using big data analytics, to effectively have access to and sift through large quantities of data more efficiently.

Further coordination and information sharing between and among public sector authorities is critical to establishing AML/CFT priorities and providing an overarching purpose for the regime. In order to empower institutions to deploy resources to high-value activities, TCH recommends that Treasury take a more prominent role in coordinating AML/CFT policy and examinations across the Government and conduct a robust and inclusive annual or biennial process to establish AML/CFT priorities, which could form the basis of financial institution examinations. This is particularly important in the U.S. where law enforcement, national security, and financial institution oversight responsibilities are dispersed among multiple agencies. This stands in contrast to other approaches (e.g., the U.K.'s Joint Money Laundering and Intelligence Task Force (JMLIT)) that better address barriers to information sharing by bringing together relevant actors to share information as well as allowing financial institutions to follow-up on SAR activity, thereby potentially improving the effectiveness of financial institution reporting mechanisms. However, as alluded to above, with any public–private sector dialogue, and more generally, we believe that national authorities should speak with one voice when providing feedback as well as disseminating red flags, threats, and typologies to the private sector as disparate voices create confusion.

Q.7. Often, financial institutions will derisk by refusing to serve customers that could be involved in illegal activity. As financial institutions start to share more information with each other, this practice could become more prominent and potential criminals could more frequently lose access to the United States' financial system altogether.

Are there instances in which derisking is actually unhelpful for law enforcement purposes, because it drives these criminals underground and makes it more difficult to track them?

---

[13] See *The Clearing House*, "A New Paradigm: Redesigning the U.S. AML/CFT Framework To Protect National Security and Aid Law Enforcement", (TCH AML/CFT Report), February 2017, available at *www.theclearinghouse.org//media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.*

At the moment, do the regulators that evaluate and enforce financial institutions compliance with our Federal money laundering take this into account?

Are there promising ways to increase cooperation between financial institutions, regulators, and law enforcement officials, so that financial institutions can make a more informed decision about when and how to derisk?

Would financial institutions need to hire more employees with a top security clearance and/or a law enforcement background for this coordination to be effective?

A.7. The current derisking trend is in part a reaction to Government and supervisory characterizations of correspondent banking as a high risk business and the evolving standards within the domestic and international community.[14] The causes are clear—the systems, processes, and people required to manage examiner expectations for clients deemed to be of "higher risk", are extremely costly. For example, a bank may prepare a lengthy report on a customer only to be criticized for not further documenting the grounds on which it decided to retain the customer. For certain regions or businesses it is often times too expensive to build out this infrastructure to support higher risk accounts. And this does not even include the risk of massive fines and reputational damage in the event a customer designated high-risk actually commits a criminal act.

As discussed previously, TCH believes that Treasury should take a more prominent role in coordinating AML/CFT policy and examinations for the regime. That includes convening on a regular basis the end users of BSA data—law enforcement, national security, and others affected by the AML/CFT regime including the State Department—and setting goals and priorities for the system. Treasury is uniquely positioned to balance the sometimes conflicting interests relating to national security, the transparency and efficacy of the global financial system, the provision of highly valuable information to regulatory, tax and law enforcement authorities, financial privacy, financial inclusion, and international development.

In addition, and as discussed above, TCH believes that greater information sharing will assist in further clarifying whether a customers' activity is, in fact, suspicious. Presently the USA PATRIOT Act grants various statutory authorities, under Sections 314(a) and 314(b) to allow for public–private and private–private sector sharing. While security clearances and additional staff may be helpful, we note that large financial institutions employ hundreds of staff members, some of whom are former law enforcement officials, to assist with compliance efforts yet it's the "check-the-box" nature of

[14] See "The Great Unbanking: Swingeing Fines Have Made Banks Too Risk-Averse", *The Economist*, July 6, 2017, available at *www.economist.com/news/leaders/21724813-it-time-rethink-anti-money-laundering-rules-swingeing-fines-have-made-banks-too-risk-averse*. See also "A Crackdown on Financial Crime Means Global Banks Are Derisking", *The Economist*, July 8, 2017, available at *www.economist.com/news/international/21724803-charities-and-poor-migrants-are-among-hardest-hit-crackdown-financial-crime-means.*

the compliance regime that prevents them from utilizing these resources for more proactive AML/CFT efforts.[15]

RESPONSES TO WRITTEN QUESTIONS OF SENATOR TILLIS FROM GREG BAER

Q.1. How can we leverage technology to make the process simultaneously less onerous on banks while enhancing the outcomes of catching illegal behavior? Are there regulatory and legislative barriers to getting that down?

A.1. Allowing financial institutions to innovate their AML programs is key to enhancing their ability to identify suspicious activity. The biggest barrier to innovation is the current exam paradigm. As one bank recently testified, from 2010–11 they were able to innovate the way in which they used technology to identify potentially suspicious activity. However, since then, they have found innovation difficult as regulatory guidance has been inappropriately applied to their programs and examiners have in turn rigorously enforced this guidance, thereby delaying the implementation of programmatic changes that used to take weeks to 9 months or a year.[1] Under the current AML/CFT regime, examiners focus on auditing banks' policies, processes, and metrics versus encouraging financial institutions to shift their resources to developing innovative and effective methods of detecting financial crime.

This is why TCH believes that Treasury should take a more prominent role in coordinating AML/CFT policy and examinations across the Government and conduct a robust and inclusive annual or biennial process to establish AML/CFT priorities and provide an overarching purpose for the regime. Furthermore, we believe that FinCEN should retake exam authority for multinational, complex financial institutions. A dedicated FinCEN exam team for this small subset of large institutions could receive appropriate security clearances, meet regularly with law enforcement and other end users, receive training in big data analytics and work with other experts in Government. They, in turn, would be supervised by Treasury officials with law enforcement, national security, and diplomatic perspectives on what is needed from an AML/CFT program. This change would promote innovative and imaginative conduct that advanced law enforcement and national security interests, rather than auditable processes and box checking. Importantly, the benefits of a FinCEN examination function would extend well beyond the handful of banks it examined. Priorities set and knowledge learned could be transferred to regulators for the remaining financial institutions. And innovation started at the largest firms, with encouragement from FinCEN, would inevitably benefit smaller firms. The result of FinCEN assuming some supervisory authority would be a massive cultural change, as the focus of exams shift-

---

[15] See Testimony of William J. Fox before the U.S. House Financial Services Subcommittees on Financial Institutions and Consumer Credit and Terrorism and Illicit Finance, November 29, 2017, available at *financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-wfox-20171129.pdf.*

[1] See Testimony of William J. Fox before the U.S. House Financial Services Subcommittees on Financial Institutions and Consumer Credit and Terrorism and Illicit Finance, November 29, 2017, available at *financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-wfox-20171129.pdf.*

ed to the real-world effectiveness of each institution's AML/CFT program, rather than the number of SARs filed or number of policies written. That change would start with those banks under sole FinCEN supervision, but would eventually spread to all institutions.

Q.2. Financial institutions often complain that FinCEN, law enforcement officials, and prudential regulators do not tell them whether their BSA filings serve a useful purpose, or how the reports they submit are being used—and that the filings go into a black hole. Can you shed some light on the filings that you make or have used and what could be done to improve this process?

A.2. TCH members report that they receive follow-up requests for additional information from law enforcement on their SAR filings in less than 10 percent of cases. For certain categories of SARs, the number of requests is close to 0 percent. It should be noted that a follow-up request does not mean that the SAR led to an arrest or conviction; it means only that someone in law enforcement wanted to learn more about the case. Our understanding is that FinCEN does not routinely research how SARs are used and what their yield is. Obviously, a more modern system would be more data-driven.

TCH believes that the SAR regime and BSA filing requirements generally, should be modernized through the tailoring of various requirements and facilitation of the submission of raw data from financial institutions to law enforcement. The current regime is built on individual, bilateral reporting mechanisms grounded in the analog technology of the 1980s, rather than the more interconnected and technologically advanced world of the 21st century.[2] Therefore, providing such data in bulk would modernize the current regime and allow institutions to provide law enforcement with information in a timelier manner. Furthermore, it would allow law enforcement, using big data analytics, to effectively have access to and sift through large quantities of data more efficiently.

Furthermore, additional pathways for AML/CFT information sharing between various stakeholders in the public and private sector should be developed. Granting law enforcement and national security authorities opportunities to provide general feedback on the reports filed, and incorporating this feedback into supervisory evaluations of firms' compliance, could assist financial institutions in targeting their resources to efforts that provide information that is of the greatest use in preventing illicit financing.

Further coordination and information sharing between and among public sector authorities is critical to establishing AML/CFT priorities and providing an overarching purpose for the regime. In order to empower institutions to deploy resources to high-value activities, TCH recommends that Treasury take a more prominent role in coordinating AML/CFT policy and examinations across the Government and conduct a robust and inclusive annual or biennial process to establish AML/CFT priorities, which could form the

[2] See *The Clearing House*, "A New Paradigm: Redesigning the U.S. AML/CFT Framework To Protect National Security and Aid Law Enforcement", (TCH AML/CFT Report), February 2017, available at *www.theclearinghouse.org//media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.*

basis of financial institution examinations. This is particularly important in the U.S. where law enforcement, national security, and financial institution oversight responsibilities are dispersed among multiple agencies. This stands in contrast to other approaches (e.g., the U.K.'s Joint Money Laundering and Intelligence Task Force (JMLIT)) that better address barriers to information sharing by bringing together relevant actors to share information as well as allowing financial institutions to follow-up on SAR activity, thereby potentially improving the effectiveness of financial institution reporting mechanisms. However, with any public–private sector dialogue, and more generally, we believe that national authorities should speak with one voice when providing feedback as well as disseminating red flags, threats, and typologies to the private sector as disparate voices create confusion.

Q.3. Another compliance challenge often cited by banks is that they feel pressured by bank examiners and law enforcement authorities to exit certain business lines or cease offering certain services to customers viewed as presenting particular money-laundering vulnerabilities, i.e., severing corresponding banking relationships with foreign institutions in certain geographic areas, and also ending money services businesses (MSBs, i.e., check cashing, money transmitters, currency exchange outlets, etc.)

As banks reevaluate their business relationships with MSBs in light of what they may view as a hostile regulatory landscape, what can we do to change this type of behavior/is this a prevalent problem in the industry?

It is my understanding that there are times when law enforcement and the bank regulators work at cross purposes. That is, law enforcement might want a bank to continue banking an individual or company that they are following and building a case against but the bank regulators, whose incentives are to not be embarrassed by their regulated entities, force the banks to "derisk" or close those accounts. Is that actually the case?

A.3. We do not have hard data on this question. With respect to specific customers, we have heard of cases where law enforcement asked a bank to keep an account open, and the bank agreed; we have also heard of cases where banks felt that the regulatory risk was too high, and declined. At a broader level, with respect to certain lines of business or regions, we do not believe there are cases where banks have agreed to remain engaged at law enforcement or other governmental request. For example, it has been reported that the State Department expressed considerable concern at the decision by banks to derisk foreign embassies in the United States, but the banks involved could not get sufficient assurance that the banking agencies would not sanction them if something went wrong, so closed or refused to open those accounts.

Q.4. In terms of AML, we know that the success of AML is centric around whether or not the predicate crime of money laundering has been reduced, but we only really know how pervasive money laundering is on a reactive basis, i.e., when someone/some entity is caught. To that end, do you believe the advent/popularity of cryptocurrencies could affect the capture of money laundering/could

it affect AML? Do enforcement authorities have the technological capabilities to work with private industry to capture mal-actors?

A.4. As a general matter, customers are using various tools to conduct transactions around the globe with bank and nonbank financial institutions. In 2013, FinCEN issued guidance indicating that a cryptocurrency "administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person."[3] We also note that in the past few years, FinCEN has levied enforcement actions against cryptocurrency exchangers. While TCH is not privy to data on the extent of money laundering within virtual currencies, others are beginning to look into this issue.[4] In addition, in a recent speech, Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker provided an example of cryptocurrencies being used for money laundering and terrorist financing stating that "law enforcement authorities recently arrested a woman in New York who used Bitcoin to launder fraud proceeds before wiring the money to ISIS."[5]

Any review of the BSA/AML regime and its effectiveness should investigate the changing ways in which customers interact with financial institutions and ensure that statutory authorities are adequately tailored to address the evolving nature of illicit finance threats.

Q.5. In your opinion, do you think that the overall AML regime has been effective? Additionally, what do you see as the best way to ensure future effectiveness?

Is it to have Treasury be the lead to:

1. Define with other stakeholders specific and clear national priorities of the regime; and
2. Determine, working with other stakeholders, clear and measurable objectives of the regime in light of those priorities. Should Treasury or someone else have to report those measurements against the objectives back to Congress?

A.5. The U.S. AML/CFT regime is broken. It is extraordinarily inefficient, outdated, and driven by perverse incentives. A core problem is that 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. Fundamental change is required to make this system an effective law enforcement and national security tool, and reduce its collateral damage.

The Department of the Treasury should reclaim responsibility for the system. That includes convening on a regular basis the end

---

[3] See FIN-2013-G001 "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", March 18, 2013, available at *www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.*

[4] For example, in January 2018, Yaya J. Fanusie and Tom Robinson published a memorandum on "Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services". Available at: *www.defend democracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.*

[5] See U.S. Department of the Treasury Under Secretary Sigal Mandelker Speech before the Securities Industry and Financial Markets Association Anti–Money Laundering and Financial Crimes Conference, (Treasury Under Secretary Mandelker's 2018 SIFMA Speech), February 13, 2018, available at *home.treasury.gov/news/press-release/sm0286.*

users of SAR data—law enforcement, national security, and others affected by the AML/CFT regime including the State Department—and publicly setting goals and priorities for the system. Treasury is uniquely positioned to balance the sometimes conflicting interests relating to national security, the transparency and efficacy of the global financial system, the provision of highly valuable information to regulatory, tax, and law enforcement authorities, financial privacy, financial inclusion, and international development.

In addition, FinCEN should retake exam authority for multinational, complex financial institutions. Relatedly, Treasury should review the BSA/AML reporting regime to ensure information of a high degree of utility is reported to law enforcement as well as encourage the exchange of AML/CFT information between the Government and the private sector as well as between and among financial institutions. Finally, one important change to the current system is the passage of legislation ending the use of shell companies with anonymous ownership.

Q.6. Mr. Baer, does the current process of having FinCEN delegate authority to the bank regulators work? What are the challenges and deficiencies of the current system and how best do we improve outcomes?

Does the current system take full advantage of technological advancements?

How does BSA affect financial institutions of different size, with different staff and tech resources?

A.6. Congress in the Bank Secrecy Act explicitly vested sole regulatory, examination, and enforcement authority in the Treasury Department, an agency with considerable financial but also law enforcement and national security knowledge—not the banking agencies. Congress rightly saw that this was an altogether different mission, requiring different expertise. However, decades ago, an understaffed and underfunded FinCEN delegated all examination authority to the banking agencies, and then abdicated any oversight role in how they conducted it.

The result is a system where the end users of suspicious activity reports, or SARs—law enforcement and national security—have little or nothing to say when a bank's compliance is evaluated. Examiners are generally not permitted to know which SARs are valued by the end users, and so focus on what they do know: policies and procedures.

For example, banks know that examiners test compliance by reviewing alerts and trying to identify cases where a SAR was not filed but arguably should have been. Therefore, they reportedly spend more time documenting decisions not to file SARs than they do following up on SARs they do file. In other words, they focus on the noise, not the signal. And they continue to use antiquated, consultant-devised, rules-based systems—rules known to the bad guys, by the way—rather than innovative artificial intelligence approaches, largely because the former are conducted under policies and procedures that have passed muster with regulators.

Furthermore, under this regime no one sets priorities—unlike any law enforcement or national security agency in the world. According to bank analysis—there is little to no governmental anal-

ysis—the great majority of SAR filings receive no uptake from law enforcement. For certain categories of SARs—structuring, insider abuse—the yield is close to 0 percent. And those categories now represent a majority of the SARs filed.

BSA/AML reform would benefit institutions of all sizes. In 2017, TCH testified before the House with a community banker who reported that his three-branch bank has four lending officers and six AML compliance officers. While TCH represents 25 large commercial banks, the regime is no more rational for smaller banks.[6]

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM GREG BAER

Q.1. What are the costs and benefits of having bank examiners assess bank compliance with the Bank Secrecy Act's (BSA) requirements instead of having anti–money laundering (AML) and combating the financing of terrorism (CFT) experts at the Financial Crimes Enforcement Network (FinCEN) examine bank compliance programs?

A.1. As you know, Congress assigned examination authority to the Treasury Department given its considerable financial, law enforcement, and national security knowledge. The benefit of delegation is clear: there are thousands of banks in the country, and bank regulators already have examiners assigned to them. Thus, they can efficiently add AML/CFT compliance to the list of items for which they examine. It would be inefficient for FinCEN to examine the vast majority of these banks, who present few issues.

On the other hand, for the largest, multinational banks, we believe that the equation is quite different. We estimate that an examination team of only 25–30 people at FinCEN could replicate the existing work of the Federal banking agencies and the IRS (for the largest MSBs) at these institutions. More importantly, a dedicated FinCEN exam team for this small subset of large institutions could receive appropriate security clearances, meet regularly with law enforcement and other end users, receive training in big data analytics, and work with other experts in Government. They, in turn, would be supervised by Treasury officials with law enforcement, national security, and diplomatic perspectives on what is needed from an AML/CFT program—not bank examiners with no experience in any of those disciplines. And when FinCEN turned to writing rules in this area, it would do so informed by its experience in the field. It would see the whole battlefield, and promote innovative and imaginative conduct that advanced law enforcement and national security interests, rather than auditable processes and box checking.

Importantly, the benefits of a FinCEN examination function would extend well beyond the handful of institutions it examined. Priorities set and knowledge learned could be transferred to regulators for the remaining financial institutions. And innovation started at the largest firms, with encouragement from FinCEN, would inevitably benefit smaller firms. The result of FinCEN as-

---

[6] See Testimony of Lloyd DeVaux before the House Financial Services Committee Subcommittee on Financial Institutions and Consumer Credit, June 28, 2017, available at *financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-ldevaux-20170628.pdf.*

suming some supervisory authority would be a massive cultural change, as the focus of exams shifted to the real-world effectiveness of each institution's AML/CFT program, rather than the number of SARs filed or number of policies written. That change would start with those banks under sole FinCEN supervision, but would eventually spread to all institutions.

Funding such an exam team could be accomplished many ways, including (i) assessing financial institutions for examinations costs;[1] or (ii) establishing a centralized team funded pro rata by each of the affected agencies but reporting directly and solely to the FinCEN Director.

Q.2. Is there a way to maintain a top-shelf effective AML/CFT policy while maintaining a commitment to increase access to financial products for the underbanked and immigrants who rely on remittance services?

A.2. With respect to remittances, the current derisking trend is in part a reaction to Government and supervisory characterizations of correspondent banking as a high risk business and the evolving standards within the domestic and international community.[2] The causes are clear—the systems, processes, and people required to manage examiner expectations for clients deemed to be of "higher risk", are extremely costly. While those who care about poverty or international development might conclude that the benefits of allowing remittances exceed the costs, in the form of potential money laundering, banking agencies in our experience have not undertaken such a cost-benefit analysis. Thus, they impose documentation requirements and expectations that make certain lines of business uneconomical.

We believe more research is warranted on how AML/CFT requirements affect the unbanked. Our understanding is that AML customer due diligence requirements are a substantial, perhaps majority, cost of opening an account. For low-dollar deposit accounts for lower income people, that can make the account difficult to offer and price.

Q.3. I'm interested in the ways in which technology can aid AML compliance efforts. What are some of the innovative technologies that you've seen that hold some promise for either the Government or the private sector?

What are the barriers to either the Government or the private sector adopting these technologies?

What can we be doing as legislators to ensure that we promote technological innovation in this sector?

---

[1] Existing statutory authority appears to allow for such an assessment and affected institutions should see a corresponding reduction in the assessment they currently pay to prudential regulators for supervision of this function. The Independent Offices Appropriation Act provides general authority for a Government agency to assess user fees or charges by administrative regulation, based on the value of the service to the recipient. See 31 U.S.C. §9701. OMB Circular No. A-25 provides further guidance regarding "user fees" ("A user charge . . . will be assessed against each identifiable recipient for special benefits derived from Federal activities beyond those received by the general public."). See OMB Circular No. A-25 Revised.

[2] See "The Great Unbanking: Swingeing Fines Have Made Banks Too Risk-Averse", *The Economist*, July 6, 2017, available at *www.economist.com/news/leaders/21724813-it-time-rethink-anti-money-laundering-rules-swingeing-fines-have-made-banks-too-risk-averse*. See also "A Crackdown on Financial Crime Means Global Banks Are Derisking", *The Economist*, July 8, 2017, available at *www.economist.com/news/international/21724803-charities-and-poor-migrants-are-among-hardest-hit-crackdown-financial-crime-means.*

A.3. Financial institutions are in the early stages of exploring various ways to apply technological innovations to AML/CFT efforts. In particular, artificial intelligence has the potential to improve the way that banks identify suspicious activity. AI does not search for typologies but rather mines data to detect anomalies. It gets progressively smarter; it won't be easily evaded; and different banks with different profiles would end up producing different outcomes.

Our banks report that they are working to pilot AI solutions in this area, yet the experts that they need to work on these initiatives are instead required to validate their current programmatic processes to examiners.[3] Furthermore, they lack feedback from the public sector on the BSA reports that they file—such feedback would assist institutions in tuning their systems to provide more targeted leads to law enforcement. Financial institutions need to be able to innovate their AML programs and coordinate that innovation with their peers. Yet, the most consequential impediment to innovation is the current regulatory structure as examiners focus on auditing banks' policies, processes, and metrics versus encouraging financial institutions to shift their resources to developing innovative methods of detecting financial crime. Banks will be reluctant to invest in systems unless someone in the Government can tell them that such systems will meet the banking examiners' expectations, and can replace old, outdated methods—in other words, that they will be rewarded, not punished, for innovation.

While there are instances where legislation is needed, in many cases agencies already have existing authority to address some of the concerns outlined during the hearing. For example, TCH believes that Treasury should take a more prominent role in coordinating AML/CFT policy and examinations across the Government, a step currently within their existing authority, to conduct a robust and inclusive annual or biennial process to establish AML/CFT priorities, which would form the basis for financial institution exams. Furthermore, we believe that FinCEN should retake exam authority for multinational, complex financial institutions, which is also within their current authorities. A dedicated FinCEN exam team for this small subset of large institutions could receive appropriate security clearances, meet regularly with law enforcement and other end users, receive training in big data analytics and work with other experts in Government. They, in turn, would be supervised by Treasury officials with law enforcement, national security, and diplomatic perspectives on what is needed from an AML/CFT program. This change would promote innovative and imaginative conduct that advanced law enforcement and national security interests, rather than auditable processes and box checking. Importantly, the benefits of a FinCEN examination function would extend well beyond the handful of institutions it examined. Innovation started at the largest firms, with encouragement from FinCEN, would inevitably benefit smaller firms. The result of FinCEN assuming some supervisory authority would be a massive cultural change, as the focus of exams shifted to the real-world effectiveness of each institution's AML/CFT program, rather than the number of SARs filed or number of policies written. That change

[3] Id.

would start with those banks under sole FinCEN supervision, but would eventually spread to all institutions.

Q.4. The regulatory definition of "financial institution" has been expanded several times over the years, both by FinCEN rulemaking and by legislation by Congress.

Should the definition of financial institutions be expanded to include other sectors? If so, which sectors?

Could these changes be made via FinCEN rulemaking or should legislation be passed?

A.4. As a general matter, the BSA/AML regime should be reviewed and its effectiveness investigated to account for the changing ways in which customers interact with bank and nonbanks and ensure that statutory authorities are adequately tailored to address the evolving nature of illicit finance threats.

Such a review could be undertaken by Treasury without Congressional action, with recommendations on further administrative, legislative, or regulatory changes that need to be made to improve the efficiency and effectiveness of the AML/CFT regime.

Q.5. In August 2017, FinCEN issued an advisory encouraging real estate brokers to share information with them that could be helpful in AML efforts, while noting they are not required to do so under current law.

How do we increase information sharing between real estate brokers and FinCEN?

Geographic Targeting Orders (GTOs), which impose additional record keeping and reporting requirements on domestic financial institutions or nonfinancial trades or businesses in a specific geographic area for transactions involving certain amounts of United States currency or monetary instruments, have been deployed since 2016 to target high-end real estate sectors in major metropolitan areas by requiring U.S. title insurance companies to identify the natural persons behind shell companies used to pay "all cash" for high-end residential real estate.

Are GTOs an effective tool or would regulation be a preferable way to cover the real estate sector?

A.5. As previously mentioned the AML/CFT regime should be reviewed and adequately tailored to address the evolving nature of illicit finance threats, including those in the real estate sector. There are substantial benefits to developing additional pathways, both formally and informally, for AML/CFT information sharing between various stakeholders in the public and private sector.

While we are not privy to any data on the effectiveness of FinCEN's GTO program, when discussing money laundering in the real estate sector we would urge Congress to pass legislation that prohibits the forming of companies with anonymous ownership. Such companies can be used by criminals to "mask their identities, involvement in transactions, and origins of their wealth, hindering law enforcement efforts to identify individuals behind illicit activity."[4]

---

[4] See FIN-2017-A003, "Advisory to Financial Institutions and Real Estate Firms and Professionals", August 22, 2017, available at *www.fincen.gov/sites/default/files/advisory/2017-08-22/Risk%20in%20Real%20 Estate%20Advisory__FINAL%20508%20Tuesday%20%28002%29.pdf.*

Q.6. Cryptocurrency exchanges are money services businesses supervised by State regulators and subject to Federal AML and CFT laws.

Should FinCEN play an enhanced role in assessing the compliance of cryptocurrency exchanges, or are State regulators sufficiently equipped to handle compliance monitoring?

What additional tools could we give regulators and law enforcement?

How prevalent is money laundering in cryptocurrency markets?

A.6. As a general matter, we believe that Treasury should take the lead in coordinating AML/CFT priorities and exams for all financial institutions, including cryptocurrency exchanges. Customers are using various tools to conduct transactions around the globe with bank and nonbank financial institutions and having one agency leading the regime would help coordinate disparate regulatory and law enforcement perspectives.

In 2013, FinCEN issued guidance indicating that a cryptocurrency "administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person."[5] We also note that in the past few years, FinCEN has levied enforcement actions against cryptocurrency exchangers. While TCH is not privy to data on the extent of money laundering within virtual currencies, we note that others are beginning to look into this issue.[6] Finally, in a recent speech, Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker provided an example of cryptocurrencies being used for money laundering and terrorist financing stating that "law enforcement authorities recently arrested a woman in New York who used Bitcoin to launder fraud proceeds before wiring the money to ISIS."[7] As circumstances change AML/CFT authorities and requirements should be flexible and tailored enough to adapt to evolving threats.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM GREG BAER

Q.1. Gaming and tourism are some of Nevada's top industries. In the State of Nevada, our gaming operators employ thousands of hard working Nevadans, and the industry as a whole domestically supports 1.7 million jobs across 40 States. Qualified casinos, like financial institutions, are also subject to Banking Secrecy Act requirements. Organizations within Nevada have suggested that gaming operators would welcome a review of BSA requirements, which they find to be burdensome. They look forward to this Committee's thoughtful, bipartisan, review of BSA requirements that

---

[5] See FIN-2013-G001 "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", March 18, 2013, available at *www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.*

[6] For example, in January 2018, Yaya J. Fanusie and Tom Robinson published a memorandum on "Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services". Available at: *www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.*

[7] See U.S. Department of the Treasury Under Secretary Sigal Mandelker Speech before the Securities Industry and Financial Markets Association Anti–Money Laundering and Financial Crimes Conference, (Treasury Under Secretary Mandelker's 2018 SIFMA Speech), February 13, 2018, available at *home.treasury.gov/news/press-release/sm0286.*

takes into account the security imperative for robust anti–money laundering efforts, as well as the impact those requirements have on all industries. For example, the Suspicious Activity Report (SAR) ($5,000) and the Currency Transaction Report (CTR) ($10,000) levels were set years ago. Some have recommended increasing these to correspond with inflation. Others believe that would be too high but do support a higher amount than currently.

One of the top priorities of the gaming industry is to remove the requirement for a detailed factual narrative for structuring in the suspicious activity forms. What do you think of this recommendation?

A.1. We strongly support that recommendation. We note that when the SAR regime was implemented in the mid-1990s it was based on the concept of providing law enforcement a narrative analytical lead, but SARs are instead used today as a source for word searches and datamining by FinCEN and law enforcement. This is particularly true with respect to structuring. Our understanding is that the yield on structuring SARs is close to zero, as most cash transactions are entirely legitimate. Thus, resources invested in constructing a narrative is wasted. To the extent that datamining identifies a structuring transaction as truly suspicious, then law enforcement can contact the bank and obtain whatever detail is necessary.

Q.2. Do you have specific recommendations regarding how the gaming industry can benefit from greater communication with Government agencies and law enforcement? Is there something the Federal Government can do to share information with casinos and others filing SARs about broad benefits that may occur because of some of the 58,000 SAR forms filed by gaming firms.

Would the creation of a Qualitative Feedback Mechanism help reduce money laundering and terrorist financing? Should the Secretary of the Treasury establish a mechanism to communicate anti–money laundering (AML) and countering terrorism financing (CTF) priorities to financial institutions, gaming establishments and Federal financial regulators? Could such a mechanism provide qualitative feedback on information shared by financial institutions with the Department of Treasury, including CTRs and SARs? Please describe the pros and cons of such a system.

A.2. There are substantial benefits to developing additional pathways, whether through a qualitative feedback mechanism or some other structure, for improved AML/CFT information sharing between various stakeholders in the public and private sector. As the Financial Action Task Force recently noted "[l]ack of guidance and feedback by public sector authorities on information shared by the private sector may hinder private sector's ability to effectively monitor transactions and provide well-developed reports to FIUs . . . [and] may also impede or discourage information sharing between different private sector entities, or between private and public sectors, and vice versa, e.g., because regulatory expectations are un-

clear or because there is insufficient information available about risks."[1]

For example, the absence of public sector feedback on SARs in the current regime is hindering financial institutions' ability to tune their systems to provide more targeted leads to law enforcement. Granting law enforcement and national security authorities opportunities to provide general feedback on the reports filed, and incorporating this feedback into supervisory evaluations of firms' compliance, could assist financial institutions in targeting their resources to efforts that provide information that is of the greatest use in preventing illicit financing.

It would also be helpful if a pathway for sharing information were established to allow financial institutions to efficiently share raw data with law enforcement along with reforms to SAR and other BSA reporting requirements. As discussed in the TCH AML/CFT report, the current regime is built on individual, bilateral reporting mechanisms grounded in the analog technology of the 1980s, rather than the more interconnected and technologically advanced world of the 21st century.[2] Therefore, providing such data in bulk would modernize the current regime and allow institutions to provide law enforcement with information in a timelier manner. Furthermore, it would allow law enforcement, using big data analytics, to effectively have access to and sift through large quantities of data more efficiently.

Further coordination and information sharing between and among public sector authorities is also critical to establishing AML/CFT priorities and providing an overarching purpose for the regime. Therefore, TCH recommends that Treasury take a more prominent role in coordinating AML/CFT policy and examinations across the Government and conduct a robust and inclusive annual or biennial process to establish AML/CFT priorities and provide an overarching purpose for the regime. This is particularly important in the U.S. where law enforcement, national security, and financial institution oversight responsibilities are dispersed among multiple agencies. This stands in contrast to other approaches (e.g., the U.K.'s Joint Money Laundering and Intelligence Task Force (JMLIT)) that better address barriers to information sharing by bringing together relevant actors to share information as well as allowing financial institutions to follow-up on SAR activity, thereby potentially improving the effectiveness of financial institution reporting mechanisms.

Q.3. The Office of the Comptroller of the Currency mentioned in its 2018 Banking Operating Plan that financial institutions should not inadvertently impair financial inclusion. But, as of September 2017, the OCC has not identified any specific issues they plan to address. We know that derisking has become an epidemic across many communities and industries, such as communities along the Southwest border, humanitarian organizations aiding Nations

---

[1] See "FATF Guidance: Private Sector Information Sharing", November 2017, p.26, available at *www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf*.

[2] See *The Clearing House*, "A New Paradigm: Redesigning the U.S. AML/CFT Framework To Protect National Security and Aid Law Enforcement", (TCH AML/CFT Report), February 2017, available at *www.theclearinghouse.org//media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf*.

wracked with violence, and remittances providers that serve fragile Nations like Somalia.

What type of guidance could the OCC, FinCEN, FDIC, and the Federal Reserve provide to help banks meet the banking needs of legitimate consumers and businesses that are at risk of losing access—or have already lost access?

A.3. The current derisking trend is in part a reaction to Government and supervisory characterizations of correspondent banking as a high risk business and the evolving standards within the domestic and international community.[3] The causes are clear—the systems, processes, and people required to manage examiner expectations for clients deemed to be "higher risk" are extremely costly. For example, a bank may prepare a lengthy report on a customer only to be criticized for not further documenting the grounds on which it decided to retain the customer. Institutions are therefore required to make difficult decisions, because it is often times too expensive to build out this infrastructure to support higher risk accounts. And this does not even include the risk of massive fines and reputational damage in the event a customer designated high-risk actually commits a criminal act.

Similarly, domestically, banks of all sizes report that customer due diligence (CDD) requirements have dramatically increased the cost of opening new accounts, and now represent a majority of those costs. Of course, disproportionate and heightened account opening requirements make low-dollar accounts for low- to moderate-income people much more difficult to offer and price. While the connection is not immediately apparent, AML/CFT expense now is clearly an obstacle to banking the unbanked, and a reason that check cashers and other forms of high-cost, unregulated finance continue to prosper. The problem, of course, is that bank examiners do not internalize those costs. And those in the Government who do internalize those costs play no role in examining the performance of financial institutions.

As noted in my testimony, TCH believes that Treasury should take a more prominent role in coordinating AML/CFT policy and examinations for the regime. That includes convening on a regular basis the end users of BSA data—law enforcement, national security, and others affected by the AML/CFT regime including the State Department—and setting goals and priorities for the system. Treasury is uniquely positioned to balance the sometimes conflicting interests relating to national security, the transparency and efficacy of the global financial system, the provision of highly valuable information to regulatory, tax and law enforcement authorities, financial privacy, financial inclusion, and international development.

In addition, while the AML/CFT regime is supposed to be risk-based, particularly in the context of correspondent banking relationships, it is instead perceived as being "zero miss or tolerance."

[3] See "The Great Unbanking: Swingeing Fines Have Made Banks Too Risk-Averse", *The Economist*, July 6, 2017, available at *www.economist.com/news/leaders/21724813-it-time-rethink-anti-money-laundering-rules-swingeing-fines-have-made-banks-too-risk-averse*. See also "A Crackdown on Financial Crime Means Global Banks Are Derisking", *The Economist*, July 8, 2017, available at *www.economist.com/news/international/21724803-charities-and-poor-migrants-are-among-hardest-hit-crackdown-financial-crime-means*.

Supervisors must reaffirm the risk-based nature of the regime and make clear that isolated failures to identify potentially suspicious activity should not call into question a bank's entire BSA/AML/OFAC compliance framework. Furthermore regulators should continue to clarify correspondent banking and other regulatory expectations and should provide banks with greater certainty that the banks' good-faith application of clear regulatory guidance and expectations will ensure that banks are found by their regulators and auditors to be in compliance with those requirements.

Q.4. Last year, the Countering Iran's Destabilizing Activities Act of 2017 (P.L. 115-44) was enacted. In Section 271, it required the Treasury Department to publish a study by May 1, 2018, on two issues:

Somali Remittances: The law required the U.S. Department of Treasury to study if banking regulators should establish a pilot program to provide technical assistance to depository institutions and credit unions that wish to provide account services to money services businesses serving individuals in Somalia. Such a pilot program could be a model for improving the ability of U.S. residents to make legitimate funds transfers through easily monitored channels while preserving strict compliance with BSA.

Sharing State Banking Exams: The law also required Treasury to report on the efficacy of money services businesses being allowed to share certain State exam information with depository institutions and credit unions to increase their access to the banking system.

Have you or your organization been involved with these Treasury studies?

A.4. TCH has not received a request to participate in this study.

Q.5. What advice did you give—or would you give—on the pilot studies?

A.5. We encourage the Treasury Department to solicit input from the industry on each of these studies to ensure that any recommendations incorporate private sector perspectives.

Q.6. In 2016, William and Margaret Frederick were moving from Ohio to Las Vegas. Unfortunately, it is alleged that the title company they used in Columbus, Ohio, fell for an email scam and wired the $216,000 profit from their home sale to a hacker, not to the Fredericks. William is 83 and Margaret is 75 and as of October, they were still trying to get their money back. While the Fredericks' tale is now a court case to determine who was responsible for the fraudulent information, we know that the Fredericks' experience is "very typical" of scams that divert an estimated $400 million a year from title companies into bogus accounts.

Please describe the responsibilities of financial firms to avoid these frauds?

What penalties should be assessed and by which agencies when financial firms enable theft?

What is the role for the Consumer Financial Protection Bureau to ensure financial firms protect their customers' money and information?

A.6. Wire transfers are a "push" payment in which a bank customer instructs its bank to pay another party. Under the law that applies to wire transfers, Uniform Commercial Code Article 4A, a bank is liable for losses resulting from unauthorized wire transfer instructions unless the bank and its customer have entered into a commercially reasonable security procedure agreement and the bank follows those procedures when it receives instructions. Generally banks enter into these agreements with their customers and have security procedures in place to verify that instructions are in fact the instructions of their customer.

In the unfortunate case described above, the instruction from the title company was authorized. However, the title company had been deceived, through means outside of the bank's control, into paying the wrong party. Legally it is not the bank's responsibility to determine if its customer has been deceived into paying a fraudulent actor. However, banks do not want their customers to be victims of fraud. In response to the increase in fraud attacks on their corporate and institutional customers banks have conducted extensive educational campaigns using in-person sessions, webinars, and conference calls to alert customers to fraud schemes and the steps customers can take to avoid fraud losses. These measures that customers are encouraged to take include verifying the authenticity of email, telephone, or other communications before relying on those communications to instruct wire transfers. Failure to take these precautions can result in a customer's authorized wire transfer instruction to its bank that is based upon information received from a criminal.

Q.7. In 2014, FinCEN issued an advisory with human trafficking red flags, to aid financial institutions in detecting and reporting suspicious activity that may be facilitating human trafficking or human smuggling.

To what extent do you assess that financial institutions are currently utilizing these red flags, in order to better assess whether their banks are being used for to finance human trafficking? If institutions are not widely utilizing the red flags, what actions is FinCEN taking to encourage them to do so?

A.7. As previously discussed, TCH recommends that Treasury set AML/CFT priorities for the regime to assist financial institutions as they work to provide leads to law enforcement—including on human trafficking.[4]

Financial institutions around the globe are proactively working among themselves and with the public sector to disrupt human trafficking networks. In a 2016 *Financial Times* op-ed, Standard Chartered's Group General Counsel discussed the need for enhanced public–private sector sharing, noting that presentations from NGOs and Government agencies "have improved banks' ability to detect potentially [human trafficking] related financial transactions. In turn, they have helped law enforcement disrupt traf-

[4] We note that the U.K.'s Joint Money Laundering Intelligence Taskforce (JMLIT) has established operational priorities for its public–private sector information sharing partnership *www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit.*

ficking networks."[5] Such movements are also underway in the United States.[6]

Furthermore, the U.K.'s Royal United Services Institute published a report in 2017 on the role financial institutions play in disrupting human trafficking. It studied efforts in both the U.K. and U.S. and notes the following: (i) the 2016 Dow Jones and ACAMS Global Anti–Money Laundering Survey found that "nearly 70 percent of respondents report their organizations have modified AML training and/or transaction monitoring to incorporate human trafficking and smuggling red flags and typologies," with heavy U.S. participation in that survey; (ii) financial institution approaches to disrupting human trafficking networks are mixed as some adapt alerts and guidance; others create bespoke algorithms; and others utilize other sources of information such as law enforcement inquiries or negative media alerts; and (iii) many financial institutions are proactively investigating historic transaction records rather than relying on real-time monitoring as it may not be as effective in detecting potential trafficking.[7]

The report also notes that barriers to financial institutions' efforts to combat human trafficking include: (i) difficulties with automating triggers as most human trafficking-specific signals are similar to normal commercial activity;[8] (ii) concerns from financial institutions that they receive no regulatory credit for their efforts and instead will be penalized or censured; (iii) the diverse number of financial institutions and payment methods, in multiple jurisdictions, over which such high volume and small denomination activity can occur which makes it difficult to detect without law enforcement leads and greater information sharing; and (iv) the lack of formal law enforcement feedback as well as coordinated law enforcement-endorsed efforts to address human trafficking.

As a general matter, the USA PATRIOT Act's Section 314(b) private sector information sharing provisions have reportedly been useful in addressing human trafficking and other crimes.[9]

Q.8. What are the pros and cons of reducing or eliminating the standards requiring SARs filing for insider abuse (i.e., employee misconduct)?

The common expectation is that any financial institution subjected to a cyberattack would be in touch with law enforcement about whether or not it's required to file an SAR. What are the

---

[5] See *Financial Times* op-ed by David Fein, "How To Beat the Money Launderers: Banks Must Work With Governments To Combat This Scourge", November 22, 2016, available at *www.ft.com/content/569c2e26-adb9-11e6-ba7d-76378e4fef24.*

[6] See *TCH Banking Perspectives* article by Juan C. Zarate and Chip Poncy, "Designing a New AML System", Q3 2016, available at *www.theclearinghouse.org/research/banking-perspectives/2016/2016-q3-banking-perspectives/a-new-aml-system.*

[7] See Tom Keating and Anne-Marie Barry, "Disrupting Human Trafficking: The Role of Financial Institutions", Whitehall Report 1–17, Royal United Services Institute for Defence and Security Studies, March 2017, available at *rusi.org/sites/default/files/201703_rusi_disrupting_human_trafficking.pdf.*

[8] FinCEN implicitly acknowledges this in their 2014 human trafficking advisory when it says "financial institutions may consider incorporating [FinCEN's red flags] into their monitoring programs. In applying these red flags, financial institutions are advised that no single transactional red flag is a clear indicator of human smuggling or trafficking-related activity." See *www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a008.*

[9] See Testimony of William J. Fox before the U.S. House Financial Services Subcommittees on Financial Institutions and Consumer Credit and Terrorism and Illicit Finance, November 29, 2017, available at *financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-wfox-20171129.pdf.*

pros and cons of eliminating SAR filing requirement for cyberattacks against financial institutions?

A.8. While we do not support eliminating SAR filings in all insider abuse cases, we do believe that those filing requirements should be further tailored, perhaps by making them subject to the same dollar thresholds as other submissions. We believe that this would allow firms to shift resources away from investigating activity that, even if it proved criminal, would almost certainly never be prosecuted, and towards innovative efforts to detect more serious offenses. We cannot think of a "con" for this change.

Similarly, with respect to cyber, we presume that cyber SAR filings are of little to no utility, for the reasons you state. However, we would strongly urge the Committee to confirm this impression with law enforcement or FinCEN—that is, by asking them whether there are investigations where a SAR filing, as opposed to direct engagement with the firm, helped make a case.

Q.9. Most of the cost of regulatory compliance for financial institutions has been in the BSA/AML area. Yet, when we talk of simplifying regulations for community banks, we have not addressed this issue even though our banks and credit unions tell us this is the most costly and complex.

Can you give a percent of staff resources invested in AML/BSA compliance for financial institutions of less than $50 billion in assets?

A.9. BSA/AML reform would benefit institutions of all sizes. In 2017, TCH testified before the House with a community banker who reported that his three-branch bank has four lending officers and six AML compliance officers. While TCH represents 25 large commercial banks, the regime is no more rational for smaller banks.[10]

RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM DENNIS M. LORMEL

Q.1. *Strengthening Financial Intelligence Tools*—You have studied the financial underpinnings of recent terrorist attacks, like the 2017 attack in Manchester, England, where a suicide bomber killed 22 people and injured more than 100. Investigations in the aftermath of that event led to the arrest of a network of at least 15 more suspects. At the time, you wrote it was unlikely our current AML and terror finance regimes could have alerted U.K. or U.S. authorities to this type of attack.

What specific financial intelligence tools should we strengthen to detect and disrupt the planning and finance of such attacks? Is our current response capability sufficiently joined up, both within the United States and with key allies, so that key financial evidence is swiftly identified and shared with relevant law enforcement authorities?

A.1. In attacks like Manchester, it is extremely unlikely that financial institutions would generate alerts through transaction moni-

[10] See Testimony of Lloyd DeVaux before the House Financial Services Committee Subcommittee on Financial Institutions and Consumer Credit, June 28, 2017, available at *financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-ldevaux-20170628.pdf.*

toring because the banking activity of most of the individuals involved would usually not raise any suspicion to cause an alert. The funding flowing through the account, particularly for homegrown violent extremists would be generated by their employment compensation, entitlement funds, or other sources that would usually not raise suspicion. If they were engaged in criminal activity, there would be more likelihood this type of funding might generate an alert as being potentially suspicious but that would be contingent on the funding flow. These types of individuals, for the most part, want to avoid detection. It's usually not until after the event occurs, when names are reported in the media that financial institutions would identify transactional activity or account relationships through name identification of the negative news.

I've written a number of articles with different ideas about identifying terrorist financing. It's extremely difficult. I'm happy to forward a sampling of the articles to provide more context. The problem is most people, including individuals working in financial institutions do not adequately understand the funding flows nor are they familiar with terrorist financing typologies. We tend to look at terrorist financing more generically and do not visualize sources of funds, methods of moving funds or how terrorists access funds. I believe there are three funding streams with numerous variations of the three primary funding streams.

I believe U.S. law enforcement and their international law enforcement do a good job of sharing and exchanging information. Law enforcement does not do as good a job sharing information with financial institutions. Part of the problem is a lack of capacity. Part of the problem is a good deal of information cannot be shared do to considerations to include grand jury secrecy and classified information. I have been a proponent for providing security clearances to select personnel in financial institutions dating back to when I formed and ran the Terrorist Financing Operations Section (TFOS) at the FBI. In fact, I recommended that the 9/11 Commission recommend that security clearances should be granted to bankers. They did not concur with this. I am still a firm believer that security clearances would lead to better information sharing.

Financial institution AML personnel are very dedicated to identifying money laundering and terrorist financing.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR SASSE FROM DENNIS M. LORMEL

Q.1. I'd like to understand better the law enforcement context for the U.S.'s efforts to fight money laundering.

Does the U.S. financial system substantially—even if inadvertently—facilitate human trafficking?

A.1. The U.S. financial system does facilitate human trafficking. The financial system also serves as a detection mechanism. I conduct a lot of AML training, speak frequently at AML and terrorist financing conferences and write articles published mostly by the Association of Certified Anti–Money Laundering Specialists (ACAMS). I make the point that financial institutions are either facilitation tools or detection mechanisms. I stress that we need to do more to enhance detection and limit facilitation.

I believe that AML compliance professionals are dedicated to identifying money laundering and especially for heinous crimes such as human trafficking. In my response to Senator Cortez Masto's questions, I spoke about proactive initiatives certain financial institutions have taken in partnership with law enforcement. Below is the answer I provided which puts context around my comment above about public–private partnerships.

The Association of Certified Anti–Money Laundering Specialists (ACAMS) has made human smuggling a long time priority. They started a working group in 2010 with a group of major banks and Homeland Security Investigations. Bank analysts and Homeland Security Investigations analysts developed patterns of activity or typologies consistent with human smuggling. JPMorgan Chase had a team of special investigators who conducted targeted transaction monitoring and identified potential suspicious activity. ACAMS gave JPMorgan Chase and Homeland Security a special award in recognition of their outstanding collaboration. Another outstanding example of public–private sector partnerships occurred in January 2018, in the run up to the Super Bowl. The ACAMS Minneapolis Chapter held a half-day long learning event focused entirely on human slavery/trafficking. I was proud to be the first speaker. U.S. Bank, Homeland Security Investigations, and the U.S. Attorney's Office in Minneapolis collaborated to develop typologies to identify human sex trafficking specifically related to travel for the Super Bowl. These types of initiatives have a great impact on crime problems like human trafficking. I must give a cautionary comment, that this type of initiative is not as easy as it sounds. It can be costly; there are regulatory concerns and other impediments that must be overcome. The September issue of *ACAMS Today* magazine had a detailed article about the Minneapolis learning event. I would be happy to provide a copy of *ACAMS Today* if you'd like one.

Q.2. What about terrorism?

A.2. Like money laundering for human trafficking, financial institutions serve as either facilitation tools or detection mechanisms for terrorist financing. It is easier to develop typologies and red flags for human trafficking and other crimes than it is for terrorist financing. That is one reason I spend a considerable amount of my time teaching and writing about terrorist financing. Terrorist financing is very complex and multifaceted. I believe there are three basic funding streams and many variations of the three funding streams. What also needs to be considered is who you are dealing with, organizations or individuals. I have a great deal of content in terms of power point presentations and articles providing greater detail that I'm happy to share.

AML professionals are vigilant and would like to identify potential terrorist financing but generally, they do not understand terrorism or the funding flows to be concerned about and how it impacts their institutions. This is not for a lack of trying. It's an extremely complex issue. I encourage financial institutions to form specialized investigations teams, analogous to law enforcement SWAT teams to address issues like terrorist financing, human trafficking and transnational criminal organizations, as you inquire

about below. One of the problems we have in AML compliance is that we are inherently reactive. The more we can be "urgently" reactive and to the extent we can be proactive, the more detective and disruptive we can be.

Q.3. What about drug cartels and violent gangs such as MS–13?

A.3. I would characterize drug cartels, violent gangs, and organized crime organizations as either transnational criminal organizations or domestic criminal organizations. Either way, they would operate locally, regionally, and/or globally. Again, financial institutions serve as facilitation tools or detection mechanisms. Here, one of my principal concerns is the nexus between transnational criminal organizations and terrorist groups. I refer to this as the problem of convergence and diversification. Criminal and terrorist groups converge to act together in criminal activity or to share the same supply chains and channels for shipping illicit goods and for human smuggling and trafficking. As these hybrid operations mature, they diversify into more seemingly legitimate activity. This is where public–private partnerships become more important and meaningful.

Q.4. Can you walk me through a typical case, either as an agent or as a field manager, where you used financial intelligence, such as suspicious activity reports, to catch these sort of criminals?

A.4. Senator, thank you for this question because it goes to the heart of my January 9th written and oral testimony. Every day, law enforcement uses BSA data, either in the form of SARs, CTRs, 8300s, or other BSA data, to predicate or enhance criminal investigations. I just attended the West Coast AML Forum annual conference in San Francisco (May 2–4, 2018). Three separate law enforcement case studies were presented that were built on SARs, CTRs, 8300s, and other BSA data. One case revolved around Ponzi schemes, one around Asian Organized Crime, and one around dark web internet sites selling illicit goods, including synthetic opioids. They were very compelling presentations demonstrating the importance of building evidence around BSA data. In addition to those presentations, I gave a presentation on terrorist financing and stated that the FBI relies extensively on SARs and CTRs for terrorist financing investigations.

To more directly answer your question, as a hypothetical, as a law enforcement agent I receive a SAR about an investment fraud. I would run the subject name(s) and collateral identifying data through the SAR database and through my agency's investigative indices. I may or may not get additional hits. However, if it's an investment fraud, it most likely will have multiple victims, perhaps through multiple financial institutions. I would contact the financial institution(s) filing the SAR(s) and request the SAR decision documentation. I would attempt to establish predicating information to open a case to present to a prosecutor. I would get grand jury subpoenas for bank account records and begin my investigation to "follow the money." As I proceed, it is likely I'll identify CTRs and additional SARs. Through bank account analysis, I'll likely identify other bank and credit card accounts and continue to build my links to co-conspirators. I'd continue to build financial evidence along with other evidence to include audio and video record-

ings, surveillance, interviews and other investigative steps to build my case. Often times an investigation as I'm describing could lead to an opportunity to establish an undercover operation where the undercovers provide money laundering services to the bad guys. I would continue to build my case to obtain an indictment and sustain a prosecution. At every step in the process, financial record and BSA data will be essential elements of the case.

I used SAR and CTR information in terrorist financing following 9/11 for purposes of developing strategic intelligence about current and emerging trends. We established a datamining initiative where we used SAR and CTR information with other buckets of information to develop said strategic intelligence. I believe that capability is more robust today than in the 2001–2003 timeframe.

In training presentations I give regarding SARs, I have a flow chart about the lifecycle of a SAR. I would be happy to provide it to you and to provide a demonstration or explanation.

Q.5. At the FBI, what percentage of the time would you estimate that unique leads are generated from AML tools, such as suspicious activity reports and currency transaction reports?

A.5. I cannot give you a definitive answer of the current status of how SAR and CTR data is used at the FBI today. When I was Chief of the Terrorist Financing Operations Section (TFOS), following its formation and through 2003, we checked for and/or used SAR and CTR data extensively. One of the processes we established was that all terrorism cases had a financial sub-file and that SAR and CTR checks were made. Between December 2000 and 9/11, while I was Chief of the Financial Crimes Section, we had an analyst checking the SAR database on a daily basis to find SARs we could take actionable steps with. We also had a pilot program regarding money laundering and running through the SAR database for SARs we could predicate investigations with and refer out to field offices. I participate in bank working group outreach meeting that TFOS has with financial institutions a few times a year. TFOS leaders discuss how SARs are used for their investigative targeting in terrorism cases. Although I cannot provide information about how other divisions within the FBI use SARs and CTRs, my sense is they are widely used. The FBI has a cadre of forensic accountants that work throughout the criminal and counterterrorism programs. My expectation is they regularly rely on BSA data in their financial investigations.

Q.6. What should our risk tolerance be for the fact that the U.S. financial system facilitates crimes like human trafficking? Should we strive to have zero incidence of money laundering in our financial system?

A.6. The Bank Secrecy Act specifically states that financial institutions have AML programs that are "reasonably designed" to identify and report suspicious activity. With the volume of transactions that take place on a daily basis it is impossible to identify all suspicious activity. Having a reasonably designed program is the appropriate standard. In a perfect world, we could consider a zero tolerance for money laundering standard. However, in the real world, that is an impossible standard. We should always strive to improve transaction monitoring and rely more on innovation to improve the

detection versus facilitation capabilities. In my view, ensuring that financial institutions develop and maintain "reasonably designed" AML standards is appropriate.

Q.7. I'd like to understand better how technological innovation is transforming the fight against money laundering and how Government policy can help or hurt these efforts.

In the health care context, I hear about how researchers have used machine learning and artificial intelligence to identify diseases and predict when they will occur, using data points that humans would have never put together. How have financial institutions or law enforcement officials been able to use of similar techniques to identify money laundering and how much more progress can be made in this front?

A.7. I believe we need to embrace technology and use technological advances to better monitor for suspicious activity and to support criminal investigations. In the last few years, technology has been greatly enhances. We should be exploiting technology as much as we can to enhance monitoring and investigative capabilities. We need to ensure the legal and regulatory framework is in place to support technology. We must also ensure that individual privacy rights are not abused. I'm not a technology expert. I would encourage the Committee to hold hearings and briefings with technology experts and privacy rights advocates to determine what technologies can be exploited in a legal framework.

I would also note, that no matter how advanced machine learning and artificial intelligence become, we will always need humans to conduct investigations and to make the decisions on filing SARs and other BSA decisions.

Q.8. Outside of AI and machine learning, how can recent FinTech innovations such as blockchain fight money laundering?

A.8. As I noted above, I am not an IT expert. However, FinTech needs to be included in the discussion about improving the effectiveness and efficiency of AML reporting requirements. I believe blockchain is only going to gain momentum and become more mainstream. We need to take a step back and better understand blockchain and accountability regarding blockchain and other emerging technology. I honestly believe, in listening to experts familiar with blockchain, that blockchain can be a tool to fight money laundering.

Q.9. What regulatory requirement or requirements—if any—most hinders the adoption of technological innovations?

A.9. As I noted above, I am not an IT expert. I'm not sure if it's a regulatory problem as much as a cost consideration. Regardless of cost considerations, the problem is not regulations. Rather it is the regulators and the lack of clarity and leadership by regulators concerning regulatory expectations. My sense is financial institutions are concerned about potential regulatory consequences they may face for enhancing technology. There is concern that if new innovations will result in criticism that the older technology will be criticized for not having picked up the same level of alerts causing them to have to look back for potential suspicious activity perceived to be missed. At the ACAMS AML Conference held in Hollywood,

Florida, from April 9–11, 2018, during a regulator panel, one regulator advised that if financial institutions upgraded their transaction monitoring system, they should run the two systems in parallel for a period of time to ensure that if one system generates more alerts, the other is assessed to see if it missed alerts. That's a cause for concern for two reasons, cost and perceived regulatory action against the financial institution. This is a deterrent and not an incentive to enhance technology.

Q.10. How much does bitcoin, blockchain, and other cryptocurrencies facilitate money laundering? How—if at all—should this impact our approach to combating money laundering in traditional banks? How can law enforcement officials best stop this newer form of money laundering?

A.10. As bitcoin, blockchain, and other cryptocurrency continue to emerge and gain popularity and usage, it will grow as a money laundering challenge. The initial reaction to bitcoin, blockchain, and other cryptocurrency, and its attractiveness to money launderers and criminals was its perceived anonymity. Experts have demonstrated that is not true and that they can identify people engaging in bitcoin and other cryptocurrency transactions. This is a money laundering deterrent. However, the more bitcoin and other cryptocurrencies are used, and the more they can be used in cash like manners, the more prevalent the money laundering challenge will become. Part of the problem is the extent to which the dark net can be used and the level of anonymity that bad guys can develop and exploit.

Q.11. I'd like to discuss Suspicious Activity Reports (SARs). Today, around 2 million SARs are filed each year. While every SAR used to be read by law enforcement officials, that is no longer the case today. Financial institutions often complain that they rarely, if ever, receive feedback from law enforcement officials on the utility of any particular suspicious activity report that they file. This lack of feedback loops increases the burdens on financial institutions, who continue to file SARs that are of little utility to law enforcement officials. It also prevents financial institutions from developing better analytical tools to more precisely discern between the signal and the noise.

What percentage of SARs are actually read by someone in law enforcement?

A.11. First, to the statement above, the number of SARs read by law enforcement and feedback regarding SARs are two separate issues and should not be compared with each other or considered a metric for whether law enforcement reviews SARs.

I cannot give a precise percentage for how many SARs are reviewed by law enforcement but based on my experience I confidently believe a very high percentage of SARs, if not all SARs, are reviewed in some fashion. At a macro level, a program level or for strategic purposes the FBI, IRS, and FinCEN possess analytics and/or datamining initiatives that scrub all SAR data. At the grassroots or field office level SARs that fall into the grassroots or field office jurisdictions throughout the U.S. are reviewed. I believe that most, if not all, SARs receive at least a cursory manual review. I think there are 94 U.S. Attorney's Offices (USAOs) in the U.S.

Each USAO has at least one SAR review team. SAR review teams are composed of agents from Federal law enforcement agencies in each jurisdiction, most prominently IRS and FBI agents and/or analysts. In addition, field office personnel or State and local law enforcement review certain SARs independent of the SAR review teams. As an example, the Manhattan District Attorney's Office has a SAR review team. I'm confident that most, if not all, SARs are reviewed by law enforcement.

Q.12. How often do financial institutions receive feedback from law enforcement officials as to the utility of their SAR filing?

A.12. Feedback from law enforcement to financial institutions regarding the value of SARs is problematic. I have frequently heard the same complaint from financial institutions. As noted above, the lack of feedback does not mean SARs were not reviewed or that SARs did not predicate and/or enhance law enforcement investigations. In response to the frustration on the part of financial institutions about the lack of SAR feedback, I always make it a point when I provide training to AML professionals to discuss how important SARs are to law enforcement. I also include in my presentations a flow chart I developed regarding the lifecycle of a SAR. As I mentioned in an earlier response to one of your questions, I'd be happy to provide the flow chart to you.

When I was the Chief of TFOS in the FBI, I frequently met with then FinCEN Director James Sloan. We often spoke about developing a consistent feedback mechanism for financial institutions but were unable to develop an adequate mechanism to do so. There are a number of inherent impediments to establishing a feedback mechanism. Such include the nature of criminal investigations. From the point a SAR is filed to the point a case is concluded, it could be a period of one or more years. If a case is a Grand Jury investigation, information cannot be disclosed by law enforcement. Law enforcement lacks the resources to consistently provide feedback. There are always new cases to move forward with and investigators don't have time to provide feedback. Impediments aside, they are no excuse for not providing feedback. I believe a feedback mechanism should be developed and implemented through FinCEN initiated by law enforcement. I concur with your comment that a SAR feedback mechanism would improve the quality of SAR submissions. I also believe that a SAR feedback would improve the morale of AML professionals who are involved in the SAR process. They would have a greater sense of accomplishment and satisfaction that their work contributes to law enforcement successes. Make no mistake; SARs play a significant role in investigations.

Q.13. While some have proposed reducing the number of SARs and CRT filings because they are often superfluous and are never read, others argue that this poses risks, because investigating minor infractions may still lead to significant law enforcement successes. How should policymakers resolve this conflict?

A.13. Having been the direct beneficiary of SARs and having used SARs at the program or macro level for strategic analysis, I'm a strong proponent that more SARs and CTRs are better. Agents who manually review SARs at the grassroots level would probably opine that less is better. In any event, a disparate SAR that may not

have a high financial loss from a consumer fraud or elderly fraud may likely be identifiable with similar SARs. When those SARs are aggregated, what was an insignificant fraud could escalate into a massive fraud case. I think policy makers should take a serious look at this issue. There are merits to both arguments. My opinion is there is more merit to not reducing the number of SARs filed, especially by increasing SAR thresholds. I am definitely staunchly against that alternative.

Q.14. How could regulators (1) set up better feedback loops between financial institutions and law enforcement officials that could help financial institutions better identify money laundering; and (2) empower financial institutions to act upon their improved ability to distinguish between useful and superfluous reports, including by filing fewer unnecessary SARs, without fearing regulatory consequences for doing so?

A.14. I do not believe regulators should have a role in SAR feedback or to have a voice in what a useful SAR is. Regulators have no authority over law enforcement, are not law enforcement and represent an impediment to law enforcement in the SAR process in certain regards. SARs are intended to assist law enforcement not the regulators. One criticism I have about regulators regarding SARs is that in a number of instances, financial institutions write SARs geared to what the regulators want versus what law enforcement wants. This is counterproductive. Where regulators can assist in the SAR process during their examinations is to identify situations where financial institutions do not file SARs or do not file adequate SARs. In my experience, the failure to file SARs or to adequately file SARs is the biggest breakdown in an AML program. This is where the regulators should be focused regarding SARs.

Q.15. Would a better feedback loop system exist if financial institutions employed more people with security clearances? If so, what, if anything, can the Federal Government do to facilitate this?

A.15. I have long been an advocate that select financial institution AML professionals be granted security clearances. In fact, I was interviewed many times by the 9/11 Commission. I strongly recommended to them they recommend that security clearances be granted to select financial institution personnel. Unfortunately, the 9/11 Commission did not concur. Despite that, I firmly believe security clearances would be beneficial and are warranted.

Security clearances have been given to select AML personnel on a limited basis through TFOS at the FBI for terrorist financing collaboration.

I do not believe that security clearances would improve the feedback issue. However, it would improve the ability of the Government to provide financial institutions with classified information.

Q.16. Often, financial institutions will derisk by refusing to serve customers that could be involved in illegal activity. As financial institutions start to share more information with each other, this practice could become more prominent and potential criminals could more frequently lose access to the United States' financial system altogether.

Are there instances in which derisking is actually unhelpful for law enforcement purposes, because it drives these criminals underground and makes it more difficult to track them?

A.16. Law enforcement would prefer that financial institutions do not derisk. Exiting relationships is a hindrance to law enforcement. It makes it more challenging for law enforcement to follow the money and to develop prosecutable cases reliant on financial evidence. There are times when law enforcement learns that financial institutions are going to exit an account relationship and law enforcement requests the financial institution maintain the banking relationship. In such instances, law enforcement will provide the financial institution with a keep open letter. Financial institutions often derisk and/or exit high risk relationships due to concern of adverse regulatory actions by their regulators.

Q.17. At the moment, do the regulators that evaluate and enforce financial institutions compliance with our Federal money laundering take this into account?

A.17. Regulators do not take this into account, which is a problem. Either real or perceived, financial institutions derisk because they are concerned that the regulators will take an enforcement action against the financial institution for the level of high risk they accept. This is where the regulators lack leadership and clarity with financial institutions. I've heard regulators asked to provide guidance respond that it is up to the financial institution to identify the appropriate level of risk they can manage. In many such high risk situations financial institutions believe it's better to exit the customer relationship and not face real or perceived regulatory action.

Q.18. Are there promising ways to increase cooperation between financial institutions, regulators, and law enforcement officials, so that financial institutions can make a more informed decision about when and how to derisk?

A.18. If financial institutions, regulators, and law enforcement could establish sustainable communications and take the time to understand each other's perspectives, a better sense of collaboration could be established and a middle ground acceptable to each other could be established. If you placed financial institutions, the regulators and law enforcement in a triangle and places financial institutions at the top and regulators and law enforcement at the bottom side points, there would be hard lines from the financial institutions to the regulators and law enforcement. Unfortunately, the line between the regulators and law enforcement would be a broken line. The hard lines are lines of communication. The broken line is a lack of communication. The point is the level of communications between the regulators and law enforcing is not good. This leaves financial institutions in direct communications with the regulators and law enforcement, which have conflicting interests.

Q.19. Would financial institutions need to hire more employees with a top security clearance and/or a law enforcement background for this coordination to be effective?

A.19. The issue of security clearances is not related to the issue of derisking. They are separate issues. I think it would be extremely beneficial if financial institutions hire more employees from law en-

forcement or the intelligence community who have security clearances. This would enable law enforcement to share classified information with financial institutions they would not have otherwise been able to share. Financial institutions derisk in order to avoid real or perceived regulatory actions like enforcement actions.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR TILLIS FROM DENNIS M. LORMEL

Q.1. How can we leverage technology to make the process simultaneously less onerous on banks while enhancing the outcomes of catching illegal behavior? Are there regulatory and legislative barriers to getting that down?

A.1. We should definitely seek to leverage and embrace technology to enhance transaction monitoring and to be more innovative. I believe the barriers to this are two pronged. First is cost considerations for financial institutions. The second is real or perceived regulatory expectations. Financial institutions are concerned about adverse regulatory action if they enhance technology. In questions from Senator Sasse I received a similar question. The answer I provided Senator Sasse is set forth below:

As I noted above, I am not an IT expert. I'm not sure if it's a regulatory problem as much as a cost consideration. Regardless of cost considerations, the problem is not regulations. Rather it is the regulators and the lack of clarity and leadership by regulators concerning regulatory expectations. My sense is financial institutions are concerned about potential regulatory consequences they may face for enhancing technology. There is concern that if new innovations will result in criticism that the older technology will be criticized for not having picked up the same level of alerts causing them to have to look back for potential suspicious activity perceived to be missed. At the ACAMS AML Conference held in Hollywood, Florida, from April 9–11, 2018, during a regulator panel, one regulator advised that if financial institutions upgraded their transaction monitoring system, they should run the two systems in parallel for a period of time to ensure one if one system generates more alerts, the other is assessed to see if it missed alerts. That's a cause for concern for two reasons, cost and perceived regulatory action against the financial institution. This is a deterrent and not an incentive to enhance technology.

Q.2. Financial institutions often complain that FinCEN, law enforcement officials, and prudential regulators do not tell them whether their BSA filings serve a useful purpose, or how the reports they submit are being used—and that the filings go into a black hole. Can you shed some light on the filings that you make or have used and what could be done to improve this process?

A.2. SARs are extremely important and make significant contributions to law enforcement investigations. Lack of feedback is a problem. The perception by financial institutions that SARs fall into a black hole is a misperception. SARs do not fall into a black hole. Financial institutions have a right to be frustrated about the lack of SAR feedback. In terms of developing a consistent feedback mechanisms, this is not an issue for the regulators. It is an issue

for FinCEN and law enforcement, mostly law enforcement. Law enforcement is the end user of SARs and the beneficiary of SAR information. Senator Sasse asked a similar question. Below is the answer I furnished him, which is relevant to your question.

Feedback from law enforcement to financial institutions regarding the value of SARs is problematic. I have frequently heard the same complaint from financial institutions. As noted above, the lack of feedback does not mean SARs were not reviewed or that SARs did not predicate and/or enhance law enforcement investigations. In response to the frustration on the part of financial institutions about the lack of SAR feedback, I always make it a point when I provide training to AML professionals about how important SARs are. I also include in my presentations a flow chart I developed regarding the lifecycle of a SAR. As I mentioned in an earlier response to one of your questions, I'd be happy to provide the flow chart to you.

When I was the Chief of TFOS in the FBI, I frequently met with then FinCEN Director James Sloan. We often spoke about developing a consistent feedback mechanism for financial institutions but were unable to develop an adequate mechanism to do so. There are a number of inherent impediments to establishing a feedback mechanism. Such include the nature of criminal investigations. From the point a SAR is filed to the point a case is concluded, it could be a period of one or more years. If a case is a Grand Jury investigation, information cannot be disclosed by law enforcement. Law enforcement lacks the resources to consistently provide feedback. There are always new cases to move forward with and investigators don't have time to provide feedback. Impediments aside, they are no excuse for not providing feedback. I believe a feedback mechanism should be developed and implemented through FinCEN initiated by law enforcement. I concur with your comment that a SAR feedback mechanism would improve the quality of SAR submissions. I also believe that a SAR feedback would improve the morale of AML professionals who are involved in the SAR process. They would have a greater sense of accomplishment and satisfaction that their work contributes to law enforcement successes. Make no mistake; SARs play a significant role in investigations.

Q.3. Another compliance challenge often cited by banks is that they feel pressured by bank examiners and law enforcement authorities to exit certain business lines or cease offering certain services to customers viewed as presenting particular money-laundering vulnerabilities, i.e., severing corresponding banking relationships with foreign institutions in certain geographic areas, and also ending money services businesses (MSBs, i.e., check cashing, money transmitters, currency exchange outlets, etc.)

As banks reevaluate their business relationships with MSBs in light of what they may view as a hostile regulatory landscape, what can we do to change this type of behavior/is this a prevalent problem in the industry?

A.3. Senator, let me answer the second part of your question first. The issue is a significant prevalent issue in the industry. The term referred to for exiting high risk relationships by financial institutions is "derisking". The problem here is with the regulators. Either

real or perceived, financial institutions believe they will face regulatory enforcement actions if they continue to bank high risk customers. This is where I believe regulators lack leadership and clarity. They do not provide guidance to financial institutions about banking high risk customers. I have heard regulators at conference state it is not their responsibility to provide such guidance but it's the responsibility of the financial institution to determine the level of risk they can manage. This lack of guidance leads to financial institutions exiting high risk customer relationships.

Q.4. It is my understanding that there are times when law enforcement and the bank regulators work at cross purposes. That is, law enforcement might want a bank to continue banking an individual or company that they are following and building a case against but the bank regulators, whose incentives are to not be embarrassed by their regulated entities, force the banks to "derisk" or close those accounts. Is that actually the case?

A.4. Unfortunately, this is the case. As noted in my response to your previous question, either real or perceived, financial institutions derisk out of fear of regulatory enforcement actions. The regulators do not provide financial institutions with leadership or clarity about maintaining high risk relationships. Consequently, financial institutions exit these relationships. Regulators state that they do not want derisking but they want inclusion. The problem is they do not provide the guidance about banking high risk customers.

Law enforcement would prefer the account relations not be exited, especially in cases of ongoing investigations. Below is the response to a similar question that I provided to Senator Sasse.

Law enforcement would prefer that financial institutions do not derisk. Exiting relationships is a hindrance to law enforcement. It makes it more challenging for law enforcement to follow the money and to develop prosecutable cases reliant on financial evidence. There are times when law enforcement learns that financial institutions are going to exit an account relationship and law enforcement requests the financial institution maintain the banking relationship. In such instances, law enforcement will provide the financial institution with a keep open letter. Financial institutions often derisk and/or exit high risk relationships due to concern of adverse regulatory actions by their regulators.

Q.5. In terms of AML, we know that the success of AML is centric around whether or not the predicate crime of money laundering has been reduced, but we only really know how pervasive money laundering is on a reactive basis, i.e., when someone/some entity is caught. To that end, do you believe the advent/popularity of cryptocurrencies could affect the capture of money laundering/could it affect AML? Do enforcement authorities have the technological capabilities to work with private industry to capture mal-actors?

A.5. The challenge of identifying money laundering is that it is an inherently reactive process. The evolution of cryptocurrency presents new challenges for financial institutions. This is certainly one area where public–private sector partnerships could better address the emerging challenges of cryptocurrency. I responded to a similar question from Senator Sasse. Below is the response I provided him with.

As bitcoin, blockchain, and other cryptocurrency continue to emerge and gain popularity and useage, it will grow as a money laundering challenge. The initial reaction to bitcoin, blockchain, and other cryptocurrency, and its attractiveness to money launderers and criminals was its perceived anonymity. Experts have demonstrated that is not true and that they can identify people engaging in bitcoin and other cryptocurrency transactions. This is a money laundering deterrent. However, the more bitcoin and other cryptocurrencies are used, and the more they can be used in cash like manners, the more prevalent the money laundering challenge will become. Part of the problem is the extent to which the dark net can be used and the level of anonymity that bad guys can develop and exploit.

Q.6. In your opinion, do you think that the overall AML regime has been effective? Additionally, what do you see as the best way to ensure future effectiveness?

A.6. As I stated in my written and oral testimony at the Committee hearing on January 9th, the flow of BSA information from financial institutions to law enforcement is invaluable. In this regard the AML regime is effective. The system is flawed when you overlay regulatory requirements. The system could be more effective and efficient. I encourage the Committee to assess the perspectives of all stakeholders in the process, especially law enforcement and financial institutions who I consider the two primary stakeholders. BSA information is intended to assist law enforcement. Financial institutions are the repository for financial intelligence and serve as the filter for identifying and reporting suspicious activity. I believe there are three primary factors that Congress should consider:

1. How to incentivize financial institutions to enhance technology and be innovative. In addition to cost factors, this will require dealing with the real or perceived regulatory expectations financial institutions are concerned about regarding upgrading technology. Financial institutions are concerned about potential adversarial regulatory consequences.
2. How to make transaction monitoring and the SAR process more effective and efficient. The key is to improve the percentage of SARs that are meaningful and are used to predicate and/or enhance law enforcement investigations.
3. How to establish a consistent and meaningful feedback mechanism from law enforcement to financial institutions regarding the value of SARs. This would be one factor that would contribute to improving the effectiveness and efficiency of the SAR process.

Q.7. Is it to have Treasury be the lead to:

1. Define with other stakeholders specific and clear national priorities of the regime; and
2. Determine, working with other stakeholders, clear and measurable objectives of the regime in light of those priorities. Should Treasury or someone else have to report those measurements against the objectives back to Congress?

A.7. This is a difficult question that requires considerable assessment by numerous stakeholders with varying perspectives. On one hand, I concur that from a practical point of view, one department or stakeholder should be the lead to establish specific and clear national priorities and set clear and measurable objectives that are reported back to Congress. My problem is that Federal departments and agencies within those departments have vastly different responsibilities and mandates. Therefore, could one department objectively determine the overall priorities for the intergovernmental community? For example, the Treasury Department is primarily responsible for sanctions and enforcement. Whereas, the Department of Justice (DOJ) and Homeland Security are responsible for law enforcement. From a practical standpoint, it would be prudent to designate Treasury to be responsible. However, without equal input, my concern would be that DOJ and Homeland Security law enforcement perspective and priorities might not be accurately stated and/or prioritized. In addition, are their other stakeholders who should be included in the reporting process such as the CIA and Department of Defense (DOD)? The CIA and DOD are both engaged in threat and/or terrorist financing. Having co-responsibility might be an acceptable alternative. However, that would be a challenge for efficiency. Perhaps Treasury, DOJ, Homeland Security, and other Government stakeholders should be responsible to submit similar reports to more specifically define their priorities, objectives and measurable.

Regardless of who is designated with reporting responsibility, I believe it would be prudent to have a reporting mechanism to Congress.

This idea may have come from the Clearinghouse report, dated February 2017, titled "A New Paradigm: Redesigning the U.S. AML/CTF Framework to Protect National Security and Aid Law Enforcement". I was not involved in the Clearing House assessment process. However, my concern is the principal participants possessed more of a Treasury perspective (sanctions and enforcement) verses a law enforcement perspective. I understand the working group included former law enforcement officials. However, in reading the Clearing House report, my concern is law enforcement interests were not adequately considered. As noted in my written and oral testimony on January 9th, I contacted then current law enforcement executive in positions like I held in the FBI, and none were included in the discussions. I believe the Clearing House report sets a good framework for improving BSA reporting. However, law enforcement should have greater engagement in the assessment process.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM DENNIS M. LORMEL

Q.1. What are the costs and benefits of having bank examiners assess bank compliance with the Bank Secrecy Act's (BSA) requirements instead of having anti–money laundering (AML) and combating the financing of terrorism (CFT) experts at the Financial Crimes Enforcement Network (FinCEN) examine bank compliance programs?

A.1. I do not believe it is practical to have FinCEN perform the bank examinations/program reviews as currently done by the regulatory agencies. First and foremost, FinCEN does not have the capacity to handle such demands. They lack the required resources. FinCEN resources do not have the same level of examination training or experience that regulatory agencies possess. I believe it is imperative that FinCENs primary responsibility continue to be to collect BSA reporting information and to serve as the conduit between financial institutions and law enforcement. FinCEN should continue to be involved in regulatory actions on a case specific basis and in conjunction with the regulators. FinCEN should continue to provide regulatory guidance to financial institutions. FinCEN should also continue to conduct the analytical work they perform in support of law enforcement.

Q.2. Is there a way to maintain a top-shelf effective AML/CFT policy while maintaining a commitment to increase access to financial products for the underbanked and immigrants who rely on remittance services?

A.2. I'm a proponent for inclusion of the underbanked and immigrants who rely on remittance services. I conduct AML, terrorist financing, and fraud training on a regular basis. I also write articles published in industry publications, such as *ACAMS Today* magazine. In these forums, I frequently state that illegal money remitters represent one of the most significant vulnerabilities to the U.S. financial system. Part of the problem is that some illegal money remitters and underbanked customers have been derisked. Derisking is a significant problem. Much of the problem regarding illegal money remittance is that different ethnic communities, especially with the underbanked and immigrants prefer to use illegal money remitters to transmit funds back to family members in their countries of origin.

One of the solutions to the issue of derisking is for regulators to provide leadership and clarity to financial institutions about regulatory expectations. Another solution for the issue if illegal money remittance is for FinCEN, law enforcement, and financial institutions to establish a partnership and working group to address the issue of illegal money remittance operations.

Q.3. I'm interested in the ways in which technology can aid AML compliance efforts. What are some of the innovative technologies that you've seen that hold some promise for either the Government or the private sector?

A.3. I'm not an IT expert. However, I believe that financial institutions should embrace technology. In doing so, they should also demand transparency with new technology driven product offerings. Regarding transaction monitoring, financial institutions should be considering technology enhancements through artificial intelligence and FinTech capabilities.

Q.4. What are the barriers to either the Government or the private sector adopting these technologies?

A.4. In my opinion, the barriers to Government are primarily cost related. The barriers also include Government bureaucracy. The barriers to the private sector, specifically to financial institutions,

are cost and real or perceived regulatory expectations. I was asked similar questions by your colleagues Senators Sasse and Tillis. Below are my responses to their questions.

1. We should definitely seek to leverage and embrace technology to enhance transaction monitoring and to be more innovative. I believe the barrios to this are two pronged. First is cost considerations for financial institutions. The second is real or perceived regulatory expectations. Financial institutions are concerned about adverse regulatory action if they enhance technology. In questions from Senator Sasse I received a similar question. The answer I provided Senator Sasse is set forth below:
2. As I noted above, I am not an IT expert. I'm not sure if it's a regulatory problem as much as a cost consideration. Regardless of cost considerations, the problem is not regulations. Rather it is the regulators and the lack of clarity and leadership by regulators concerning regulatory expectations. My sense is financial institutions are concerned about potential regulatory consequences they may face for enhancing technology. There is concern that if new innovations will result in criticism that the older technology will be criticized for not having picked up the same level of alerts causing them to have to look back for potential suspicious activity perceived to be missed. At the ACAMS AML Conference held in Hollywood, Florida, from April 9–11, 2018, during a regulator panel, one regulator advised that if financial institutions upgraded their transaction monitoring system, they should run the two systems in parallel for a period of time to ensure one if one system generates more alerts, the other is assessed to see if it missed alerts.

That's a cause for concern for two reasons, cost and perceived regulatory action against the financial institution. This is a deterrent and not an incentive to enhance technology.

Q.5. What can we be doing as legislators to ensure that we promote technological innovation in this sector?

A.5. Technology innovation is important. If I was a legislator, I would consider what I could do to incentivize financial institutions to embrace technology. One thing I would assess is how to encourage regulators to take a leadership role and to provide financial institutions with guidance and clarity to change the real or perceived concern by financial institutions that there could be adverse regulatory enforcement actions for enhancing technology as addressed in the response to the prior question.

Q.6. The regulatory definition of "financial institution" has been expanded several times over the years, both by FinCEN rulemaking and by legislation by Congress.

Should the definition of financial institutions be expanded to include other sectors? If so, which sectors?

A.6. The one sector that comes to mind where the definition of "financial institution" might be included is the real estate sector. As addressed in Geographic Targeting Orders (GTOs), issued by FinCEN to require U.S. title insurance companies to identify the

natural persons behind shell companies used to pay "all cash" for high-end residential real estate in six major metropolitan areas, money laundering through real estate is a significant problem. Certainly, where focus was placed on this specific money laundering problem, the GTOs were warranted. But the problem of money laundering through real estate is much broader. There are a number of real estate schemes to include criminal property flipping that have had a detrimental economic impact on many U.S. cities.

I believe that to answer how broadly the real estate sector should be regulated as a financial institution requires considerable assessment. Stakeholders should include FinCEN, real estate professionals and experts, financial institutions, law enforcement, and academics who have researched money laundering in the real estate sector. As an example, the Terrorism, Transnational Crime and Corruption Center (TraCCC) at George Mason University (GMU), held a daylong conference at GMU's Schar School of Policy and Government to learn about money laundering through the real estate sector. The forum was held on March 23, 2018. Speakers included experts from the real estate sector, law enforcement banks, Government, associations, nongovernment organizations, and academia. I served as a moderator for a panel addressing new approaches to countering money laundering in real estate in the U.S. A draft report has been circulated to conference speakers and organizers. The report is in the process of being finalized. If you are interested, I'd be happy to provide a copy of the report after it's published.

Q.7. Could these changes be made via FinCEN rulemaking or should legislation be passed?

A.7. I believe both FinCEN rulemaking and legislation are warranted. I believe that the GTO's issued by FinCEN are an outstanding example of FinCEN rulemaking. However, the long-term solution is legislation. Congress should consider establishing a working group to assess how best to craft legislation to address the broader risks of money laundering through real estate.

Q.8. In August 2017, FinCEN issued an advisory encouraging real estate brokers to share information with them that could be helpful in AML efforts, while noting they are not required to do so under current law.

How do we increase information sharing between real estate brokers and FinCEN?

A.8. Meaningful information sharing between real estate brokers and FinCEN is more likely to be accomplished through rulemaking and legislative requirements. An alternative that could result in voluntary information is to promote awareness through outreach, particularly in the real estate sector, about the risk and consequences of money laundering through real estate.

Q.9. Geographic Targeting Orders (GTOs), which impose additional record keeping and reporting requirements on domestic financial institutions or nonfinancial trades or businesses in a specific geographic area for transactions involving certain amounts of United States currency or monetary instruments, have been deployed since 2016 to target high-end real estate sectors in major metropolitan

areas by requiring U.S. title insurance companies to identify the natural persons behind shell companies used to pay "all cash" for high-end residential real estate.

Are GTOs an effective tool or would regulation be a preferable way to cover the real estate sector?

A.9. I applaud the GTOs. They are a good step forward in addressing the money laundering issues in real estate. The GTO's focus on one significant money laundering problem. I believe this has had the intended impact and that is why the GTOs were extended in 2017. As noted in the response to the prior question, I believe the long-term solution is regulations that are broader than the one issue addressed in the GTOs. Regulations need to address a broader range of money laundering risks in the real estate sector.

Q.10. Cryptocurrency exchanges are money services businesses supervised by State regulators and subject to Federal AML and CFT laws.

Should FinCEN play an enhanced role in assessing the compliance of cryptocurrency exchanges, or are State regulators sufficiently equipped to handle compliance monitoring?

A.10. I will address this question first at the State level and then at the Federal level. Overall, State regulators do a good job at enforcing State regulatory compliance requirements. However, there is no uniformity among States about regulatory requirements. Regulatory requirements vary from State to State. My sense is New York probably has the most stringent State requirements. At the Federal Government level, we need to assess the roles and perspectives Government agency stakeholders have with respect to cryptocurrency exchanges. For instance, FinCEN issued guidance to cryptocurrency exchanges in 2013. Since cryptocurrency exchanges are MSBs, they would be subject to Federal review by the IRS, who examines MSBs from a Federal regulatory perspective. In addition, the Securities and Exchange Commission (SEC) and the Commodities Futures Trading Commission (CFTC) each have interests. In some situations, the SEC could consider the trade of cryptocurrency securities transactions. In some situations, the CFTC could consider virtual currency as a commodity.

The question of should FinCEN play an enhanced role in assessing the compliance of cryptocurrency exchanges should be assessed along with the roles of the IRS, SEC, and CFTC. One question is, does FinCEN have the capacity, in terms of resources, to take on enhanced responsibilities. FinCEN should certainly provide continued guidance and rulemaking. In terms of supervision, IRS should continue to have examination responsibility. The problem here is the same question as I posed for FinCEN. Does the IRS possess adequate resources to address regulatory examination requirements?

Q.11. What additional tools could we give regulators and law enforcement?

A.11. The tools that regulators and law enforcement need to address the AML challenges posed by cryptocurrency begin with budget enhancements. From the regulators side, enhanced resources are needed in terms of personnel and equipment to perform an adequate level of regulatory examinations. Whether it's the IRS

or FinCEN, resource enhancements are needed. Law enforcement is less pressed for resource enhancements, although the need for resource enhancements should be assessed. Regulators and law enforcement could use budget enhancements to address the training requirements necessary to gain and maintain the skill sets required to address the evolving challenges posed by cryptocurrencies.

Q.12. How prevalent is money laundering in cryptocurrency markets?

A.12. I cannot speak definitively about how prevalent money laundering is in cryptocurrency markets. However, like with all types of financial institutions, there is a risk for money laundering. Like financial institutions, cryptocurrency markets serve as a facilitation tool or a detection mechanism. Our challenge is to make cryptocurrency markets more of a detection mechanism.

The common belief that cryptocurrencies can be anonymous makes cryptocurrency more attractive to money laundering. Law enforcement has begun to state that cryptocurrencies are not as anonymous as thought and that they can trace transactions and those transacting in cryptocurrency. The more law enforcement proves this fact by making arrests, getting convictions, and seizing illicit assets, the greater the deterrent there will be for money laundering through cryptocurrency. That said, the more cryptocurrency transactions become cash like transactions, the greater the likelihood for money laundering. AML transaction monitoring is inherently reactive, which poses a significant challenge for those fighting money laundering. Cryptocurrency is an evolving space. AML technology must evolve along with cryptocurrency technology.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM DENNIS M. LORMEL

Q.1. Gaming and tourism are some of Nevada's top industries. In the State of Nevada, our gaming operators employ thousands of hard working Nevadans, and the industry as a whole domestically supports 1.7 million jobs across 40 States. Qualified casinos, like financial institutions, are also subject to Banking Secrecy Act requirements. Organizations within Nevada have suggested that gaming operators would welcome a review of BSA requirements, which they find to be burdensome. They look forward to this Committee's thoughtful, bipartisan, review of BSA requirements that takes into account the security imperative for robust anti–money laundering efforts, as well as the impact those requirements have on all industries. For example, the Suspicious Activity Report (SAR) ($5,000) and the Currency Transaction Report (CTR) ($10,000) levels were set years ago. Some have recommended increasing these to correspond with inflation. Others believe that would be too high but do support a higher amount than currently,

A.1. I would like to comment here that I am not in favor of raising the SAR or CTR reporting thresholds. In today's world, where it takes small amounts of funds to commit a terrorist act, we need

the thresholds where they are. Most financial institutions will tell you the reporting thresholds do not cause extra burden to them.

Q.2. One of the top priorities of the gaming industry is to remove the requirement for a detailed factual narrative for structuring in the suspicious activity forms. What do you think of this recommendation?

A.2. I was the direct beneficiary of SARs when I was an FBI agent, especially following the terrorist attacks of 9/11. I formed and ran the Terrorist Financing Operations Section (TFOS). Following 9/11, we began a datamining project and included SAR narratives and SAR identifying information like addresses, phone numbers, and other collateral information. From a macro or program level, I liked the narrative information for all SARs to include structuring. That said, SARs are a subjective topic. If you speak to law enforcement agents at the field or grass roots level, especially those who physically review SARs, they would likely agree that structuring narratives are cumbersome and not necessary. There is no easy solution to the SAR narrative question.

Q.3. Do you have specific recommendations regarding how the gaming industry can benefit from greater communication with Government agencies and law enforcement? Is there something the Federal Government can do to share information with casinos and others filing SARs about broad benefits that may occur because of some of the 58,000 SAR forms filed by gaming firms.

A.3. I am a huge proponent for public and private partnerships and collaboration. When I ran the Financial Crimes Section at the FBI prior to 9/11, I had frequent conversation with the then Director of FinCEN, James Sloan about developing a feedback mechanism for financial institutions regarding SARs. There were numerous inherent impediments to establishing a feedback mechanism. That should not be an excuse. FinCEN and law enforcement should revisit this issue and determine how to more consistently provide feedback to financial institutions, including Casinos.

Q.4. Would the creation of a Qualitative Feedback Mechanism help reduce money laundering and terrorist financing? Should the Secretary of the Treasury establish a mechanism to communicate anti–money laundering (AML) and countering terrorism financing (CTF) priorities to financial institutions, gaming establishments, and Federal financial regulators? Could such a mechanism provide qualitative feedback on information shared by financial institutions with the Department of Treasury, including CTRs and SARs? Please describe the pros and cons of such a system.

A.4. As mentioned in the answer above, I am a firm believer in the benefits of a feedback mechanism regarding SARs. I would welcome a feedback mechanism. I do believe that would improve the identification of money laundering and terrorist financing. From an intangible standpoint, a consistent feedback mechanism would greatly improve the morale and motivation of the AML professionals involved in the SAR process. There is a constant sense that SARs go into a black hole. That is not true. SARs are extremely valuable. If AML professionals received consistent feedback, there would be more interest in filing better quality SARs that would improve the

investigative process and lead to more prosecutions and disruptions.

I do not like the idea of Treasury providing money laundering and terrorist financing priorities to financial institutions because their issues are with sanctioning and enforcement actions and not law enforcement. Non-Treasury law enforcement agencies, such as the FBI have primary criminal and intelligence for terrorism and many criminal violations. I'm not comfortable with Treasury setting priorities for matters they have limited or no jurisdiction over. If Treasury acted as a bridge with law enforcement then perhaps it would be workable.

Q.5. The Office of the Comptroller of the Currency mentioned in its 2018 Banking Operating Plan that financial institutions should not inadvertently impair financial inclusion. But, as of September 2017, the OCC has not identified any specific issues they plan to address. We know that derisking has become an epidemic across many communities and industries, such as communities along the Southwest border, humanitarian organizations aiding Nations wracked with violence, and remittances providers that serve fragile Nations like Somalia.

What type of guidance could the OCC, FinCEN, FDIC, and the Federal Reserve provide to help banks meet the banking needs of legitimate consumers and businesses that are at risk of losing access—or have already lost access?

A.5. Inclusion or derisking is a sensitive issue. Although the regulators preach inclusion and the harm of derisking, they do not adequately provide the needed guidance to financial institutions. In my view and what I have observed in working groups that discuss this issue and in other forums, the regulators do not demonstrate any leadership or clarity in providing direction. Regulators will state that it is up to banks to determine the level of risk they can manage and offer no guidance about regulatory expectations. Consequently, that lack of guidance causes financial institutions to be more risk averse and exit relationships for fear that the regulators would take a negative view and some action against the institution for banking high risk customers. Regulators should take a leadership role and provide clear guidance about regulatory expectations beyond stating that financial institutions need to identify and manage their risk.

Q.6. Last year, the Countering Iran's Destabilizing Activities Act of 2017 (P.L. 115-44) was enacted. In Section 271, it required the Treasury Department to publish a study by May 1, 2018, on two issues:

Somali Remittances: The law required the U.S. Department of Treasury to study if banking regulators should establish a pilot program to provide technical assistance to depository institutions and credit unions that wish to provide account services to money services businesses serving individuals in Somalia. Such a pilot program could be a model for improving the ability of U.S. residents to make legitimate funds transfers through easily monitored channels while preserving strict compliance with BSA.

Sharing State Banking Exams: The law also required Treasury to report on the efficacy of money services businesses being allowed

to share certain State exam information with depository institutions and credit unions to increase their access to the banking system.

Have you or your organization been involved with these Treasury studies?

A.6. I have not been engaged in the Treasury studies. I am in favor of such pilot programs

Q.7. What advice did you give—or would you give—on the pilot studies?

A.7. Somalia is a high risk country for terrorism. That said, the stories of bulk cash being carried to Somalia from the U.S. because MSBs are not banked and NGOs are forced to currier money is extremely problematic. To expand on my answer above about regulatory agencies not taking or demonstrating a leadership role, this would be a great opportunity for that to change. I would recommend Treasury and the regulators take a leadership role in working with financial institutions to bank MSBs in the Somali region and to what extent the depository institutions should have a risk tolerance for. Part of the lack of leadership on the part of the regulators results in a lack of clarity with banks in terms of the level of risk they should take on and the perceived regulatory response to financial institutions considering taking on such risk. This is where leadership and clarity would be helpful in formulating more realistic risk tolerance thresholds and would lead to less derisking.

I like the idea of MSBs being able to share certain State exam information with depository institutions and credit unions. In most instances, it would provide information that should lead to establishing or maintaining a banking relationship.

Q.8. In 2016, William and Margaret Frederick were moving from Ohio to Las Vegas. Unfortunately, it is alleged that the title company they used in Columbus, Ohio, fell for an email scam and wired the $216,000 profit from their home sale to a hacker, not to the Fredericks. William is 83 and Margaret is 75 and as of October, they were still trying to get their money back. While the Fredericks' tale is now a court case to determine who was responsible for the fraudulent information, we know that the Fredericks' experience is "very typical" of scams that divert an estimated $400 million a year from title companies into bogus accounts.

Please describe the responsibilities of financial firms to avoid these frauds?

A.8. These situations are devastating to the victims, especially elderly victims like the Fredericks. I wish there was a simple recourse for the Frederick's but there is not. The financial institutions involved in the transaction do not owe the Fredericks or the title company a fiduciary duty. The financial institution has a responsibility to have a reasonably designed AML program. What that means is the program is reasonably designed to identify and report suspicious activity to FinCEN. Your question does not give much context about the banking relationships involved in this case. The Frederick's recourse should be with the title company who fell for the phishing/email scam. It's likely the escrow company did not

have adequate controls. There are, unfortunately, to many cases like this. They usually wind up in civil law suits.

Depending on the case specifics, it is not likely the bank would be found negligent or responsible. Again, the culpability is likely to lie with the escrow company. The bank would not be responsible for the escrow company's falling victim to the scammers.

Q.9. What penalties should be assessed and by which agencies when financial firms enable theft?

A.9. In the event that the financial institution did not have a reasonably designed AML program to identify suspicious activity, the bank failed to file SARs or to adequately file SARs than the bank should face an enforcement action by their regulators and/or FinCEN. If it was a one off fraud, and the bank had a reasonably designed program it is unlikely they would be held culpable. Invariably, many of these cases wind up with civil law suits filed against the bank. In at least some such cases, the bank will opt to settle the law suit and avoid trial to avert adverse publicity and reputational damage.

Q.10. What is the role for the Consumer Financial Protection Bureau to ensure financial firms protect their customers' money and information?

A.10. The CFPB is intended to help consumers protect their assets from fraud. I'm not sure of the role the CFPB would play in a scenario involving the Fredericks. If the escrow company was negligent and lacked adequate internal controls, they should be held culpable for the loss. I'm not a lawyer so I cannot speak to the legal ramifications. Again, I'm not sure of what the CFPB could or should do.

Q.11. In 2014, FinCEN issued an advisory with human trafficking red flags, to aid financial institutions in detecting and reporting suspicious activity that may be facilitating human trafficking or human smuggling.

To what extent do you assess that financial institutions are currently utilizing these red flags, in order to better assess whether their banks are being used for to finance human trafficking? If institutions are not widely utilizing the red flags, what actions is FinCEN taking to encourage them to do so?

A.11. Human trafficking is a heinous crime problem. I believe that AML professionals are dedicated professionals and are very concerned about human trafficking. I cannot speak definitively as to how widely financial institutions use the FinCEN red flags regarding human trafficking or to the extent FinCEN provides guidance regarding human trafficking. However, I do believe many financial institutions use human trafficking and smuggling red flags from multiple sources. There is other red flag guidance that financial institutions use that comes from FATF, Homeland Security Investigations, the FBI and other viable sources. It should be noted that the Polaris Project has written a great reference guide about human slavery (trafficking), titled "Typologies of Modern Slavery". In addition, human trafficking is widely discussed at industry training conferences. Training is one of the core pillars of an AML

program. Human smuggling typologies and warning signs are frequent topics.

The Association of Certified Anti–Money Laundering Specialists (ACAMS) has made human smuggling a long time priority. They started a working group in 2010 with a group of major banks and Homeland Security Investigations. Bank analysts and Homeland Security Investigations analysts developed patterns of activity or typologies consistent with human smuggling. JPMorgan Chase had a team of special investigators who conducted targeted transaction monitoring and identified potential suspicious activity. ACAMS gave JPMorgan Chase and Homeland Security a special award in recognition of their outstanding collaboration. Another outstanding example of public–private sector partnerships occurred in January 2018, in the run up to the Super Bowl. The ACAMS Minneapolis Chapter held a half-day long learning event focused entirely on human slavery/trafficking. I was proud to be the first speaker. U.S. Bank, Homeland Security Investigations, and the U.S. Attorney's Office in Minneapolis collaborated to develop typologies to identify human sex trafficking specifically related to travel for the Super Bowl. These types of initiatives have a great impact on crime problems like human trafficking. I must give a cautionary comment that this type of initiative is not as easy as it sounds. It can be costly; there are regulatory concerns and other impediments that must be overcome. The September issue of *ACAMS Today* magazine had a detailed article about the Minneapolis learning event. I would be happy to provide a copy of *ACAMS Today* if you'd like one.

Q.12. What are the pros and cons of reducing or eliminating the standards requiring SARs filing for insider abuse (i.e., employee misconduct)?

A.12. I do not believe there are any pros to reducing or eliminating SAR filing for insider abuse. If the insider abuse would be considered suspicious activity, SARs should be filed. Insider abuse can be devastating to financial institutions and should be dealt with harshly. It's one thing if insiders embezzle or defraud their employer. It's another issue when insiders facilitate external fraud schemes. That can be more devastating to the financial institution, as well as to outsiders exposed to the fraud or other crime problem.

Q.13. The common expectation is that any financial institution subjected to a cyberattack would be in touch with law enforcement about whether or not it's required to file an SAR. What are the pros and cons of eliminating SAR filing requirement for cyberattacks against financial institutions?

A.13. As I mentioned responding to an earlier question, I do not see any pros for eliminating SAR filing requirements regarding cyberattacks. There are only cons. That is unless the cyberattack has no financial lead value. I believe that most if not all cyberattacks have a financial component to them. Therefore, it is incumbent that SARs be filed to ensure the financial considerations receive adequate attention from financial experienced investigators. More importantly, FinCEN has a cyberteam that assesses and addresses cyber SARs. I believe that not all cyberthreats, where SARs are generated, are reported to law enforcement other than through

the SAR filing. Also, when cyberthreats are reported to cyber investigators, I'm not sure that the follow up cyber investigation has a financial component as it would if SARs were filed.

Q.14. Gaming and tourism are some of Nevada's top industries. In the State of Nevada, our gaming operators employ thousands of hard working Nevadans, and the industry as a whole domestically supports 1.7 million jobs across 40 States. Qualified casinos, like financial institutions, are also subject to Banking Secrecy Act requirements. Organizations within Nevada have suggested that gaming operators would welcome a review of BSA requirements, which they find to be burdensome. They look forward to this Committee's thoughtful, bipartisan review of BSA requirements that takes into account the security imperative for robust anti–money laundering efforts, as well as the impact those requirements have on all industries. The Suspicious Activity Report (SAR) ($5,000) and the Currency Transaction Report (CTR) ($10,000) levels were set years ago. Some have recommended increasing these to correspond with inflation. Others believe that would be too high but do support a higher amount than currently,

From a law enforcement perspective, are there risks to raising the amounts? Is it possible that having CTRs at higher levels could result in more fraud and terrorist financing? If the amounts were raised, to what amount do you recommend?

A.14. I am a firm believer that the SAR and CTR thresholds should not be raised. This would be detrimental to law enforcement, especially considering the threat of homegrown violent extremists. Homegrown violent extremists would be more likely to transact in amounts below the $5,000 and $10,000 threshold levels. As the Chief of the Financial Crimes Section and founder of the Terrorist Financing Operations Section (TFOS) at the FBI, I was the direct beneficiary of SAR and CTR data. I saw firsthand how information below the threshold levels was used in investigations. I believe in 2004 or 2005, my successor as Chief of TFOS, Michael Morehart, testified about not raising the thresholds before a Congressional Committee. Subsequent to that, GAO conducted a review of the threshold issue and concured that law enforcement benefited from SAR and CTR information at the current thresholds. My apology for not being more specific about the hearing or report date. At this point in time, I do not recall the specifics and in deference to time in completing my response to questions, I was unable to conduct the necessary research.

I also believe that most financial institutions would state that the current thresholds do not cause them any greater work than they would if the thresholds were raised. This topic comes up at industry conferences and financial institution representatives have stated this regularly.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM HEATHER A. LOWE

Q.1. *Information Sharing Among Banks*—While you have generally supported increased information sharing between banks and the U.S. Government, and among banks, you also have sounded an alarm about the importance of appropriate privacy safeguards

around bank–bank information sharing, particularly where an individual's access to financial services may be at risk if negative but inaccurate information on them gets into the system, as with inaccurate credit reporting.

Can you describe the types of safeguards you think would be important if we were to consider clarifying or expanding this authority? In particular, should we consider implementing a system of redress or information correction for such individuals, and if so how would you configure such new protections, and how would you envision that process actually working?

A.1. The general rule around information sharing among banks should be that data is anonymized before being shared. This is consistent with the Clearing House's recommendations. Instances where an individual's personal and/or account information can be shared among banks should be very clearly circumscribed. A system of redress should be established for individuals to review and rectify incorrect information that may be forming the basis of banks' decisions to deny an individual banking services, as is the case with credit information.

When the banks ask for permission to share information, they are asking for that permission not just among banks in the U.S., but globally. As such, rules circumscribing the sharing of individuals' personal and account information and processes for redress should be crafted in conjunction with other major financial centers. FinCEN (the U.S.'s financial intelligence center) could initiate and lead this process through its membership in the Egmont Group, the umbrella organization for more than 135 financial intelligence centers around the world.

Q.2. *Bank Derisking/Remittances*—Your testimony emphasized the importance of Know Your Customer procedures for banks. But in recent years many financial institutions have opted to shed accounts of customers with personal or commercial links to parts of the world where it can be difficult to ascertain the final recipient of a financial transaction—an especially important concern to Somali communities in Ohio, for example. Whether we are talking about family remittances, or funds transfers for humanitarian purposes, this derisking has presented hurdles to effort to get resources to some of the most at-risk populations on Earth. And customers who lose accounts or are unable to move money through the regulated financial system are often forced to use less transparent, safe and regulated channels, undermining AML/CFT goals. The Financial Action Task Force (FATF) has recently suggested making inappropriate derisking a priority.

From your perspective, what steps can be taken as part of BSA modernization to address the derisking problem and provide relief to both banks and their customers? How specifically can we better balance KYC obligations with the need to facilitate the flow of remittances, and the legitimate work of charities and humanitarian organizations, abroad?

A.2. My organization focuses on the movement of illicit money out of developing countries the effect of that financial flow for development, and not financial flows into developing countries, so we have not focused a great deal on the remittances and nonprofit issues.

Nonprofit organizations like the Charity and Security Network, Oxfam, and the Center for Global Development, and intergovernmental organizations such as the World Bank, the IMF, the OECD and others have been doing a great deal more research in this area and I would recommend speaking with them for more developed and far-reaching recommendations.

Having said that, there are three somewhat different problems in the derisking area with root causes that are not all AML-related, and I think that is a really important point here. One is that banks that are no longer willing to provide banking services to money service businesses (MSBs) that are the primary movers of remittances. Second is banks choosing not to do business with correspondent banks in certain very high-risk countries. (The Somali remittance problems are a combination of both these first and second categories.) Third, is the problem of banks choosing not to provide banking services for charities/nonprofits. These are related issues, but not the same issues. Something to bear in mind as well is that the World Bank has found that the cost of transmitting remittances has actually decreased over the past several years, suggesting that some of the problems in the sector may really be location specific, such as with Somalia, as opposed to being as widespread as discussion on this topic might suggest.

In 2012 and the following 2 years, FATF Recommendations and related guidance were published relating to risks posed by nonprofits and risks posed by MSBs. That guidance suggested that those entire sectors were particularly vulnerable to money laundering with no nuance, which resulted in banks categorizing them all as high risk, regardless of the nature of those businesses, the strength of their compliance programs, their clientele, or other risk assessment factors. The general refrain from banks was that it was too costly to do proper AML vetting on all these "high risk" entities. Banks also said they were pulling out of high risk areas because of an increase in fines and penalties, but very few fines/penalties have been levied related to servicing MSB or nonprofit clients, which begs the question of whether this reaction was simply disproportionate or driven by other motives, such as an excuse to get out of these relatively low-margin lines of business.

For example, Barclays in the U.K. caused a bit of a crisis when it closed the accounts of the vast majority of the money service businesses it serviced. But it held on to MSBs with assets of $10m or more. However, the significant MSB money laundering case on record actually relates to Western Union, one of the world's largest and well-capitalized MSBs. Barclays' decision to jettison smaller MSB accounts was made not in relation to actual enforcement trends, how good their MSB clients' compliance programs were, or other risks relating to the individual MSB's business or other relevant factors, it was made on whether the bank wanted to keep that capitalization or not and bother to continue servicing smaller accounts where its margin was smaller and getting smaller because of compliance costs. It would be interesting to find out pre-2012 margins on these business lines versus post-2012 margins so that Congress has a frame of reference for what a bank consider an unacceptable margin in these business lines.

And that raises an important point in all of this that is very often missed. There has been huge bank consolidation leading to behemoth banks that do not consider providing services to smaller account holders to be worth the cost. (In our experience, smaller, local banks rarely provide adequate international transfer services and did not do so prior to AML regulation.) We see that every day as banking fees for people who have little savings climb while those who have sizable accounts have no fees at all. Banks are doing everything they can to increase their profit margins with little regard to the effect on the average account holder. That's today's business model, and bank decisions regarding MSB and nonprofit account holders are driven in large part by this model. Furthermore, the Center for Global Development put out a report on derisking in 2015. In that report, they noted that some banks have "derisked" and then beefed up their own money transmitter services, suggesting a possible move to undermine competition and seize the market themselves.

So there are problems, some of which are not actually AML related, but the following are some measures that can be taken in the AML sphere to help in this area:

- Better nuanced Recommendations and guidance from FATF and regulators is needed.
  - In October 2014, FATF spoke out against blanket derisking and said that FIs should derisk only on a case by case basis. FinCEN, the FDIC, and the OCC followed that up asking banks to come to the regulators if they felt pressure to terminate an MSB relationship. Other regulators have followed.
  - Unfortunately it seems that there is no hard data to be able to measure what has happened in the market since.
  - After an outcry from the global nonprofit community, FATF revised its guidance with respect to the problematic Recommendation 8, but I think it still needs further revision and U.S. Treasury could use its influence to make that happen. Please contact Kay Guinane at the Charity and Security Network for further information (kguinane@charityandsecurity.org).
- Banks should have access to information from FinCEN about whether an MSB has been the subject of formal warnings/cease and desists which are not public information, so that they can better judge the strength of an MSB's compliance program and its weaknesses.
- Create a low-cost certification scheme for smaller MSBs. Such a scheme would create benchmarks for MSB compliance programs, similar to what has been done in the development of an ISO standard for anticorruption compliance. This could perhaps be subsidized by a fund the big banks pay into for the smaller MSBs.
- One element of compliance cost is identifying the true owners and controllers of MSBs and charities, as well as the remitters themselves. Transparency about who owns and controls companies would be a real help with that.

- National ID schemes for individuals around the world are also important. India leading the way in effectively doing this in rural populations living in poverty—the hardest to reach and often recipients of remittances. While it may seem to be outside of Congress' remit, USAID has financially supported these initiatives in the past and Congress could prioritize funding to USAID to continue and/or increase this work.

Q.3. *Scope of AML Reporting*—In recent House testimony, you noted that AML compliance and reporting is undertaken by a wide range of entities and persons beyond the banking sector. You also made clear that there are entities and persons not currently regulated or required to have AML programs in place, that really ought to if the system is to be comprehensive.

Can you give us a sense of the scope of entities and persons you think we ought to have in mind, beyond the banking sector, when contemplating an update to our current anti–money laundering framework and its underlying authorities?

A.3. FATF has identified several of what it calls Designated Non-Financial Businesses and Professions, or DNFPB's, as businesses and professions that are susceptible for, or can be used to play a part in, money laundering. The idea is that these businesses and professions should identify who they are doing business with, in some cases carry out some customer due diligence, and file suspicious activity reports if they think a transaction is suspicious.

The U.S. already requires some DNFBPs to have those AML programs, such as casinos and dealers in precious metals and stones. Treasury regulations originally also included others, including travel agents, those involved in real estate closings, and car, plane, and boat dealers, among others, but then Treasury gave them a "temporary" exemption from the requirements with no sunset for that exemption which has now been in place for many years. Still others never made it on any list, and those four are lawyers, accountants, corporate service providers, and escrow agents. For these four, AML programs would really be about knowing with whom you are doing business and not permitting practitioners in these businesses and professions to be able to have plausible deniability that they didn't have reason to know or suspect that they were providing services that might be laundering dirty money.

While there are clearly several businesses and professions missing from U.S. regulation, I would focus on five of them: lawyers, those involved in real estate closings, corporate service providers, escrow agents, and accountants.

Lawyers: Of course criminals need and use legal services. A *60 Minutes* piece that aired last year featured undercover footage from an organization called Global Witness, showing just how easy it is to walk into a law firm in New York and get a lawyer to easily suggest ways in which structures could be created to spend money that is clearly the proceeds of corruption to buy real estate, planes, etc. One attorney even suggested running the dirty money through the lawyer's client account to clean it. It was a real eye-opener. In 2010, the American Bar Association published what I would characterize as sound *Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing*,

but I encourage you to ask every lawyer you know if they have implemented it. It is unlikely that they have even heard of it. This voluntary guidance is simply not enough.

Escrow Agents: Senate Permanent Subcommittee on Investigations' 2010 report *Keeping Foreign Corruption Out of the United States: Four Case Histories* tells the story of how one escrow agent, McAfee & Taft, refused to provide escrow services to Teodorin Obiang, the corrupt, playboy son of the long time dictator of the impoverished Nation of Equatorial Guinea, because the anti–money laundering policy they had voluntarily put in place prescribed that they do so. Another escrow agent without an AML program happily took that money.

Corporate Service Providers: The Panama Papers showed just how entangled corporate service providers like Mossack Fonseca can be in facilitating money laundering, corruption, and tax evasion. The book *Global Shell Games* details research by a team of American and Australian academics into just how easy it is to create an anonymous company to engage in terror finance or corruption in different countries around the world through corporate service providers. They found that the easiest country in which to do so was the United States. One email response to the researchers' inquiry from a corporate service provider in Florida was, "[Y]our started purpose could well be a front for funding terrorism, and who the f—— would get involved in that? Seriously, 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 that 5k a month, and I doubt you are going to find any suckers that will do it for less, if at all. If you are working with less than serious money, don't waste anybody's time here. Using a f——— google account also shows you are just a f——— poser and loser. If you have a serious proposal, write it up and we will consider it. Your previous message and this one are meaningless crap. Get a clue. Just how stupid do you think we are?"

Those Involved in Real Estate: With respect to real estate, since July 2016, FinCEN has had geographic targeting orders in place in various counties in New York, Florida, Texas, and California, requiring title insurance companies to collect beneficial ownership information for those entities buying high value real estate with cash. They found that about 30 percent of the beneficial owners identified by the title companies already had SARs filed on them by other financial institutions. That's nearly one third. Exposés like *The New York Times*' "Towers of Secrecy" show just how easy it is for people to hide behind anonymous companies and buy real estate with proceeds of crime and corruption. It is central to the 2017 indictment of Paul Manafort and Richard Gates as well.

Q.4. *Cryptocurrencies*—As the use of cryptocurrencies continues to evolve and to spread, questions have been raised about the abuse of such virtual currency for money laundering and other illicit purposes.

Can you please comment on the current exploitation of virtual currency for illicit finance purposes, as well as the potential for blockchain technology to short-circuit our current AML regulatory

and enforcement frameworks? In your opinion, what tools should the U.S. Government be developing, now, to head off this threat?

A.4. I am not sufficiently informed to provide a detailed response to this question, but recommend that you contact the following people to develop a greater understanding of the threats and opportunities posed by both cryptocurrencies (referred to as "virtual currencies" in international regulatory parlance) and the blockchain technology that underpins them, but also has much wider applications.

Yaya Fanusie, Director of Analysis, Center on Sanctions and Illicit Finance (yaya@defenddemocracy.org); Tom Robinson, COO and Cofounder, Elliptic (tom@elliptic.co); Jamie Smith, Global Chief Communications Officer, The Bitfury Group (jamie.smith@bitfury.com).

RESPONSES TO WRITTEN QUESTIONS OF SENATOR SASSE FROM HEATHER A. LOWE

Q.1. This hearing discussed the importance of increasing information sharing between financial institutions and with law enforcement officials.

What—if any—are the privacy risks with facilitating the sharing of such information?

What are the best ways to mitigate such privacy concerns?

Increased information sharing between financial institutions could make it easier for individuals to be completely cut out of the United States' financial system. How should wrongly targeted individuals be able to challenge their designation?

What should our risk tolerance be for the fact that the U.S. financial system facilitates crimes like human trafficking? Should we strive to have zero incidence of money laundering in our financial system?

A.1. There are three types of privacy risks that I would identify here—the information security risk, the risk of personal information being sold or otherwise transmitted by financial institutions for reasons other than communicating risk of criminal activity, and the "cut out" risk. I do not have the right expertise to effectively address the information security risk, and recommend that you speak with cybersecurity experts focusing on the financial sector and to FinCEN/law enforcement regarding their cybersecurity protections (and protections on the BSA database), as those will be the two types of entities between which this information would be passed and collected.

Regarding the risk of information being sold or otherwise transmitted for purposes other than detection of criminal activity, the laws and regulations around what type of information can be transmitted, to whom, and how and how long it should be retained should be very clearly defined in legislation/regulation.

The risk that someone could be incorrectly identified as a bad actor and cut out of the global financial system is certainly a risk here. It is a common complaint associated with being added to the OFAC's Specially Designated Nationals and Blocked Persons (SDN) list. Another complaint about the SDN list is that sometimes people do not know why they have been placed on the SDN list and

there is no procedure for challenging the designation. In that case, there is one body making those designations. In a world of financial institution information sharing, those decisions would be just as opaque, could have been made by any financial institution, and there is even less redress because a financial institution is never under an obligation to open an account for someone.

Ultimately, we are also talking about information sharing that is global and repercussions that are global, so I don't think the U.S. will be able to create a redress system alone. I think a redress system would probably need to involve FinCEN, however, because of the confidential nature of the information involved. FinCEN is the U.S.'s Financial Intelligence Unit, or FIU. Most other countries with any sort of AML monitoring that might end up denying someone access also have an FIU. Those FIUs are, with some exceptions, members of a body called the Egmont group, which has rules and methods for information sharing among Egmont FIUs. There are over 135 FIU members of Egmont at present. The U.S. could spearhead the creation of a redress process in this area that involved the Egmont FIUs, or a review panel housed within that secretariat the was, perhaps, funded by bank contribution.

In terms of expectations with respect to money laundering, at my organization, Global Financial Integrity, we always speak in terms of curtailing the problem. We understand that it can never be entirely prevented. However, I caution against using terms like "tolerance." There is no acceptable level of known money laundering that should be tolerated. We need to have reasonable expectations with respect to how much money laundering can be detected by financial institutions that have well-crafted and executed AML compliance programs in place, and we need reasonable expectations as to what a well-crafted and executed AML program is. Congress is currently in the dark with respect to independently verifiable information about the nonpublic citations financial institutions are currently receiving for compliance program failures and whether they are reasonable. Congress has only the complaints of industry representatives themselves, many of whom resent AML compliance and reporting requirements writ large and have every incentive to overstate the problem. The massive fines levied on banks in recent years have been the result of knowing, willful, and egregious violations of laws and regulations in the AML area in order to turn a blind eye to money laundering their clearly knew about in order to increase profits. There should be zero tolerance for that.

Q.2. I'd like to understand better how technological innovation is transforming the fight against money laundering and how Government policy can help or hurt these efforts.

In the health care context, I hear about how researchers have used machine learning and artificial intelligence to identify diseases and predict when they will occur, using data points that humans would have never put together. How have financial institutions or law enforcement officials been able to use of similar techniques to identify money laundering and how much more progress can be made in this front?

Outside of AI and machine learning, how can recent FinTech innovations such as blockchain fight money laundering?

What regulatory requirement or requirements—if any—most hinders the adoption of technological innovations?

How much does bitcoin, blockchain, and other cryptocurrencies facilitate money laundering? How—if at all—should this impact our approach to combating money laundering in traditional banks? How can law enforcement officials best stop this newer form of money laundering?

A.2. With respect to the first bulleted question, there is a very wide world of financial analytics in use to identify money laundering and expertise to create the algorithms used in these processes. I am not an expert in analytics, unfortunately, but there is an entire industry of people who can provide a helpful response to this question, although they may not be able to answer this broad of a question in written form.

With respect to the remaining bullet points, the most significant block to adopting new technologies is, I believe, a concern that regulators will not recognize the use of a new technology as a positive development in examinations. I therefore support the creation of a technological "sandbox", as has been proposed by The Clearing House and has been implemented in the U.K. It is important to note that the U.K. structure appears to have some specific safeguards to protect consumers which they consider to be an integral part of their system. U.K. regulators presented their approach at a recent FATF industry consultation meeting I attended. They stressed the importance of ensuring that consumers were protected at all times as innovative approaches were being tested, and the U.S. should do the same. In the House of Representatives, Members are discussing legislative language that does not require any of the safeguards present in the U.K. system, potentially giving financial institutions an unlimited safe harbor for the use of any new technology with no Government oversight. This is a significant danger because if a financial institution spends the money to integrate new technology that, it turns out, isn't as effective as alternative methods, they would have no incentive to change their approach. They would incur some unwelcome cost for doing so and they'd have the security of an unlimited safe harbor, so there would be no incentive to act.

Connecting this in with blockchain technology, there is certainly work being done in this area. You may wish to reach out to Tom Robinson, COO and Cofounder, Elliptic (tom@elliptic.co). Elliptic is a company that finds ways to identify the "anonymous" digital currency traders to help with customer due diligence problems associated with digital currencies.

Mr. Robinson recently coauthored a paper entitled "Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services" with the Foundation for Defense of Democracy's Yaya Fanusie, a long-time expert on illicit and terror finance who has been researching the linkages between terror finance and digital currency. I would recommend reaching out to Mr. Fanusie to further explore this area. Yaya Fanusie, Director of Analysis, Center on Sanctions and Illicit Finance (yaya@defenddemocracy.org).

Q.3. I'd like to discuss Suspicious Activity Reports (SARs). Today, around 2 million SARs are filed each year. While every SAR used

to be read by law enforcement officials, that is no longer the case today. Financial institutions often complain that they rarely, if ever, receive feedback from law enforcement officials on the utility of any particular suspicious activity report that they file. This lack of feedback loops increases the burdens on financial institutions, who continue to file SARs that are of little utility to law enforcement officials. It also prevents financial institutions from developing better analytical tools to more precisely discern between the signal and the noise.

What percentage of SARs are actually read by someone in law enforcement?

A.3. I am not aware of credible estimates. This question will need to be answered by FinCEN.

Q.4. How often do financial institutions receive feedback from law enforcement officials as to the utility of their SAR filing?

A.4. Such feedback is rare. While law enforcement cannot and should not share information about an ongoing investigation, at the very least they could be collecting statistics about the number of SARs/CTRs from a given financial institution that they followed up on in some way. Where a SAR from a financial institution (or many SARs from several institutions, which is more likely) helped law enforcement bring a strong case, it could be worthwhile to positively identify the banks that helped the case in this way once the case is resolved. Positive reinforcement is important. I once highlighted a seminal case regarding tax evasion and money laundering at an international AML conference in Florida. A very excited compliance officer from the U.S. Virgin Islands approached me after presentation—she had been the person to file the SAR that resulted in the case and she had never known what had happened to it. She was thrilled that her actions had made a difference, and remembered the SAR because the activity seemed so odd to her at the time. I believe that we would have a much more robust AML defense system in the U.S. if more bankers and compliance officers were given such opportunities to feel like their actions really made a difference. Therefore, I am in favor of initiatives like FinCEN Exchange, announced in December, to enhance information sharing with Financial Institutions. However FinCEN needs to make this a meaningful program in its execution if it is to have any impact.

Q.5. While some have proposed reducing the number of SARs and CRT filings because they are often superfluous and are never read, others argue that this poses risks, because investigating minor infractions may still lead to significant law enforcement successes. How should policymakers resolve this conflict?

A.5. The driving force behind this complaint from industry is the amount of resources spent on drafting SARs, including preparatory investigation time. CTR filings are automatically generated when more than $10,000 is deposited, so should be discussed separately if there really are valid concerns there. One source of tension in this area appears to be that law enforcement wants SARs to include as much information as possible, in as standard a format as possible, and that their demands for greater detail and specificity have grown over time. This has obviously developed over time as law enforcement has identified what information is most useful to

them and the presentation that is most useful—specificity that the financial institutions have actually asked for over time. However, financial institution employees may not have the desired level of detail that law enforcement would like—that is simply a reality of money laundering cases which often involve hidden conduct and individuals. The SAR instructions properly allow filers to indicate on the form that the information is "unknown"; that option should be honored by law enforcement rather than trying to require bank employees to become detectives uncovering illegal conduct.

Q.6. How could regulators (1) set up better feedback loops between financial institutions and law enforcement officials that could help financial institutions better identify money laundering; and (2) empower financial institutions to act upon their improved ability to distinguish between useful and superfluous reports, including by filing fewer unnecessary SARs, without fearing regulatory consequences for doing so?

A.6. I believe my answer is subsumed in the responses above.

Q.7. Would a better feedback loop system exist if financial institutions employed more people with security clearances? If so, what, if anything, can the Federal Government do to facilitate this?

A.7. I do not have an opinion on this question.

Q.8. Often, financial institutions will derisk by refusing to serve customers that could be involved in illegal activity. As financial institutions start to share more information with each other, this practice could become more prominent and potential criminals could more frequently lose access to the United States' financial system altogether.

Are there instances in which derisking is actually unhelpful for law enforcement purposes, because it drives these criminals underground and makes it more difficult to track them?

At the moment, do the regulators that evaluate and enforce financial institutions compliance with our Federal money laundering take this into account?

Are there promising ways to increase cooperation between financial institutions, regulators, and law enforcement officials, so that financial institutions can make a more informed decision about when and how to derisk?

Would financial institutions need to hire more employees with a top security clearance and/or a law enforcement background for this coordination to be effective?

A.8. My organization focuses on the movement of illicit money out of developing countries the effect of that financial flow for development, and not financial flows into developing countries, so we have not focused a great deal on the remittances and nonprofit issues. Nonprofit organizations like the Charity and Security Network, Oxfam, and the Center for Global Development, and intergovernmental organizations such as the World Bank, the IMF, the OECD and others have been doing a great deal more research in this area and I would recommend speaking with them for more developed and far-reaching recommendations.

Having said that, there are three somewhat different problems in the derisking area with root causes that are not all AML-related,

and I think that is a really important point here. One is that banks that are no longer willing to provide banking services to money service businesses (MSBs) that are the primary movers of remittances. Second is banks choosing not to do business with correspondent banks in certain very high-risk countries. (The Somali remittance problems are a combination of both these first and second categories.) Third, is the problem of banks choosing not to provide banking services for charities/nonprofits. These are related issues, but not the same issues. Something to bear in mind as well is that the World Bank has found that the cost of transmitting remittances has actually decreased over the past several years, suggesting that some of the problems in the sector may really be location specific, such as with Somalia, as opposed to being as widespread as discussion on this topic might suggest.

In 2012 and the following 2 years, FATF Recommendations and related guidance were published relating to risks posed by nonprofits and risks posed by MSBs. That guidance suggested that those entire sectors were particularly vulnerable to money laundering with no nuance, which resulted in banks categorizing them all as high risk, regardless of the nature of those businesses, the strength of their compliance programs, their clientele, or other risk assessment factors. The general refrain from banks was that it was too costly to do proper AML vetting on all these "high risk" entities. Banks also said they were pulling out of high risk areas because of an increase in fines and penalties, but very few fines/penalties have been levied related to servicing MSB or nonprofit clients, which begs the question of whether this reaction was simply disproportionate or driven by other motives, such as an excuse to get out of these relatively low-margin lines of business.

For example, Barclays in the U.K. caused a bit of a crisis when it closed the accounts of the vast majority of the money service businesses it serviced. But it held on to MSBs with assets of $10m or more. However, the significant MSB money laundering case on record actually relates to Western Union, one of the world's largest and well-capitalized MSBs. Barclays' decision to jettison smaller MSB accounts was made not in relation to actual enforcement trends, how good their MSB clients' compliance programs were, or other risks relating to the individual MSB's business or other relevant factors, it was made on whether the bank wanted to keep that capitalization or not and bother to continue servicing smaller accounts where its margin was smaller and getting smaller because of compliance costs. It would be interesting to find out pre-2012 margins on these business lines versus post-2012 margins so that Congress has a frame of reference for what a bank consider an unacceptable margin in these business lines.

And that raises an important point in all of this that is very often missed. There has been huge bank consolidation leading to behemoth banks that do not consider providing services to smaller account holders to be worth the cost. (In our experience, smaller, local banks rarely provide adequate international transfer services and did not do so prior to AML regulation.) We see that every day as banking fees for people who have little savings climb while those who have sizable accounts have no fees at all. Banks are doing everything they can to increase their profit margins with little regard

to the effect on the average account holder. That's today's business model, and bank decisions regarding MSB and nonprofit account holders are driven in large part by this model. Furthermore, the Center for Global Development put out a report on derisking in 2015. In that report, they noted that some banks have "derisked" and then beefed up their own money transmitter services, suggesting a possible move to undermine competition and seize the market themselves.

So there are problems, some of which are not actually AML related, but the following are some measures that can be taken in the AML sphere to help in this area:

- Better nuanced Recommendations and guidance from FATF and regulators is needed.
  - In October 2014, FATF spoke out against blanket derisking and said that FIs should derisk only on a case by case basis. FinCEN, the FDIC, and the OCC followed that up asking banks to come to the regulators if they felt pressure to terminate an MSB relationship. Other regulators have followed.
  - Unfortunately it seems that there is no hard data to be able to measure what has happened in the market since.
  - After an outcry from the global nonprofit community, FATF revised its guidance with respect to the problematic Recommendation 8, but I think it still needs further revision and U.S. Treasury could use its influence to make that happen. Please contact Kay Guinane at the Charity and Security Network for further information (kguinane@charityandsecurity.org).
- Banks should have access to information from FinCEN about whether an MSB has been the subject of formal warnings/cease and desists which are not public information, so that they can better judge the strength of an MSB's compliance program and its weaknesses.
- Create a low-cost certification scheme for smaller MSBs. Such a scheme would create benchmarks for MSB compliance programs, similar to what has been done in the development of an ISO standard for anticorruption compliance. This could perhaps be subsidized by a fund the big banks pay into for the smaller MSBs.
- One element of compliance cost is identifying the true owners and controllers of MSBs and charities, as well as the remitters themselves. Transparency about who owns and controls companies would be a real help with that.
- National ID schemes for individuals around the world are also important. India leading the way in effectively doing this in rural populations living in poverty—the hardest to reach and often recipients of remittances. While it may seem to be outside of Congress' remit, USAID has financially supported these initiatives in the past and Congress could prioritize funding to USAID to continue and/or increase this work.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR TILLIS FROM HEATHER A. LOWE

Q.1. How can we leverage technology to make the process simultaneously less onerous on banks while enhancing the outcomes of catching illegal behavior? Are there regulatory and legislative barriers to getting that down?

Financial institutions often complain that FinCEN, law enforcement officials, and prudential regulators do not tell them whether their BSA filings serve a useful purpose, or how the reports they submit are being used—and that the filings go into a black hole. Can you shed some light on the filings that you make or have used and what could be done to improve this process?

A.1. While law enforcement cannot and should not share information about an ongoing investigation, at the very least they could be collecting statistics about the number of SARs/CTRs from a given financial institution that they followed up on in some way. Where a SAR from a financial institution (or many SARs from several institutions, which is more likely) helped law enforcement bring a strong case, it could be worthwhile to positively identify the banks that helped the case in this way once the case is resolved. Positive reinforcement is important. I once highlighted a seminal case regarding tax evasion and money laundering at an international AML conference in Florida. A very excited compliance officer from the U.S. Virgin Islands approached me after presentation—she had been the person to file the SAR that resulted in the case and she had never known what had happened to it. She was thrilled that her actions had made a difference, and remembered the SAR because the activity seemed so odd to her at the time. I believe that we would have a much more robust AML defense system in the U.S. if more bankers and compliance officers were given such opportunities to feel like their actions really made a difference. Therefore, I am in favor of initiatives like FinCEN Exchange, announced in December, to enhance information sharing with Financial Institutions. However FinCEN needs to make this a meaningful program in its execution if it is to have any impact.

Q.2. Another compliance challenge often cited by banks is that they feel pressured by bank examiners and law enforcement authorities to exit certain business lines or cease offering certain services to customers viewed as presenting particular money-laundering vulnerabilities, i.e., severing corresponding banking relationships with foreign institutions in certain geographic areas, and also ending money services businesses (MSBs, i.e., check cashing, money transmitters, currency exchange outlets, etc.)

As banks reevaluate their business relationships with MSBs in light of what they may view as a hostile regulatory landscape, what can we do to change this type of behavior/is this a prevalent problem in the industry?

A.2. My organization focuses on the movement of illicit money out of developing countries the effect of that financial flow for development, and not financial flows into developing countries, so we have not focused a great deal on the remittances and nonprofit issues. Nonprofit organizations like the Charity and Security Network, Oxfam, and the Center for Global Development, and intergovern-

mental organizations such as the World Bank, the IMF, the OECD and others have been doing a great deal more research in this area and I would recommend speaking with them for more developed and far-reaching recommendations.

Having said that, there are three somewhat different problems in the derisking area with root causes that are not all AML-related, and I think that is a really important point here. One is that banks that are no longer willing to provide banking services to money service businesses (MSBs) that are the primary movers of remittances. Second is banks choosing not to do business with correspondent banks in certain very high-risk countries. (The Somali remittance problems are a combination of both these first and second categories.) Third, is the problem of banks choosing not to provide banking services for charities/nonprofits. These are related issues, but not the same issues. Something to bear in mind as well is that the World Bank has found that the cost of transmitting remittances has actually decreased over the past several years, suggesting that some of the problems in the sector may really be location specific, such as with Somalia, as opposed to being as widespread as discussion on this topic might suggest.

In 2012 and the following 2 years, FATF Recommendations and related guidance were published relating to risks posed by nonprofits and risks posed by MSBs. That guidance suggested that those entire sectors were particularly vulnerable to money laundering with no nuance, which resulted in banks categorizing them all as high risk, regardless of the nature of those businesses, the strength of their compliance programs, their clientele, or other risk assessment factors. The general refrain from banks was that it was too costly to do proper AML vetting on all these "high risk" entities. Banks also said they were pulling out of high risk areas because of an increase in fines and penalties, but very few fines/penalties have been levied related to servicing MSB or nonprofit clients, which begs the question of whether this reaction was simply disproportionate or driven by other motives, such as an excuse to get out of these relatively low-margin lines of business.

For example, Barclays in the U.K. caused a bit of a crisis when it closed the accounts of the vast majority of the money service businesses it serviced. But it held on to MSBs with assets of $10m or more. However, the significant MSB money laundering case on record actually relates to Western Union, one of the world's largest and well-capitalized MSBs. Barclays' decision to jettison smaller MSB accounts was made not in relation to actual enforcement trends, how good their MSB clients' compliance programs were, or other risks relating to the individual MSB's business or other relevant factors, it was made on whether the bank wanted to keep that capitalization or not and bother to continue servicing smaller accounts where its margin was smaller and getting smaller because of compliance costs. It would be interesting to find out pre-2012 margins on these business lines versus post-2012 margins so that Congress has a frame of reference for what a bank consider an unacceptable margin in these business lines.

And that raises an important point in all of this that is very often missed. There has been huge bank consolidation leading to behemoth banks that do not consider providing services to smaller

account holders to be worth the cost. (In our experience, smaller, local banks rarely provide adequate international transfer services and did not do so prior to AML regulation.) We see that every day as banking fees for people who have little savings climb while those who have sizable accounts have no fees at all. Banks are doing everything they can to increase their profit margins with little regard to the effect on the average account holder. That's today's business model, and bank decisions regarding MSB and nonprofit account holders are driven in large part by this model. Furthermore, the Center for Global Development put out a report on derisking in 2015. In that report, they noted that some banks have "derisked" and then beefed up their own money transmitter services, suggesting a possible move to undermine competition and seize the market themselves.

So there are problems, some of which are not actually AML related, but the following are some measures that can be taken in the AML sphere to help in this area:

- Better nuanced Recommendations and guidance from FATF and regulators is needed.
  - In October 2014, FATF spoke out against blanket derisking and said that FIs should derisk only on a case by case basis. FinCEN, the FDIC, and the OCC followed that up asking banks to come to the regulators if they felt pressure to terminate an MSB relationship. Other regulators have followed.
  - Unfortunately it seems that there is no hard data to be able to measure what has happened in the market since.
  - After an outcry from the global nonprofit community, FATF revised its guidance with respect to the problematic Recommendation 8, but I think it still needs further revision and U.S. Treasury could use its influence to make that happen. Please contact Kay Guinane at the Charity and Security Network for further information (kguinane@charityandsecurity.org).
- Banks should have access to information from FinCEN about whether an MSB has been the subject of formal warnings/cease and desists which are not public information, so that they can better judge the strength of an MSB's compliance program and its weaknesses.
- Create a low-cost certification scheme for smaller MSBs. Such a scheme would create benchmarks for MSB compliance programs, similar to what has been done in the development of an ISO standard for anticorruption compliance. This could perhaps be subsidized by a fund the big banks pay into for the smaller MSBs.
- One element of compliance cost is identifying the true owners and controllers of MSBs and charities, as well as the remitters themselves. Transparency about who owns and controls companies would be a real help with that.
- National ID schemes for individuals around the world are also important. India leading the way in effectively doing this in rural populations living in poverty—the hardest to reach and often recipients of remittances. While it may seem to be out-

side of Congress' remit, USAID has financially supported these initiatives in the past and Congress could prioritize funding to USAID to continue and/or increase this work.

Q.3. It is my understanding that there are times when law enforcement and the bank regulators work at cross purposes. That is, law enforcement might want a bank to continue banking an individual or company that they are following and building a case against but the bank regulators, whose incentives are to not be embarrassed by their regulated entities, force the banks to "derisk" or close those accounts. Is that actually the case?

A.3. There is no reputational risk associated with continuing to bank a customer when instructed to do so by law enforcement. A bank will not be sanctioned by examiners for doing so. The information will not be made public. This seems a spurious complaint if it is being made by industry.

Q.4. In terms of AML, we know that the success of AML is centric around whether or not the predicate crime of money laundering has been reduced, but we only really know how pervasive money laundering is on a reactive basis, i.e., when someone/some entity is caught.

To that end, do you believe the advent/popularity of cryptocurrencies could affect the capture of money laundering/could it affect AML? Do enforcement authorities have the technological capabilities to work with private industry to capture mal-actors?

A.4. *NOTE:* Your introduction suggests some confusion with respect to money laundering (i.e., reference to "whether or not the predicate crime of money laundering has been reduced"). It is critical to understand that money laundering is a crime in and of itself and is not a predicate offense. The crime is thought by many to be the crime of laundering/disguising/accepting the funds of some underlying crime that generated money, otherwise known as a predicate offense or, in U.S. statutory terms, a specified unlawful activity (SUA). That is correct, but it is not complete. A person can be convicted of money laundering if they believed they were accepting/disguising the proceeds of an SUA and took steps to do so. That means that even if nobody has been convicted of the underlying crime that is the SUA, a person can be convicted of laundering the related funds. However, in almost every "money laundering" case you have heard of, the banks were not charged with actual criminal money laundering. They were charged with violations of provisions of the Bank Secrecy Act requiring financial institutions to have in place measures to detect when someone is trying to use the institution to launder money and preventative measures that detect if anyone inside the institution is allowing money to be laundered by the institution.

The advent and popularity of digital currencies are an emerging threat in the money laundering field because much of our AML policies depend on a financial institution carrying out "due diligence" and "know your customer" checks. That is why accounts opened by companies with hidden beneficial ownership are such a problem. One of the biggest challenges with digital currencies is also the fact that the transactions are essentially conducted anonymously. For more information, I recommend that you contact Tom

Robinson, COO and Cofounder, Elliptic (tom@elliptic.co). Elliptic is a company that finds ways to identify the "anonymous" digital currency traders to help with customer due diligence problems associated with digital currencies.

Mr. Robinson recently coauthored a paper entitled "Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services" with the Foundation for Defense of Democracy's Yaya Fanusie, a long-time expert on illicit and terror finance who has been researching the linkages between terror finance and digital currency. I would recommend reaching out to Mr. Fanusie to further explore this area. Yaya Fanusie, Director of Analysis, Center on Sanctions and Illicit Finance (yaya@defenddemocracy.org).

Q.5. In your opinion, do you think that the overall AML regime has been effective? Additionally, what do you see as the best way to ensure future effectiveness?

Is it to have Treasury be the lead to:

1. Define with other stakeholders specific and clear national priorities of the regime; and

2. Determine, working with other stakeholders, clear and measurable objectives of the regime in light of those priorities. Should Treasury or someone else have to report those measurements against the objectives back to Congress?

A.5. My organization has estimated that just 11 types of transnational crime generate a total proceeds of between $1.6 and $2.2 trillion annually. There are many, many more types of crime that generate proceeds in this world. Most of that money must be laundered in some way. As noted above, there is very little prosecution for large-scale criminal money laundering, even when it seems from charging documents that criminal money laundering (which includes an intent standard) was taking place. In addition, individuals are not being prosecuted and jailed for their actions in the cases that we see, which would be a significant deterrent to money laundering. That may be changing, however, as I note in a recent piece that I wrote about the Rabobank case. So I would say that we are not prosecuting criminal money laundering and that is a problem.

What you are asking, however, is really whether the regulatory regime that is in place to detect money laundering and prevent banks from engaging in it has been effective. There is no way to determine this through data because hard data (not extrapolated estimates) of the amount of money laundered in the world do not and cannot exist by their very nature. What I can say is that the AML compliance violation cases that we have seen over the past few years (HSBC, Wachovia, Citigroup, BNP Paribas, Rabobank, etc.) tell us that many large international bank were either paying lip service to complying with the legal requirements or were actively subverting the measures up until about 2010. I have no reason to believe that these cases are not indicative of an industry-wide approach because banks had absolutely no incentive to comply with laws which would ultimately require them to turn away clients and money that they had previously banked very willingly. The question at this point is whether, now that there has been some significant enforcement of AML compliance laws, banks are

actually complying with those laws and regulations and if they are turning away business/closing accounts where there is significant indication of money laundering.

The crescendo of complaints by the industry about the "rising cost" of compliance indicates that this is the case. I have "rising cost" in quotations because we are talking about the cost of complying with laws that have been in place for many, many years now, so this is neither a new cost nor one that could not have been anticipated, and should be estimated in terms of costs that should have been incurred and spread over that lengthy time period. The other indication that the regime is now having an effect is the industry's disproportionate measures in what has come to be called "derisking" entire client categories and/or business with certain countries. Some of that activity may be due to a serious concern by the bank about managing the risks associated with a certain business, but research has indicated that some banks may be jettisoning some types of business in order to freeze out competition for those services and then offering those services themselves (such as in the money transmission area).

In some cases, I think certain actions are being taken in order to try to force deregulation, such as when Bank of America, a major provider of banking services to foreign embassies in the U.S., sent a letter to its embassy clients that it was going close their accounts and cease to provide banking services to them only one week before closing their accounts. The action seemed clearly designed to create a diplomatic crisis for the U.S. Government, to be blamed on U.S. AML regulation. If Bank of America's concern was really AML related, they should have worked with FinCEN and law enforcement to identify accounts, individuals and activities of concern and, after doing so, closed the accounts in accordance with a process that was agreed with the Government. If the decision was that they simply did not want to service what they perceived as a high-risk client but they hadn't actually observed money laundering red flags associated with the accounts, they should have provided the embassies with adequate notice, giving them time to find an alternative service provider and to migrate their accounts. Instead, they chose to create an unnecessary and unwarranted diplomatic crisis which should have had the effect of undermining their credibility in speaking out with AML regulatory concerns. It certainly undermined their credibility with me.

Giving FinCEN total responsibility for establishing annual AML priorities for banks and monitoring every bank's progress every 3 months, as was recommended by the Clearing House, is extremely ill-advised. A financial institution understands its own business and products better than anyone else. It is therefore best-placed to determine what its AML risks are and how best to address those risks within the systems that it has created. We support the idea of a financial institution working with FinCEN/Treasury to discuss those risks in the context of national and global trends observed by FinCEN, and whether adjustments might be made as a result, however. In addition, reviewing each financial institution's progress in AML every 3 months seems like far too short a time frame to observe how an FI is progressing in this respect, however, and en-

tirely impractical from a Government resource allocation perspective.

On a related note the suggestion that FinCEN be given access to bulk data transfers from financial institutions to enable it to analyze AML trends and patterns across institutions is another potentially useful idea. But questions about the effectiveness and cost of this proposal include whether FinCEN currently has the technological capability and personnel needed to perform that type of data analysis or whether it would need to be built, which could be a significant expense. In addition, charging FinCEN with industrywide data collection and analysis should not be seen as a way for banks to absolve themselves of their AML obligations. The banks would retain their position as the primary gateway into the U.S. financial system, so the first level of responsibility to safeguard the system against money-laundering abuses must remain with the individual banks who open their accounts to individuals and entities around the world.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM HEATHER A. LOWE

Q.1. What are the costs and benefits of having bank examiners assess bank compliance with the Bank Secrecy Act's (BSA) requirements instead of having anti–money laundering (AML) and combating the financing of terrorism (CFT) experts at the Financial Crimes Enforcement Network (FinCEN) examine bank compliance programs?

A.1. I am not sure it will make much of a difference. Currently, you have examiners sitting at the Securities and Exchange Commission, the Commodities Futures Trading Commission and other specialized agencies who have specific AML/CFT training. When they have AML/CFT enforcement questions, they liaise with FinCEN as needed. If you had those people instead within FinCEN, they have easy access to FinCEN personnel but would have to reach out to the other agencies for sector-specific guidance. Would bringing all of the examiners into FinCEN result in a more coherent approach to examination? Unlikely, unless specific changes were made to the examination procedures and incentives for examiners. However, I can also imagine that should there be more coherence in examination procedure across industries, it would give rise to the problem that examinations are not nuanced enough and therefore not even addressing issues specific to a given industry where AML/CFT risks may be significant. I can imagine that industry complaints about that would surge. No company will ever be happy with the way they are examined, so it is most important to work with industry to identify real problems which result in ineffective or inadequate AML oversight and with law enforcement to identify areas where the resources being expended by industry seem disproportionate to the value of information gleaned from their efforts, and not just industry complaints.

Q.2. Is there a way to maintain a top-shelf effective AML/CFT policy while maintaining a commitment to increase access to financial products for the underbanked and immigrants who rely on remittance services?

I'm interested in the ways in which technology can aid AML compliance efforts. What are some of the innovative technologies that you've seen that hold some promise for either the Government or the private sector?

What are the barriers to either the Government or the private sector adopting these technologies?

What can we be doing as legislators to ensure that we promote technological innovation in this sector?

A.2. The most significant block to adopting new technologies is, I believe, a concern that regulators will not recognize the use of a new technology as a positive development in examinations. I therefore support the creation of a technological "sandbox", as has been proposed by The Clearing House and has been implemented in the U.K. It is important to note that the U.K. structure appears to have some specific safeguards to protect consumers which they consider to be an integral part of their system. U.K. regulators presented their approach at a recent FATF industry consultation meeting I attended. They stressed the importance of ensuring that consumers were protected at all times as innovative approaches were being tested, and the U.S. should do the same. In the House of Representatives, members are discussing legislative language that does not require any of the safeguards present in the U.K. system, potentially giving financial institutions an unlimited safe harbor for the use of any new technology with no Government oversight. This is a significant danger because if a financial institution spends the money to integrate new technology that, it turns out, isn't as effective as alternative methods, they would have no incentive to change their approach. They would incur some unwelcome cost for doing so and they'd have the security of an unlimited safe harbor, so there would be no incentive to act.

Q.3. The regulatory definition of "financial institution" has been expanded several times over the years, both by FinCEN rulemaking and by legislation by Congress.

Should the definition of financial institutions be expanded to include other sectors? If so, which sectors?

Could these changes be made via FinCEN rulemaking or should legislation be passed?

A.3. FATF has identified several of what it calls Designated Non-Financial Businesses and Professions, or DNFPB's, as businesses and professions that are susceptible for, or can be used to play a part in, money laundering. The idea is that these businesses and professions should identify who they are doing business with, in some cases carry out some customer due diligence, and file suspicious activity reports if they think a transaction is suspicious.

The U.S. already requires some DNFBPs to have those AML programs, such as casinos and dealers in precious metals and stones. Treasury regulations originally also included others, including travel agents, those involved in real estate closings, and car, plane, and boat dealers, among others, but then Treasury gave them a "temporary" exemption from the requirements with no sunset for that exemption which has now been in place for many years. Still others never made it on any list, and those four are lawyers, accountants, corporate service providers, and escrow agents. For these four,

AML programs would really be about knowing with whom you are doing business and not permitting practitioners in these businesses and professions to be able to have plausible deniability that they didn't have reason to know or suspect that they were providing services that might be laundering dirty money.

While there are clearly several businesses and professions missing from U.S. regulation, I would focus on five of them: lawyers, those involved in real estate closings, corporate service providers, escrow agents, and accountants.

Lawyers: Of course criminals need and use legal services. A *60 Minutes* piece that aired last year featured undercover footage from an organization called Global Witness, showing just how easy it is to walk into a law firm in New York and get a lawyer to easily suggest ways in which structures could be created to spend money that is clearly the proceeds of corruption to buy real estate, planes, etc. One attorney even suggested running the dirty money through the lawyer's client account to clean it. It was a real eye-opener. In 2010, the American Bar Association published what I would characterize as sound *Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing*, but I encourage you to ask every lawyer you know if they have implemented it. It is unlikely that they have even heard of it. This voluntary guidance is simply not enough.

Escrow Agents: Senate Permanent Subcommittee on Investigations' 2010 report *Keeping Foreign Corruption Out of the United States: Four Case Histories* tells the story of how one escrow agent, McAfee & Taft, refused to provide escrow services to Teodorin Obiang, the corrupt, playboy son of the long time dictator of the impoverished Nation of Equatorial Guinea, because the anti–money laundering policy they had voluntarily put in place prescribed that they do so. Another escrow agent without an AML program happily took that money.

Corporate Service Providers: The Panama Papers showed just how entangled corporate service providers like Mossack Fonseca can be in facilitating money laundering, corruption, and tax evasion. The book *Global Shell Games* details research by a team of American and Australian academics into just how easy it is to create an anonymous company to engage in terror finance or corruption in different countries around the world through corporate service providers. They found that the easiest country in which to do so was the United States. One email response to the researchers' inquiry from a corporate service provider in Florida was, "[Y]our started purpose could well be a front for funding terrorism, and who the f—— would get involved in that? Seriously, 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 that 5k a month, and I doubt you are going to find any suckers that will do it for less, if at all. If you are working with less than serious money, don't waste anybody's time here. Using a f——— google account also shows you are just a f——— poser and loser. If you have a serious proposal, write it up and we will consider it. Your previous message and this one are meaningless crap. Get a clue. Just how stupid do you think we are?"

Those Involved in Real Estate: With respect to real estate, since July 2016, FinCEN has had geographic targeting orders in place in various counties in New York, Florida, Texas, and California, requiring title insurance companies to collect beneficial ownership information for those entities buying high value real estate with cash. They found that about 30 percent of the beneficial owners identified by the title companies already had SARs filed on them by other financial institutions. That's nearly one third. Exposés like *The New York Times*' "Towers of Secrecy" show just how easy it is for people to hide behind anonymous companies and buy real estate with proceeds of crime and corruption. It is central to the 2017 indictment of Paul Manafort and Richard Gates as well.

Q.4. In August 2017, FinCEN issued an advisory encouraging real estate brokers to share information with them that could be helpful in AML efforts, while noting they are not required to do so under current law.

How do we increase information sharing between real estate brokers and FinCEN?

A.4. Voluntary measures will not yield the necessary results because it is rare for a business to voluntarily want to lose out on a sale or for it to be discovered that if you work with a particular agent they may provide information to law enforcement about your transcation. Any measure must be industrywide and required to maintain a level playing field. It is necessary to bring them into the definition of Financial Institution. Please see response to previous question.

Q.5. Geographic Targeting Orders (GTOs), which impose additional record keeping and reporting requirements on domestic financial institutions or nonfinancial trades or businesses in a specific geographic area for transactions involving certain amounts of United States currency or monetary instruments, have been deployed since 2016 to target high-end real estate sectors in major metropolitan areas by requiring U.S. title insurance companies to identify the natural persons behind shell companies used to pay "all cash" for high-end residential real estate.

Are GTOs an effective tool or would regulation be a preferable way to cover the real estate sector?

A.5. GTOs are an effective tool for the purposes they were created—to gather intelligence for specific cases or, as in this case, to gather intelligence about the extent of a problem to inform decisions about how to move forward. They should not be used as a long-term measure. With respect to the Title Insurer GTOs, FinCEN now has the information it needs to move forward with a rulemaking—there is clearly a problem in the real estate industry.

However, I would note that I would not focus regulation in the real estate sector on title insurers, but rather on real estate agents, who have the longest and most personal relationship with the buyer and are in a much better position to identify red flags. Furthermore, it is very easy for a cash buyer of real estate to avoid title insurers entirely (which launderers have apparently not realized yet). If I'm trying to launder money through real estate and I'm making an all-cash purchase, I don't need a mortgage and so title insurance isn't actually required. If I'm going to flip the prop-

erty to launder the funds, then I'm not too worried about a challenge to title down the line (my buyer will get their own title insurance and my lack of it doesn't affect that). If I am concerned that the title is not clean and it will therefore be difficult to sell the property, I can have an attorney carry out a title search or I can even do it myself—the search itself is not difficult (I would probably need legal assistance to fix any problems I found however, if I didn't simply abandon that particular purchase). So if I were a money launderer I would simply avoid the title insurers and avoid the disclosures entirely.

Q.6. Cryptocurrency exchanges are money services businesses supervised by State regulators and subject to Federal AML and CFT laws.

Should FinCEN play an enhanced role in assessing the compliance of cryptocurrency exchanges, or are State regulators sufficiently equipped to handle compliance monitoring?

What additional tools could we give regulators and law enforcement?

How prevalent is money laundering in cryptocurrency markets?

A.6. There is certainly work do be done in the area of digital currency/blockchain technology. I am far from an expert in this area, so I will make some recommendations for people to contact. Before I do, however, I would note that I was concerned by the Treasury representative's statement that they felt they had adequately regulated in the digital currency space by regulating the exchangers. Technology has moved on, and the advent of "mixers", which are now used to make it incredibly difficult for the exchangers to identify where the currency they are exchanging is coming from, makes that regulation now insufficient.

You may wish to reach out to Tom Robinson, COO and Cofounder, Elliptic (tom@elliptic.co). Elliptic is a company that finds ways to identify the "anonymous" digital currency traders to help with customer due diligence problems associated with digital currencies.

Mr. Robinson recently coauthored a paper entitled "Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services" with the Foundation for Defense of Democracy's Yaya Fanusie, a long-time expert on illicit and terror finance who has been researching the linkages between terror finance and digital currency. I would recommend reaching out to Mr. Fanusie to further explore this area. Yaya Fanusie, Director of Analysis, Center on Sanctions and Illicit Finance (yaya@defenddemocracy.org).

Finally, Ms. Jamie Smith, Global Chief Communications Officer, The Bitfury Group (jamie.smith@bitfury.com), is an excellent resource as well.

Both Ms. Smith and Mr. Fanusie have extensive prior experience working within U.S. Government agencies and understand political context well.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM HEATHER A. LOWE

Q.1. What is the most effective action a consumer can take to protect against identity theft if the consumer's information has been

compromised? Please include a detailed description of the differences between credit freezes, credit locks, and fraud alerts, including how long each takes to activate and deactivate and the relative benefits and drawbacks of each.

A.1. Unfortunately, I am not an expert on U.S. consumer banking laws and cannot provide an informed response to your question.

Q.2. Many States have laws requiring credit bureaus to provide credit freezes. Can you describe what these laws generally require and discuss whether it is appropriate for Congress to create a Federal standard?

A.2. Unfortunately, I am not an expert on U.S. consumer banking laws and cannot provide an informed response to your question.

Q.3. Gaming and tourism are some of Nevada's top industries. In the State of Nevada, our gaming operators employ thousands of hard working Nevadans, and the industry as a whole domestically supports 1.7 million jobs across 40 States. Qualified casinos, like financial institutions, are also subject to Banking Secrecy Act requirements. Organizations within Nevada have suggested that gaming operators would welcome a review of BSA requirements, which they find to be burdensome. They look forward to this Committee's thoughtful, bipartisan, review of BSA requirements that takes into account the security imperative for robust anti–money laundering efforts, as well as the impact those requirements have on all industries. For example, the Suspicious Activity Report (SAR) ($5,000) and the Currency Transaction Report (CTR) ($10,000) levels were set years ago. Some have recommended increasing these to correspond with inflation. Others believe that would be too high but do support a higher amount than currently.

One of the top priorities of the gaming industry is to remove the requirement for a detailed factual narrative for structuring in the suspicious activity forms. What do you think of this recommendation?

Do you have specific recommendations regarding how the gaming industry can benefit from greater communication with Government agencies and law enforcement? Is there something the Federal Government can do to share information with casinos and others filing SARs about broad benefits that may occur because of some of the 58,000 SAR forms filed by gaming firms.

Would the creation of a Qualitative Feedback Mechanism help reduce money laundering and terrorist financing? Should the Secretary of the Treasury establish a mechanism to communicate anti–money laundering (AML) and countering terrorism financing (CTF) priorities to financial institutions, gaming establishments, and Federal financial regulators? Could such a mechanism provide qualitative feedback on information shared by financial institutions with the Department of Treasury, including CTRs and SARs? Please describe the pros and cons of such a system.

A.3. Financial Institutions file SARs because they believe that activity is suspicious, and descriptions of what they saw that seemed suspicious is important information for law enforcement. SARs are subject to automated data analysis and human review, and the narratives provide information that may seem unimportant alone, but takes on greater significance when reviewed in light of other

SARs. I would not remove the narrative requirement unless law enforcement takes the position that it is of limited value.

Lack of feedback from the Government on what happens to SARs and CTRs has long been a complaint of Financial Institutions. I once highlighted a seminal case regarding tax evasion and money laundering at an international AML seminar in Florida. A very excited compliance officer from the U.S. Virgin Islands approached me after presentation—she had been the person to file the SAR that resulted in the case and she had never known what had happened to it. She was thrilled that her actions had made a difference. I believe that we would have a much more robust AML defense system in the U.S. if more bankers and compliance officers were given such opportunities to feel like their actions really made a difference. Therefore, I am in favor of initiatives like FinCEN Exchange, announced in December, to enhance information sharing with Financial Institutions. I would strongly recommend that the gaming industry engage with FinCEN quickly to ensure that this initiative is set up for the gaming industry in a way that results in practical and meaningful exchange of information with the Government as opposed to something less useful.

I am wary when it comes to the Government setting AML priorities for the industry. It already happens to some extent, but I would strongly caution against actually transferring responsibility for setting AML priorities for individual Financial Institutions from those institutions to FinCEN. Financial Institutions are best placed to understand their business and their systems and the money laundering risks inherent therein, and create the systems that work best in their business models to combat money laundering. FinCEN and/or other regulators should review those assessments but cannot be responsible for carrying them out.

Q.4. The Office of the Comptroller of the Currency mentioned in its 2018 Banking Operating Plan that financial institutions should not inadvertently impair financial inclusion. But, as of September 2017, the OCC has not identified any specific issues they plan to address. We know that derisking has become an epidemic across many communities and industries, such as communities along the Southwest border, humanitarian organizations aiding Nations wracked with violence, and remittances providers that serve fragile Nations like Somalia.

What type of guidance could the OCC, FinCEN, FDIC, and the Federal Reserve provide to help banks meet the banking needs of legitimate consumers and businesses that are at risk of losing access—or have already lost access?

A.4. My organization focuses on the movement of illicit money out of developing countries the effect of that financial flow for development, and not financial flows into developing countries, so we have not focused a great deal on the remittances and nonprofit issues. Nonprofit organizations like the Charity and Security Network, Oxfam, and the Center for Global Development, and intergovernmental organizations such as the World Bank, the IMF, the OECD and others have been doing a great deal more research in this area and I would recommend speaking with them for more developed and far-reaching recommendations.

Having said that, there are three somewhat different problems in the derisking area with root causes that are not all AML-related, and I think that is a really important point here. One is that banks that are no longer willing to provide banking services to money service businesses (MSBs) that are the primary movers of remittances. Second is banks choosing not to do business with correspondent banks in certain very high-risk countries. (The Somali remittance problems are a combination of both these first and second categories.) Third, is the problem of banks choosing not to provide banking services for charities/nonprofits. These are related issues, but not the same issues. Something to bear in mind as well is that the World Bank has found that the cost of transmitting remittances has actually decreased over the past several years, suggesting that some of the problems in the sector may really be location specific, such as with Somalia, as opposed to being as widespread as discussion on this topic might suggest.

In 2012 and the following 2 years, FATF Recommendations and related guidance were published relating to risks posed by nonprofits and risks posed by MSBs. That guidance suggested that those entire sectors were particularly vulnerable to money laundering with no nuance, which resulted in banks categorizing them all as high risk, regardless of the nature of those businesses, the strength of their compliance programs, their clientele, or other risk assessment factors. The general refrain from banks was that it was too costly to do proper AML vetting on all these "high risk" entities. Banks also said they were pulling out of high risk areas because of an increase in fines and penalties, but very few fines/penalties have been levied related to servicing MSB or nonprofit clients, which begs the question of whether this reaction was simply disproportionate or driven by other motives, such as an excuse to get out of these relatively low-margin lines of business.

For example, Barclays in the U.K. caused a bit of a crisis when it closed the accounts of the vast majority of the money service businesses it serviced. But it held on to MSBs with assets of $10m or more. However, the significant MSB money laundering case on record actually relates to Western Union, one of the world's largest and well-capitalized MSBs. Barclays' decision to jettison smaller MSB accounts was made not in relation to actual enforcement trends, how good their MSB clients' compliance programs were, or other risks relating to the individual MSB's business or other relevant factors, it was made on whether the bank wanted to keep that capitalization or not and bother to continue servicing smaller accounts where its margin was smaller and getting smaller because of compliance costs. It would be interesting to find out pre-2012 margins on these business lines versus post-2012 margins so that Congress has a frame of reference for what a bank consider an unacceptable margin in these business lines.

And that raises an important point in all of this that is very often missed. There has been huge bank consolidation leading to behemoth banks that do not consider providing services to smaller account holders to be worth the cost. (In our experience, smaller, local banks rarely provide adequate international transfer services and did not do so prior to AML regulation.) We see that every day as banking fees for people who have little savings climb while those

who have sizable accounts have no fees at all. Banks are doing everything they can to increase their profit margins with little regard to the effect on the average account holder. That's today's business model, and bank decisions regarding MSB and nonprofit account holders are driven in large part by this model. Furthermore, the Center for Global Development put out a report on derisking in 2015. In that report, they noted that some banks have "derisked" and then beefed up their own money transmitter services, suggesting a possible move to undermine competition and seize the market themselves.

So there are problems, some of which are not actually AML related, but the following are some measures that can be taken in the AML sphere to help in this area:

- Better nuanced Recommendations and guidance from FATF and regulators is needed.
  - In October 2014, FATF spoke out against blanket derisking and said that FIs should derisk only on a case by case basis. FinCEN, the FDIC, and the OCC followed that up asking banks to come to the regulators if they felt pressure to terminate an MSB relationship. Other regulators have followed.
  - Unfortunately it seems that there is no hard data to be able to measure what has happened in the market since.
  - After an outcry from the global nonprofit community, FATF revised its guidance with respect to the problematic Recommendation 8, but I think it still needs further revision and U.S. Treasury could use its influence to make that happen. Please contact Kay Guinane at the Charity and Security Network for further information (kguinane@charityandsecurity.org).
- Banks should have access to information from FinCEN about whether an MSB has been the subject of formal warnings/cease and desists which are not public information, so that they can better judge the strength of an MSB's compliance program and its weaknesses.
- Create a low-cost certification scheme for smaller MSBs. Such a scheme would create benchmarks for MSB compliance programs, similar to what has been done in the development of an ISO standard for anticorruption compliance. This could perhaps be subsidized by a fund the big banks pay into for the smaller MSBs.
- One element of compliance cost is identifying the true owners and controllers of MSBs and charities, as well as the remitters themselves. Transparency about who owns and controls companies would be a real help with that.
- National ID schemes for individuals around the world are also important. India leading the way in effectively doing this in rural populations living in poverty—the hardest to reach and often recipients of remittances. While it may seem to be outside of Congress' remit, USAID has financially supported these initiatives in the past and Congress could prioritize funding to USAID to continue and/or increase this work.

Q.5. Last year, the Countering Iran's Destabilizing Activities Act of 2017 (P.L. 115-44) was enacted. In Section 271, it required the Treasury Department to publish a study by May 1, 2018, on two issues:

Somali Remittances: The law required the U.S. Department of Treasury to study if banking regulators should establish a pilot program to provide technical assistance to depository institutions and credit unions that wish to provide account services to money services businesses serving individuals in Somalia. Such a pilot program could be a model for improving the ability of U.S. residents to make legitimate funds transfers through easily monitored channels while preserving strict compliance with BSA.

Sharing State Banking Exams: The law also required Treasury to report on the efficacy of money services businesses being allowed to share certain State exam information with depository institutions and credit unions to increase their access to the banking system.

Have you or your organization been involved with these Treasury studies?

What advice did you give—or would you give—on the pilot studies?

A.5. I have not been involved with either of these Treasury studies because other organizations have been leading research and advocacy on remittance issues. They may have been involved in and/or consulted on these issues. Please contact: Kay Guinane, Director of the Charity and Security Network (kguinane@charityandsecurity.org); Vijaya Ramachandran, Senior Fellow at the Center for Global Development (vramachandran@cgdev.org).

Q.6. In 2016, William and Margaret Frederick were moving from Ohio to Las Vegas. Unfortunately, it is alleged that the title company they used in Columbus, Ohio, fell for an email scam and wired the $216,000 profit from their home sale to a hacker, not to the Fredericks. William is 83 and Margaret is 75 and as of October, they were still trying to get their money back. While the Fredericks' tale is now a court case to determine who was responsible for the fraudulent information, we know that the Fredericks' experience is "very typical" of scams that divert an estimated $400 million a year from title companies into bogus accounts.

Please describe the responsibilities of financial firms to avoid these frauds?

What penalties should be assessed and by which agencies when financial firms enable theft?

What is the role for the Consumer Financial Protection Bureau to ensure financial firms protect their customers' money and information?

A.6. As noted above, I am not an expert on U.S. consumer banking laws and cannot provide an informed response to your question with respect to CFPB. Your question regarding the title insurance company's culpability is a fact-specific question of criminal or tortious liability that I am unable to answer in this format, and does not relate to money laundering.

Q.7. In 2014, FinCEN issued an advisory with human trafficking red flags, to aid financial institutions in detecting and reporting suspicious activity that may be facilitating human trafficking or human smuggling.

To what extent do you assess that financial institutions are currently utilizing these red flags, in order to better assess whether their banks are being used for to finance human trafficking? If institutions are not widely utilizing the red flags, what actions is FinCEN taking to encourage them to do so?

A.7. I have not seen any data pertaining to the number of SARs filed in relation to human trafficking or smuggling in the United States, so I do not have enough information to provide an accurate assessment. FinCEN has an online tool that can be used to look at the number of SARs filed with respect to specific activities, but unfortunately human trafficking is not one of the categories. However, anecdotally I can say that human trafficking and human smuggling are issues where I have seen a relatively large number of training programs offered to compliance personnel in recent years. It is therefore on the radar of compliance personnel in the U.S. at least. I would recommend that you reach out to FinCEN for an answer to this question and, if they are not currently collecting statistics to be able to answer this question, ask or legislate for them to do so. You might also reach out to Polaris for further discussions on the intersection between money laundering and human trafficking.

Q.8. What are the pros and cons of reducing or eliminating the standards requiring SARs filing for insider abuse (i.e., employee misconduct)?

A.8. I do not have a strong opinion about this issue. Logically, however, I think it is helpful for FinCEN to know the identifying information of people who have been found by financial institutions to be engaging in fraudulent activity or other malfeasance, and for the CFPB to be aware of the same if it involved harm to consumers, but I do not necessarily think a SAR is likely to be the most effective way to communicate that.

Q.9. The common expectation is that any financial institution subjected to a cyberattack would be in touch with law enforcement about whether or not it's required to file an SAR. What are the pros and cons of eliminating SAR filing requirement for cyberattacks against financial institutions?

A.9. Cyberattacks are an ever-growing threat to the financial services sector and, therefore, to the business and individual consumers with accounts at financial institutions. A great deal of personal information is collected and held by financial institutions, so they are a particular target for that reason as well. I think FinCEN does a good job of explaining why they want cyberattacks to be reported in SAR form, how they have used such information in the past, and what information is most useful for them in a SAR relating to cyberattacks in an October 2016 Advisory. In December 2017, news broke in the U.K. that the U.K.'s Financial Conduct Authority had found that U.K. banks were significantly under-reporting the full extent of cyberattacks. As history has shown in a number of AML-related areas, it is unlikely that U.S. banks are reporting more rig-

orously. This puts not only account holders at risk, but the entire fabric of our financial system.

Q.10. As you know, under current regulations, FinCEN currently exempts a range of institutions from the requirement to maintain an anti–money laundering program. The list of exempted institutions includes "pawnbrokers," "private bankers," "seller of vehicles, including automobiles, airplanes and boats," as well persons "involved in real estate closings and settlements" among others.

In your view, what are some of the most glaring exemptions on this list?

Are there any additional categories of institution, such as persons involved in the art market or lawyers that should be required to establish minimum anti–money laundering program requirements?

A.10. FATF has identified several of what it calls Designated Non-Financial Businesses and Professions, or DNFPB's, as businesses and professions that are susceptible for, or can be used to play a part in, money laundering. The idea is that these businesses and professions should identify who they are doing business with, in some cases carry out some customer due diligence, and file suspicious activity reports if they think a transaction is suspicious.

The U.S. already requires some DNFBPs to have those AML programs, such as casinos and dealers in precious metals and stones. Treasury regulations originally also included others, including travel agents, those involved in real estate closings, and car, plane, and boat dealers, among others, but then Treasury gave them a "temporary" exemption from the requirements with no sunset for that exemption which has now been in place for many years. Still others never made it on any list, and those four are lawyers, accountants, corporate service providers, and escrow agents. For these four, AML programs would really be about knowing with whom you are doing business and not permitting practitioners in these businesses and professions to be able to have plausible deniability that they didn't have reason to know or suspect that they were providing services that might be laundering dirty money.

While there are clearly several businesses and professions missing from U.S. regulation, I would focus on five of them: lawyers, those involved in real estate closings, corporate service providers, escrow agents, and accountants.

Lawyers: Of course criminals need and use legal services. A *60 Minutes* piece that aired last year featured undercover footage from an organization called Global Witness, showing just how easy it is to walk into a law firm in New York and get a lawyer to easily suggest ways in which structures could be created to spend money that is clearly the proceeds of corruption to buy real estate, planes, etc. One attorney even suggested running the dirty money through the lawyer's client account to clean it. It was a real eye-opener. In 2010, the American Bar Association published what I would characterize as sound *Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing*, but I encourage you to ask every lawyer you know if they have implemented it. It is unlikely that they have even heard of it. This voluntary guidance is simply not enough.

Escrow Agents: Senate Permanent Subcommittee on Investigations' 2010 report *Keeping Foreign Corruption Out of the United States: Four Case Histories* tells the story of how one escrow agent, McAfee & Taft, refused to provide escrow services to Teodorin Obiang, the corrupt, playboy son of the long time dictator of the impoverished Nation of Equatorial Guinea, because the anti–money laundering policy they had voluntarily put in place prescribed that they do so. Another escrow agent without an AML program happily took that money.

Corporate Service Providers: The Panama Papers showed just how entangled corporate service providers like Mossack Fonseca can be in facilitating money laundering, corruption, and tax evasion. The book *Global Shell Games* details research by a team of American and Australian academics into just how easy it is to create an anonymous company to engage in terror finance or corruption in different countries around the world through corporate service providers. They found that the easiest country in which to do so was the United States. One email response to the researchers' inquiry from a corporate service provider in Florida was, "[Y]our started purpose could well be a front for funding terrorism, and who the f—— would get involved in that? Seriously, 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 that 5k a month, and I doubt you are going to find any suckers that will do it for less, if at all. If you are working with less than serious money, don't waste anybody's time here. Using a f——— google account also shows you are just a f——— poser and loser. If you have a serious proposal, write it up and we will consider it. Your previous message and this one are meaningless crap. Get a clue. Just how stupid do you think we are?"

Those Involved in Real Estate: With respect to real estate, since July 2016, FinCEN has had geographic targeting orders in place in various counties in New York, Florida, Texas, and California, requiring title insurance companies to collect beneficial ownership information for those entities buying high value real estate with cash. They found that about 30 percent of the beneficial owners identified by the title companies already had SARs filed on them by other financial institutions. That's nearly one third. Exposés like *The New York Times*' "Towers of Secrecy" show just how easy it is for people to hide behind anonymous companies and buy real estate with proceeds of crime and corruption. It is central to the 2017 indictment of Paul Manafort and Richard Gates as well.

Q.11. In recent years we've witnessed a seemingly endless string of money laundering violations by some of the largest global banks, with Deutsche Bank being the most recent megabank to disregard the anti–money laundering requirements contained in the Bank Secrecy Act.

Given that large megabanks continued to disregard their obligations under the law, what in your view should this Committee do to ensure compliance, particularly by the largest global banks?

A.11. Unfortunately for the banking community, many of the high profile, incredibly egregious cases that involve the biggest banks in

the world have eroded public trust that banks will indeed act in a manner that is law-abiding and actively try to turn away proceeds of crime. Even many bankers lack faith in their institutions. You may find a 2015 study by the University of Notre Dame and the law firm of Labaton Sucharow, entitled "The Street, the Bull, and the Crisis", to be of interest. The researchers surveyed more than 1,200 U.S. and U.K.-based financial services professionals to examine views on workplace ethics, the nexus between principles and profits, the state of industry leadership and confidence in financial regulators. As the report states, "The answers are not pretty. Despite the headline-making consequences of corporate misconduct, our survey reveals that attitudes toward corruption within the industry have not changed for the better."

There are forms of enforcement that we have not been pursuing that I believe would be highly dissuasive. The first is prosecuting the individuals that are behind the decisions that are resulting in these money laundering violations. When a banker sees his or her colleague being prosecuted for decisions that bring the proceeds of crime into the bank, he or she will be careful not to do the same. Second, prosecution of financial institutions has historically been for regulatory violations of the BSA as opposed to the criminal act of money laundering, even when the hallmarks of a clear money laundering case are present. We need to begin to criminally prosecute these entities as well. Finally, when a financial institution is convicted of or pleads guilty to felonious behavior, it must trigger any cross-debarments that we have built into our legal system. For example, Credit Suisse should have lost its status as a Qualified Professional Asset Manager (QPAM) in 2014 by virtue of its conviction for facilitating large-scale tax evasion by Americans. However, as with several similar cases which preceded it, the Department of Labor waived Credit Suisse's disqualification and allowed the bank to continue to enjoy this "privileged" status under U.S. law that meant that the bank had to meet fewer regulatory requirements in its handling of U.S. pension funds—something we tend to try to keep felons away from for public policy reasons.

Q.12. Despite record fines, rarely have the individuals who run the largest global banks been held accountable for their firms' willful disregard of anti–money laundering and counterterrorism financing rules included in the Bank Secrecy Act.

Can you discuss why we've seen such low levels of individual accountability for such violations? To what degree does the lack of clear chains of responsibility within large firms contribute to the lack of accountability among senior leaders?

A.12. The Department of Justice is the most appropriate body to answer this question because it is the body that has taken these decisions based on the evidence before it, prosecution guidelines, and cost/benefit analysis. However, there have certainly been a few cases where information made publicly available the Statement of Facts attached to relevant Deferred Prosecution Agreements, such as excerpts from emails between executives, strongly suggested that there was sufficient evidence to bring individuals to trial in certain cases, and yet we did not see that happen. When I have asked the DOJ about this, they have responded that they did not

feel that they had sufficient evidence to move forward with prosecution.

After receiving a fair amount of criticism about this, in September 2015 the DOJ released a memo outlining its intention to more frequently prosecute individuals. It would be worthwhile to ask for the DOJ for statistics around prosecutions of individuals before and after the publication of the memo. It is possible that we are seeing the first significant example of this approach being applied to a large bank money laundering case in the case of Rabobank, as I explain more fully in a recent blog post that was heavily quoted in the press. It will be important to keep an eye on whether individual executives are prosecuted in that case for the reasons outlined in the blog.

Q.13. Just as the success of the BSA is reliant on good behavior by individual employees of financial institutions, the efficacy of the BSA also depends on regulatory and supervisory accountability. U.S. anti–money laundering efforts in recent years at times failed to recognize the cumulative effect of the violations they cited, leading them to permit massive problems to occur before any serious enforcement actions were taken.

What in your view should be done to address this problem and ensure that regulators are holding repeat violators of the Bank Secrecy Act accountable?

To your knowledge, to what extent are Bank Secrecy Act deficiencies currently factored into the management aspect of firms' CAMELS rating?

A.13. It seems clear that any policies in place regarding number and nature of infractions leading to escalation in enforcement actions are either insufficient or not adhered to. Either way, this is an area that could certainly benefit from Congressional review. Policies on elevation/escalation need to be clear, proportionate, and enforced in a way that results in meaningful adjustments/reforms being carried out by banks when they have been the subject of violation notices.

While I think the revolving door issue is a tricky one (we want experienced people in Government and in financial institutions and they should have the ability to progress their careers), I am concerned that there may not be sufficient safeguards preventing regulators from moving directly to work for the banks that they have been regulating. In the recent Rabobank case, Rabobank's OCC examiner put Rabobank under a Formal Agreement (requiring reform of their AML compliance program), and then while that Formal Agreement was still in place, she was hired by Rabobank as a senior executive overseeing compliance at the bank. According to Rabobank's Plea Agreement and accompanying Information, the OCC released Rabobank form that Formal Agreement within the year, although bank employees reported that nothing substantial having changed within the bank's compliance program in that time. Whether or not the executive used her close ties to the OCC to get the Formal Agreement dismissed, measures should be put in place to ensure that the revolving door does not allow this type of situation to arise.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

COUNTERING INTERNATIONAL MONEY LAUNDERING

Countering International Money Laundering

Total Failure is 'Only a Decimal Point Away'

By John A. Cassara

August 2017

FACTCOALITION

Financial Accountability & Corporate Transparency

Countering International Money Laundering

Total Failure is "Only a Decimal Point Away"

August 2017

By John A. Cassara

Acknowledgements

The FACT Coalition would like to thank the Ford Foundation and the Wallace Global Foundation for their support for this report.

The FACT Coalition would also like to thank Clark Gascoigne (Deputy Director), Jacob Wills (Communications and Operations Associate) and Yaroslav Pustarnakov (Advocacy Intern) for their contributions to the report. FACT also appreciates the contributions of Liz Confalone and Heather Lowe (Global Financial Integrity); Mark Hays, Stefanie Ostfeld, and Eryn Schornick (Global Witness); Elise Bean; Jo Marie Griesgraber (New Rules for Global Finance); Susan Harley (Public Citizen); and Nathan Proctor (Fair Share).

Cover Image Sources: Billion Photos / Shutterstock.
Cover Image Copyright: All Rights Reserved.
Cover Design: Clark Gascoigne

Copyright © 2017 The FACT Coalition. Some Rights Reserved.

This work by John A. Cassara and the FACT Coalition is licensed under a Creative Commons Attribution 4.0 License. To view the terms of this license, visit www.creativecommons.org/licences/by/4.0. The cover image is copyrighted, with all rights reserved.

The recommendations are those of the author and the FACT Coalition. The views expressed in this report are those of the author and the Coalition, and do not necessarily reflect the views of our funders, our members, or those who provided review.

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 promotes 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 **5**
"TOTAL FAILURE IS JUST A DECIMAL POINT AWAY" 5
WHAT CAN BE DONE? 5
I. INTRODUCTION **7**
II. BACKGROUND **9**
DEFINITION 9
MAGNITUDE 9
III. SITUATION IN THE UNITED STATES **15**
V. BOTTOM LINE RESULTS **17**
VII. POLICY RECOMMENDATIONS **19**
CONGRESS 19
Congress Should Move Legislation to End the Abuse of Anonymous Shell Companies by Requiring Beneficial Ownership Transparency. *19*
Make All Felonies Predicate Offences for Money Laundering *19*
Establish a Global Network of Trade Transparency Units (TTUs) *19*
Promote Usage of the Legal Entity Identifier (LEI) *20*
Expand Due Diligence Obligations to Transactional Lawyers and Formation Agents *20*
INTER-AGENCY RECOMMENDATIONS 21
Develop an Updated Anti-Money Laundering Strategy *21*
Adapt Crime Fighting Strategies to Cover Mobile Payments *21*
Require Beneficial Ownership Information from Government Contractors *21*
Legal Entity Identifier in Procurement *21*
TREASURY DEPARTMENT AND THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN) 21
A FATF Recommendation on Trade-Based Money Laundering (TBML) *21*
Strengthen Due Diligence Requirements for Financial Institutions *22*
Initiate a New Money Services Business (MSBs) Registration Effort *22*
Close Gatekeeper Loopholes *23*
DEPARTMENT OF JUSTICE 24
Hold Individuals Accountable for Corporate Wrongdoing *24*
Change the Incentives for Law Enforcement *24*
Enhance AML/CFT Training *24*
VII. CONCLUSION **25**
ABOUT THE AUTHOR **27**
ABOUT THE FACT COALITION **29**
REFERENCES **31**

Executive Summary

Worldwide anti-money laundering efforts are currently just a decimal point away from total failure. Failure would have a dramatic impact on U.S. law enforcement and financial systems. Why? Because outside of crimes of passion, criminals, kleptocrats, and unscrupulous companies are typically motivated by *greed*.

In today's interconnected world, the manifestations of unfettered avarice impact us all. We see it in our communities: the opioid, methamphetamine, and cocaine epidemics are devastating. Financial fraud, fraud in government contracting, identity theft, and worse endanger individuals and our communities and waste taxpayer dollars. Terror finance and sanctions busting threaten national security.

Law enforcement, policymakers, and the media can get so distracted with the immediacy of the criminal behavior it is easy to forget that the aim of criminal activity isn't the crime itself—but the *proceeds* of the crime. Advocates, scholars and researchers have all questioned the efficacy of the "War on Drugs."[1] But why don't we acknowledge that our inability to stop the laundering and seize the proceeds fuels the greed behind the drug trade?

How much money is being laundered? Estimates are difficult without better data, but the International Monetary Fund (IMF) and United Nations Office on Drugs and Crime (UNODC) estimate the scale of global money laundering falls somewhere around two to five percent of global gross domestic product — approximately $1.5 trillion to $3.7 trillion in 2015. The IRS observes: "money laundering is tax evasion in progress." If tax evasion here and abroad is included in the count, the magnitude of international money laundering is staggering.

"Total Failure Is Just a Decimal Point Away"

How well are we doing in fighting the problem? The data we do have presents a bleak picture. Here are a few sobering numbers:

- According to the UNODC, less than one percent of global illicit financial flows are seized and forfeited.
- Raymond Baker, a longtime financial crime expert, notes that the numbers show enforcement fails 99.9 percent of the time. "In other words, total failure is just a decimal point away."
- Dated information suggests money launderers face a less than five percent risk of conviction in the United States. The situation in most areas of the world is even worse.

What Can Be Done?

This report advances a number of "steps-forward" on how to more effectively combat money laundering.

Congress

- Congress should move legislation to end the abuse of anonymous shell companies by requiring beneficial ownership transparency.
- Congress should make all felonies predicate offences for money laundering.
- Congress should provide specific line item funding to the U.S. Trade Transparency Units (TTUs) so as to enhance their analytic capabilities and augment the personnel necessary to foster trade transparency in the United States and to expand the international TTU network.
- Congress should pass legislation which requires U.S. companies that engage in financial transactions to obtain a Legal Entity Identifier (LEI).

- Congress should pass legislation requiring transactional lawyers, and anyone else who forms legal entities, to carry out anti-money laundering due diligence.

Inter-Agency

- The U.S. should develop an updated anti-money laundering strategy to address new and continuing threats to the financial system.
- The U.S. should convene an inter-agency task force to adapt crime-fighting strategies to cover the use of mobile payment systems.
- The administration should require bidders for federal contracts and grants to publicly disclose their beneficial ownership information.
- The administration should adopt the Legal Entity Identifier (LEI), or a similar, non-proprietary and open system, that makes the hierarchy of entity ownership transparent, as the standard identifier in the federal procurement process.

Treasury Department and the Financial Crimes Enforcement Network (FinCEN)

- The Department of the Treasury, which leads the U.S. Financial Action Task Force (FATF) delegation, should introduce a resolution calling for members to promote trade transparency in order to combat trade-based money laundering and value transfer.
- Treasury should instigate a new rule-making process to strengthen due diligence requirements for financial institutions.
- FinCEN should be tasked with aggressive outreach to communities that rely on informal Money Service Businesses (MSBs). FinCEN should pre-empt state MSB licensing requirements and establish uniform licensing requirements that would be applicable to any company designated as an MSB/money transmitter in the United States.
- FinCEN should finalize the proposed rule to impose anti-money laundering (AML) and suspicious activity reporting requirements on registered investment advisers.
- FinCEN should re-examine each of the temporary AML exemptions to determine whether these exemptions are still warranted.

Department of Justice

- The Department of Justice should ensure that the top decision-makers at financial institutions, accounting firms, and law firms are held personally accountable for the actions of their organizations.
- Justice should change the incentives for law enforcement to encourage them to pursue complex financial crimes cases.
- Justice should provide specific funds for anti-money laundering/counter-terrorist finance (AML/CFT) training to the 93 U.S. Attorneys' offices.

The following report details the near failure of current efforts to combat money laundering and the rationale for comprehensive reform. These specific recommendations form the basis of a new approach to addressing money laundering and the dangerous threats to our safety and security from the crimes funded through illicit finance.

I. Introduction

The worldwide failure to successfully combat money laundering has dramatic impact. Outside of crimes of passion, for example, murder committed in a jealous rage, criminals, criminal organizations, kleptocrats, and some businesses and corporations are typically motivated by *greed*. In today's increasingly interconnected world, the manifestations of unfettered avarice impact all of us — politically, socially, economically, and culturally. Around the world people see it in their communities. In the United States and elsewhere, the opioid, methamphetamine, and cocaine epidemics are devastating. Gang violence, financial fraud, fraud in government contracting, corruption, a plethora of internet scams and ransomware attacks, identity theft, and other crimes affect our daily lives. Terror finance and sanctions busting threaten national security.

Law enforcement, policymakers, and the media can get so distracted with the immediacy of the criminal behavior that it is easy to forget the aim of these criminal activities is not the crime itself — but the *proceeds* of crime. Advocates, scholars and researchers have all questioned the efficacy of the "War on Drugs."[2] But why don't we acknowledge that our inability to stop the laundering and seize the proceeds fuels the greed behind the drug trade?

Financial crimes and abusive tax evasion practiced by the elites contribute to the deterioration of social compacts. Worldwide, distrust in the privileged class has seemingly reached epidemic proportions[3] coupled with (if not driven by) a corresponding absence of accountability.[4] Anger and inequality are common themes in both the developed and developing world.

In other words, many of the ills we face come back to *money*. As detailed in this report, money laundering is the great enabler because it turns criminal proceeds into seemingly clean money that can be freely spent. And yet, our efforts to combat international money laundering are almost a complete failure. This report, some of which is adapted from a recent article I wrote for *The Hill*,[5] will explain the shortcomings of our current approach to combating financial crime, and it will outline a number of recommendations for improving those efforts.

II. Background

Definition

Once criminals and criminal organizations accumulate money from their illicit activities, they must try to hide it or disguise it so authorities cannot determine from where the dirty money comes. A working definition of money laundering is "the hiding or disguising of the proceeds of any form of criminal activity." The key word in that definition is *any*. In the United States, we limit the definition to stated "predicate offenses" — or specified unlawful activities — that generate the illicit money upon which money laundering charges can be brought when criminals seek to hide or disguise those illicit proceeds, such as narcotics trafficking, fraud, smuggling, selling child pornography, etc. The international norm to charge money laundering is broader and includes "all serious crimes."[6]

Magnitude

How much money is being laundered? Unfortunately, the estimates are all over the map. The Financial Action Task Force (FATF), an international anti-money laundering/counter-terrorist finance (AML/CFT) policymaking body, has stated that, "Due to the illegal nature of the transactions, precise statistics are not available and it is therefore impossible to produce a definitive estimate of the amount of money that is globally laundered every year." With that caveat in mind, the International Monetary Fund (IMF) has estimated that money laundering comprises approximately 2 to 5 percent of the world's gross domestic product (GDP) each year, or approximately $1.5 trillion to $3.7 trillion in 2015 — nearly the size of the U.S. federal budget.[7] Similarly, the United Nations Office on Drugs and Crime (UNODC) conducted a study to determine the magnitude of illicit funds. According to the UNODC, in 2009, criminal proceeds amounted to 3.6 percent of global GDP (See Table 1).[8]

Table 1: The International Monetary Fund (IMF) Estimates of Money-Laundering as a Percent of Global GDP[9]

Table 1: FATF estimate of money-laundering (1988)

Amounts estimated to have been laundered (1988)	As a percentage of global GDP
US$0.34 trillion	2.0%

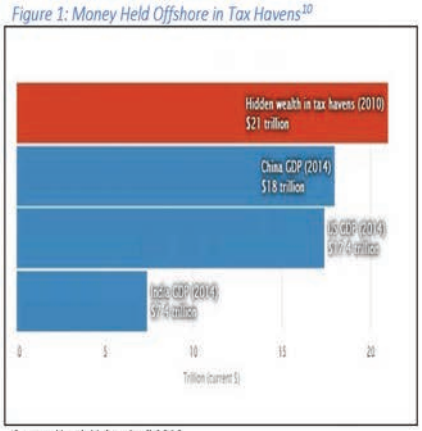
Source: International Monetary Fund, Financial System Abuse, *Financial Crime and Money Laundering- Background Paper*, February 12, 2001.

Table 2: IMF estimates of money laundered (1998)

	Minimum	Maximum	Mid-point
IMF estimates of money laundered as a percentage of global GDP	2%	5%	3.5%
Estimate for 1996 in trillion US$	0.6	1.5	1.1
Estimate for 2005 in trillion US$	0.9	2.3	1.5
Estimate for 2009 in trillion US$	**1.2**	**2.9**	**2.0**

Source: United Nations Office on Drugs and Crime, October 2011

Figure 1: Money Held Offshore in Tax Havens[10]



Source: Youth Voice, April 2016

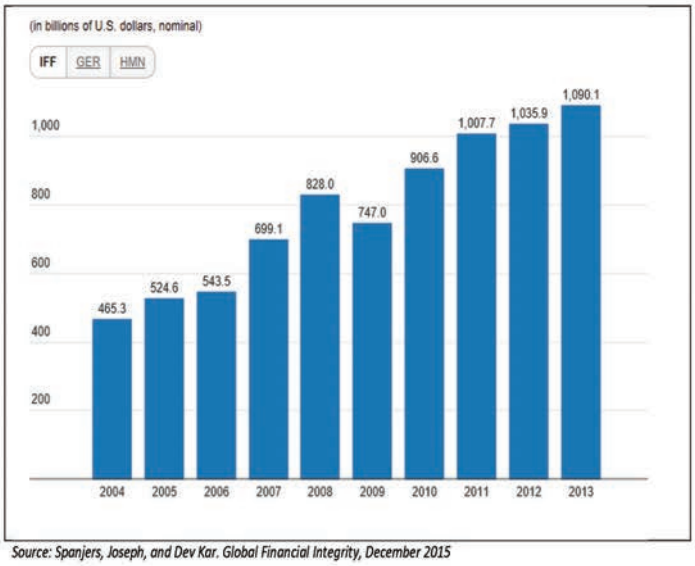
The magnitude of international money laundering is probably much higher depending upon what is included in the count.

For example, there is an international movement to recognize tax evasion as a predicate offense to charge money laundering.[11] A study by the Tax Justice Network estimated that, in 2010, between $21 trillion and $32 trillion was hiding in more than 80 international tax havens. The study also found that privileged elites in 139 lower and middle-income countries had $7.3 trillion to $9.3 trillion in unrecorded offshore wealth while, at the same time, most of the governments of the countries involved were borrowing themselves into bankruptcy and other economic dangers (See Figure 1).[12]

The 2016 release of the "Panama Papers" offers additional proof of the scope of the problem, showing how one Panamanian law firm created a network of over 200,000 non-transparent entities allowing criminals, corrupt government officials, taxpayers, and others to hide their income and wealth.

Global Financial Integrity estimates that the developing world lost $1.1 trillion in illicit outflows in 2013 alone, largely through abusive trade misinvoicing. This practice is a form of trade-based money laundering and a common denominator in both customs fraud and tax evasion (See Figure 2).[13]

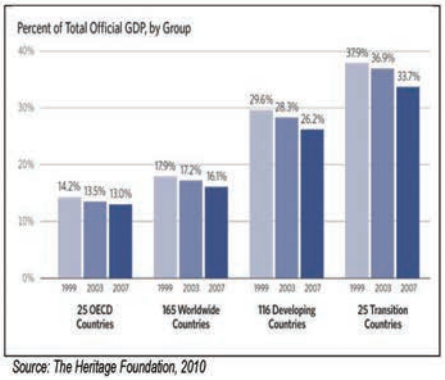
Figure 2: Illicit Financial Flows from Developing Countries: 2004-2013[14]



Source: Spanjers, Joseph, and Dev Kar. Global Financial Integrity, December 2015

Further complicating reliable estimates on the magnitude of international money laundering is the enormity of "black" and "grey" markets around the world. Underground, informal, "parallel," cash-based economies can comprise a substantial portion of a country's GDP. For example, in the economies of countries as diverse as India and Mexico, the underground or black market is estimated at 30 percent or more of GDP.[15] In Egypt, the estimates reach 40 percent.[16] Most economic activity in the Democratic Republic of the Congo takes place in the informal sector, estimated to be up to ten times the size of the formal sector, with many transactions, even those of legitimate businesses, carried out in cash (often in U.S. dollars).[17] International grey markets often include barter trade and forms of cyber payments — two common money laundering methodologies on opposite ends of the tech spectrum — that are generally impervious to financial transparency reporting requirements, taxes, and law enforcement countermeasures (See Figure 3).

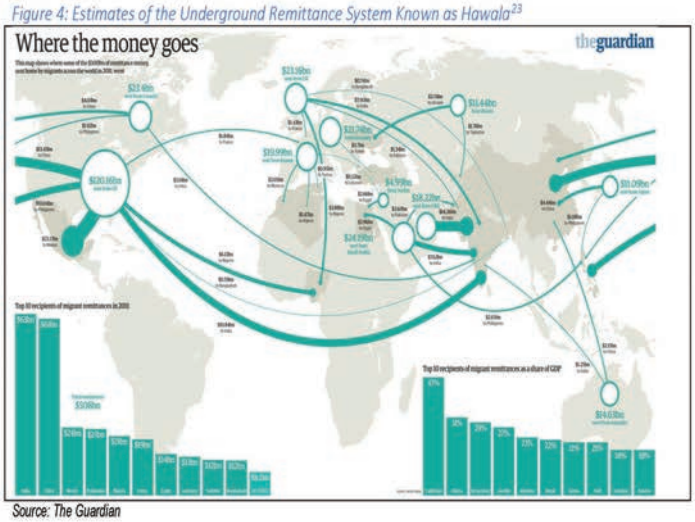
Figure 3: Size and Development of the Shadow Economy[18]



Source: The Heritage Foundation, 2010

There are an estimated 232 million migrant workers around the world.[19] Globalization, demographic shifts, regional conflicts, income disparities, and the instinctive search for a better life continue to encourage ever more workers to cross borders in search of jobs and security.[20] Many countries are dependent on remittances as an economic lifeline. The World Bank estimated that global remittances reached $707 billion in 2016.[21] These estimates cover what was officially remitted. Unofficially, nobody knows. However, the International Monetary Fund believes, "Unrecorded flows through informal channels are believed to be at least 50 percent larger than recorded flows."[22] So, using the above World Bank and IMF estimates, unofficial remittances are enormous. The funds are almost entirely underground and the networks practically impervious to the tax man and law enforcement (See Figure 4).

Figure 4: Estimates of the Underground Remittance System Known as Hawala[23]



Source: The Guardian

Using just one example, economists believe that the underground remittance system known as hawala is a $100 billion industry worldwide. No government should prevent hard working immigrants that wish to send a portion of their income back to their home countries to support their loved ones. However, because of the opaque and underground nature of the financial system, hawala is also a money laundering mechanism. As such, it is abused by criminals and terrorists, endangering national and international security.[24]

Figure 5: Percent of U.S. Properties over $3 Million Bought by Limited Liability Corporations, by Quarter[25]

Source: Ana Swanson, Washington Post, April 2016

The purchase of expensive real estate is another example where there are rising concerns of international money laundering. For example, last year the Chinese spent almost $30 billion on residential property in the United States. The Chinese are also purchasing properties in major western cities such as London, Sydney, Vancouver, Toronto, and Auckland. Most of the purchases are made in cash. The flight of private wealth and tainted money leaving China appears to be due to worries about the economic outlook and the clampdown on corruption. As one former ambassador to China said, the country could very well be "the number one exporter of hot money in the world." Yet China has strict capital controls that limit its citizens to only transferring the equivalent of approximately $50,000 a year out of the country. Despite the restrictions, the torrent of money continues.[26] Anonymous shell companies are a prime method for evading these safeguards, and their use in real estate transactions are widespread and rising (See Figure 5).

III. Situation in the United States

While the anti-money laundering regime is generally better in the United States than in other countries, there remain serious gaps in the U.S. framework — particularly regarding beneficial ownership, trade-based money laundering, and the treatment of the gatekeepers of the financial system (also known as designated non-financial businesses and professions, or DNFBPs).

The total amount of money laundered in the United States is conservatively estimated in the hundreds of billions of dollars every year.[27] According to the Internal Revenue Service, tax evasion is also skyrocketing, and the IRS believes that "money laundering is in effect tax evasion in progress."[28] While tax evasion is not yet considered to be a predicate offense for U.S. money laundering, related crimes are. For example, identity theft connected to tax fraud is rampant, which correlates to a 2015 Treasury Department paper[29] that states fraud is the largest predicate offense for money laundering in the United States — surprisingly, not the proceeds of narcotics trafficking.

Furthermore, money laundering in the United States is grossly underestimated. If we want to better understand the true scale of the problem facing the United States, we should systematically study trade-based money laundering (TBML) and value transfer. Dr. John Zdanowicz, an academic and early pioneer in the field of TBML, examined 2013 U.S. trade data obtained from the U.S. Census Bureau. By examining under-valued exports ($124 billion) and over-valued imports ($94 billion), Dr. Zdanowicz found that $218 billion was illicitly moved out of the United States in the form of value transfer. That figure represents 5.69 percent of U.S. trade.[31]

Table 2: Trade Based Money-Laundering Estimates[30]

Money Illicitly Moved Into The U.S.	
Under-Valued Imports	$272,753,571,621
Over-Valued Exports	$68,332,594,940
Total	$341,086,166,561
As a Percent of Total U.S. Trade	8.87%
Money Illicity Moved Out of the U.S.	
Over-Valued Imports	$94,796,135,280 over valued
Under-Valued Exports	$124,116,420,714 under valued
Total	$218,912,555,994
As a Percent of Total U.S. Trade	5.69%

Source: Zdanowicz, June 2015

Examining over-valued exports ($68 billion) and under-valued imports ($273 billion), Dr. Zdanowicz calculates that $341 billion was moved illegally into the United States — representing 8.87 percent of U.S. trade in 2013 (See Table 2). Almost all of this trade-fraud has escaped both detection and enforcement. Customs fraud is the primary predicate offense of TBML, and the loss of revenue to the United States is staggering. Because TBML often masks underground financial systems, there are concurrent threats to our national security. In just one example, U.S. officials have estimated that the black-market peso exchange — one of the most pernicious trade-based money laundering systems used by narcotics traffickers — is also one of the "largest money laundering methodologies in the Western hemisphere."[32] But the Department of the Treasury appears reluctant to even estimate the magnitude of the scope of the TBML problem.[33]

Of course, laundered money has an exponential effect. A few years ago, the GAO released a report estimating that the amount of drug dollars smuggled across the border from the United States into Mexico primarily to facilitate "placement" into foreign financial institutions approached approximately $39 billion. Of that $39 billion, GAO found that U.S. and Mexican law enforcement and customs officials combined had intercepted only pennies on every dollar smuggled.[34] Those numbers are extremely troubling, because intercepting bulk cash is a comparatively straight-forward anti-money laundering enforcement effort. Performing poorly in intercepting bulk cash does not bode well for the more complex efforts to combat money laundering, including through cyber smuggling, trade-based money laundering, and layering illicit proceeds through a labyrinth of anonymous shell corporations.

The long-term economic consequences of our failure to effectively combat money laundering are far worse than the simple estimates listed above suggest, thanks to the "miracle of compounding." Per an analysis of J.R. Helming, assume narcotics cartels receive a 5% return on the above $39 billion. After 20 years, that $39 billion mushrooms into a $1.7 trillion problem.[35] And that is just one year of enforcement failure, representing just the southwest border, and for just one comparatively straight-forward asset class.

U.S. anti-money laundering investigations are stifled, in part, by the lack of transparency regarding beneficial ownership of legal entities formed in America. According to one study, the United States is one of the easiest places in the world for terrorists, human traffickers, and corrupt foreign politicians to open anonymous companies to launder illicit money with impunity.[37] When investigating the most heinous crimes, it is commonplace for law enforcement to hit a dead-end when encountering a shell company (See Figure 7).

Figure 7: Average Number of Approaches Needed to Find a Provider Willing to set up an Untraceable Shell Company[36]

Source: The Economist, April 2012

"Anonymous shell companies... are one of the primary tools used by bad guys to openly acquire and access nefarious funds," wrote Dennis Lormel, the FBI's former anti-terror finance chief, in 2013. "These dubious dealings are not limited to... 'offshore' tropical islands. The United States is among the most egregious offenders with its woeful lack of regulations requiring the true ownership of companies to be identified."[38]

In April 2016, Patrick Fallon, head of the FBI's financial crimes section, noted: "While we [in the U.S. talk] about offshore accounts in other countries, I think we have a lot of room for improvement here to promote transparency... It is a significant impediment to our investigations when we can't determine who the true owner is of a company."[39]

Furthermore, the Financial Action Task Force sharply criticized the U.S. for its beneficial ownership problems — as well as for shortcomings with regards to U.S. treatment of investment advisers, lawyers, accountants, and real estate agents — in its latest mutual evaluation report published in December 2016.[40]

V. Bottom Line Results

Reliable statistics on money laundering enforcement are hard to find and sometimes dated. Yet the data that do exist present a bleak picture. It is important to remember that in anti-money laundering efforts, the bottom-line *measurables* (a term used frequently within the U.S. government) are neither the number of financial intelligence reports filed nor the politically popular but vague term of *disruption*. Rather, the metrics that matter are the number of arrests, convictions, and illicit money identified, seized, and forfeited. In other words, divide the trillions upon trillions that are being laundered by effective enforcement actions.

Despite periodic, positive, public pronouncements from the Department of the Treasury and various administrations, here are a few sobering numbers:

- According to the United Nations Office on Drugs and Crime (UNODC), less than 1 percent of global illicit financial flows are currently being seized and forfeited.[41]
- According to Raymond Baker, a longtime authority on financial crimes, using statistics provided by U.S. Treasury officials concerning the amount of dirty money coming into the United States and the portion caught by anti-money laundering enforcement efforts, the numbers show enforcement is successful 0.1 percent of the time and fails 99.9 percent of the time. "In other words, total failure is just a decimal point away," notes Mr. Baker.[42]
- Dated information suggests that, in the United States, money launderers face a less than 5 percent risk of conviction (some plead to lesser charges). Currently, there are about 700 money laundering convictions a year. That seems like a large number, but — divided into the amount of criminal activity — it is paltry. Besides, many convictions simply reflect additional counts added on against people charged with other crimes.[43]
- According to the U.S. State Department, the situation in most areas of the world is even worse.[44]

The Philippines has a large economy and is increasingly recognized as an important regional financial center. Since 2001, only 49 anti-money laundering cases have been filed. So far, of those 49 cases, there has not been a single successful prosecution or conviction.[45]

The British Virgin Islands is advertised as the world's leading offshore center[46] with more offshore companies than any other country. In 2014, there was one prosecution for money laundering.[47]

According to the Angolan Central Bank, approximately $17 billion has left the Angolan economy in the last five years alone — several orders of magnitude above foreign direct investment into the country. The origin of this money is unclear. Additional value is transferred out of the country through abusive trade misinvoicing. Widespread corruption in government and commerce facilitates money laundering. In 2015, there were not any prosecutions or convictions for money laundering.[48]

In Japan, the numbers of investigations, prosecutions, and convictions for money laundering are so low that they are not even publicly released.[49]

The list goes on and on. In fact, the State Department's 2016 International Narcotics Control Strategy Report[50], which tracks countries' anti-money laundering efforts around the world, reinforces this conclusion. While there are many positive developments, a comprehensive and objective reading of the report's statistics on prosecutions

and convictions is sobering. Ron Pol, a researcher on anti-money laundering measures, writes: "[Existing] anti-money laundering legislation is perhaps the least effective of any anti-crime measure, anywhere." [51]

If our current anti-money laundering countermeasures are "a decimal point away from total failure," isn't it time to introduce a new strategy and tactics?

VII. Policy Recommendations

We can do better. Here are a number of measures that could significantly improve U.S. anti-money laundering enforcement.

Congress

Congress Should Move Legislation to End the Abuse of Anonymous Shell Companies by Requiring Beneficial Ownership Transparency.

Anonymous U.S. shell companies are one of the top tools used by criminals, terrorists, kleptocrats, and tax evaders looking to conceal funds from law enforcement. A simple fix — requiring the real owner of a U.S. company to be named during the incorporation process — will cut down, in dramatic fashion, the ability of criminals to finance their crimes. This information should also be updated with authorities whenever beneficial ownership information changes.

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 Financial Action Task Force (FATF), a collection of more than 30 governments which sets international anti-money laundering (AML) standards. Worse yet, the United States uses one list for crimes committed in the U.S. 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. One of the significant loopholes that this would fix would be to make tax evasion a predicate offense for money laundering, bringing us in line with the international anti-money laundering standards set by FATF in 2012, which state that countries should ensure that "tax crimes" are predicate offenses.[52] 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.

Establish a Global Network of Trade Transparency Units (TTUs)

One key countermeasure for 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 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, trade-based money laundering (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 U.S.-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 $1 billion.[53]

Specific line item funding should be provided to the U.S. TTU so as to enhance its analytic capabilities and augment the personnel necessary to foster trade transparency in the United States and to expand the international TTU network.

Promote Usage of the Legal Entity Identifier (LEI)

The Legal Entity Identifier (LEI) is a unique 20-character code that identifies distinct legal entities that engage in financial transactions. The LEI is a global, non-proprietary identification system and freely accessible. Over 435,000 legal entities from more than 195 countries have now been issued LEIs. The LEI will be a linchpin for financial data — the first global and unique entity identifier enabling risk managers and regulators to identify parties to financial transactions instantly and precisely. And, as LEI is adopted, subsequent iterations of the program will begin linking beneficial ownership data to these unique identifiers, thus helping create transparency not only around company structures but around ownership structures as well. The widespread use of LEI will help provide financial transparency, accountability, and assist investigators in following the money trail. Currently, an international collaborative effort between public and private entities is developing the LEI, with the support of the Financial Stability Board (FSB) and the endorsement of the G-20. Legislation should be passed that requires U.S. companies that engage in financial transactions to obtain an LEI.[54]

Expand Due Diligence Obligations to Transactional Lawyers and Formation Agents

In December 2016, the Financial Action Task Force came out with its latest mutual evaluation report on the progress of the United States in meeting the FATF anti-money laundering and counter-terrorism financing standards. 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 U.S. AML regime. Second, it noted that lawyers, accountants, real estate agents and other significant professional service providers operating in the United States 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 United States should take the steps necessary to meet its FATF commitments.

Inter-Agency Recommendations

Develop an Updated Anti-Money Laundering Strategy

Following the completion of the U.S. Money Laundering Threat Assessment in 2005,[55] the U.S. government produced an inter-departmental National Anti-Money Laundering (AML) Strategy Report.[56] Ten years later, the U.S government completed a new money laundering risk assessment in 2015.[57] It should follow that threat assessment with an updated strategy to strengthen U.S. anti-money laundering enforcement efforts to counter threats to the financial system. Action items should be included in the report and Congress should hold the agencies, departments, and bureaus responsible if they fail to implement them. There was no accountability in the failure to implement action items in our last (2007) Anti-Money Laundering Strategy Report.

Adapt Crime Fighting Strategies to Cover Mobile Payments

Fewer criminals are carrying suitcases full of cash. And, while most still use traditional banks, increasingly, mobile payment systems are the money laundering vehicle of choice. These new and emerging financial structures have fewer rules, less transparency and greater flexibility to route and hide illicit funds.

The U.S. should convene an inter-agency anti-money laundering task force to develop specific recommendations on how to best address this growing threat to undermining enforcement of anti-money laundering laws.[58]

Require Beneficial Ownership Information from Government Contractors

The administration should require bidders for federal contracts and grants to publicly disclose their beneficial ownership information, as a means to ensure that fraudsters, criminals, and sanctioned individuals are not recipients of taxpayer money. This information should be publicly available for free in a machine-readable format, such as the Open Contracting Data Standards and operable across government-led initiatives on federal spending transparency.

Legal Entity Identifier in Procurement

In February 2016, the General Services Administration (GSA) issued a request for information to assess and replace the current identifier used to track and verify entities that receive federal funds. The administration has the authority to assign a unique entity identifier without any action from Congress. At a minimum, the administration should adopt the Legal Entity Identifier (LEI) — or a similar, non-proprietary and open system, that makes the hierarchy of entity ownership transparent — as a standard identifier in the procurement process by requiring bidders for federal contracts and grants to disclose both their LEI identification number and a list of their beneficial owners. A company's LEI should be included as a mandatory field in the GSA database for companies seeking to bid on federal contracts.

Treasury Department and the Financial Crimes Enforcement Network (FinCEN)

A FATF Recommendation on Trade-Based Money Laundering (TBML)

The international Financial Action Task Force recognizes that trade-based money laundering (TBML) is an enormous concern. In fact, FATF believes it is one of the three major global money laundering methodologies. However, in 2012, when the current FATF recommendations were reviewed, updated, and promulgated, TBML was not specifically addressed. The U.S. Department of the Treasury, which leads the U.S. FATF delegation,

should introduce a resolution calling for members to promote trade transparency in order to combat trade-based money laundering and value transfer.

Strengthen Due Diligence Requirements for Financial Institutions

FinCEN published a rule in May 2016 that requires U.S. financial institutions to collect what the rule describes as "beneficial ownership" information for legal entities opening new accounts. Unfortunately, the rule's definition of 'beneficial owner" does not comport with internationally recognized definitions, due to multiple loopholes and poor drafting. While the rule does require information to be provided about the people who directly or ultimately (through another level or more of corporate ownership) own shares in the corporate client, it only requires this information if someone owns a 25 percent or greater interest. If nobody owns that much of the company, then the bank does not need to identify any of the ultimate shareholders. In that case, the only person a bank has to list as a 'beneficial owner' is a senior manager of the corporate client, and a manager is simply not a beneficial owner as the term is otherwise internationally understood. The rule also allows a trustee to be named as the "beneficial owner" of a trust, even though trustees typically are not the true owner of the trust's assets. The result is that the rule's current definition of beneficial owner — and therefore the information a bank needs to collect about who owns or controls their corporate clients — is insufficient, not in compliance with international standards, and allows a bank to skirt 'know your customer' checks.

In addition, the bank does not have to incorporate the beneficial ownership information into its electronic records, it does not have to keep copies of information provided as verification that the people listed as beneficial owners exist, and the bank is permitted to legally rely on the information provided by the person from the company filling out the beneficial ownership form, even though the form only requires that they provide information "to the best of their knowledge," which may be very little or entirely inaccurate. The Treasury Department should instigate a new rule-making process to close these loopholes and improve the rule.

Initiate a New Money Services Business (MSBs) Registration Effort

In the late 1990s, a study sponsored by FinCEN estimated that there were over 200,000 Money Services Businesses (MSBs) in the United States., including businesses that cash checks, issue money orders, and execute wire transfers. After the September 11th attack and passage of the 2001 USA PATRIOT Act, MSBs were required to register with FinCEN and obtain licenses in the states in which they do business. However, according to the government's own data, the federal registration program has not been successful, with only about one-quarter of the estimated number of MSBs having registered with FinCEN. Moreover, not all states require licensing for companies which do not maintain a physical location in the state, and few states have made MSB licensing a priority. The resulting multiple gaps in federal and state registration and licensing data is of increasing concern, because approximately one-half of all suspicious activity reports (SARs) filed with FinCEN every year originate via MSBs. The tens of thousands of MSBs absent from the federal registration and state licensing processes include hawaladars, casas de cambio, and a myriad of informal money transfer services exploited by money launderers. The diversity and accessibility of the MSB sector also presents ongoing, grave challenges for effective oversight.

It is a federal offense to fail to register with FinCEN, to operate a money transmitting business in contravention of any applicable state licensing requirements, or to transport or transmit funds that are known to have been derived from a criminal offense or intended to be used to promote or support unlawful activity. The Internal

Revenue Service (IRS) is responsible for ensuring that MSBs register with FinCEN and for conducting AML/CFT compliance examinations, but it has neither the personnel nor the resources to fulfill those responsibilities.

The IRS should be given additional resources to carry out its MSB duties or it should delegate those duties to FinCEN, which should initiate a new, intensive MSB registration and oversight effort over the next two years. FinCEN should undertake an aggressive effort to identify unregistered or unlicensed MSBs and ensure they fulfill their registration and licensing requirements. FinCEN should also consider pre-empting state MSB licensing requirements by issuing a rule establishing uniform licensing requirements applicable to every MSB/money transmitter operating in the United States. Creating uniform, nationwide licensing standards and procedures would reduce the accumulative regulatory burden for inter-state MSBs while also providing a more uniform and efficient set of laws for money transmitters to follow.

Close Gatekeeper Loopholes

The following are recommendations for actions that FinCEN should take to close U.S. loopholes related to the gatekeepers of the financial system (also known as designated non-financial businesses and professions, or DNFBPs) that enable corrupt individuals and criminals to launder money through the U.S. financial system.

Finalize AML Requirements for Registered Investment Advisers

In 2015, FinCEN proposed a rule to require registered investment advisers to comply with anti-money laundering (AML) and suspicious activity reporting (SAR) requirements. FinCEN should finalize the proposed rule to impose anti-money laundering and suspicious activity reporting requirements on registered investment advisers.[59] The rule would apply to investment professionals for some of the largest financial players in the United States today, including hedge funds, private equity funds, trusts, foundations, and other pooled investment vehicles which collectively determine whether billions of dollars will enter the U.S. financial system, including offshore dollars from a variety of sources. While many U.S. investment advisers have voluntary AML and SAR reporting programs, none are currently subject to mandatory AML and SAR program requirements, despite their ongoing money laundering vulnerabilities. The absence of any legal obligation on the part of registered investment advisers to detect and prevent money laundering stands in stark contrast to the AML and SAR obligations of banks, securities firms, mutual funds, insurance companies, and other financial institutions operating in the United States.

Today, many investment advisers can accept funds from shell corporations and partnerships with hidden owners, conduct suspicious transactions with no questions asked, and witness highly suspect transactions with no obligation to report the activity to law enforcement. FinCEN should undertake to finalize the rule as soon as possible in order to close the current, glaring gap in AML protections safeguarding the U.S. financial system from abuse by terrorists, money launderers, and other criminals.

Re-Examine All Temporary AML Exemptions

FinCEN should also examine each of the temporary anti-money laundering (AML) exemptions now in existence, including for "seller[s] of vehicles, including automobiles, airplanes, and boats", persons involved with real estate closings, and "private bankers." to determine whether these exemptions are still warranted.

Department of Justice

Hold Individuals Accountable for Corporate Wrongdoing

U.S. law enforcement agencies should ensure that the top decision-makers at financial institutions, accounting firms, and law firms are held personally accountable for the actions of their organizations. In September 2015, the U.S. Department of Justice published a memorandum outlining steps it was taking to ensure that where corporate misconduct was identified, individuals responsible for the wrongdoing were also held accountable.[60] This important policy should be reaffirmed by the Attorney General and solidified by nominating to key posts in the Justice Department, such as the Deputy Attorney General, Assistant Attorney General (Criminal Division), Assistant Attorney General (Tax Division), and U.S. Attorney Offices, officials committed to bringing cases against individuals for white collar crime and strongly enforcing anti-money laundering and tax laws. Beyond criminal prosecution, regulators can also take action against individuals by requiring personnel changes, suspending or debarring them from regulated industries, or suspending or revoking their licenses to engage in certain types of business. Deterring corporate misconduct starts with individual accountability.

Change the Incentives for Law Enforcement

Law enforcement personnel at the federal, state, and local levels are rated and promoted, in large part, by the number of cases they make. Management of a given field office or police department is also rated in part by case statistics. Cases and publicity also influence budgets. Thus, it is only natural for law enforcement officers and their managers to prioritize shorter-term investigations. In other words, although not part of official policy, often the emphasis is put on comparatively simple cases and quick arrests that look good statistically but that do not have much of an impact on the entrenched criminal enterprises.

The incentives should be changed. Financial crimes investigators require specialized expertise and should be rewarded for it. Recognition (in many forms) should be given to those law enforcement officers that pursue the proceeds of crime — not the oftentimes straightforward predicate offense used to charge money laundering. Law enforcement personnel involved with complex financial crimes cases often cannot fairly compete via promotion boards against colleagues with good statistics covering straightforward criminal activity. This is an important reason why "impact cases" or headline grabbing financial crimes investigations that drive reforms have almost disappeared. Each department and agency has its own internal policies that govern promotion, but thought should be given to incentivizing meaningful financial crimes investigations.

Enhance AML/CFT Training

Criminal activity takes place at the local level. Yet, it is precisely at the state and local levels where law enforcement professionals have the least knowledge of money laundering and terror finance and their countermeasures. Many are unaware of common money laundering methodologies and investigative tools that are available. Local analysts and investigators cannot recognize suspicious financial and value transfer activities, if they do not recognize telltale indicators. The Department of Justice should provide specific funds for anti-money laundering/counter terror finance (AML/CFT) training to the 93 U.S. Attorneys' offices. Excellent training is also provided by the Bureau of Justice Assistance grants to the State and Local Ant-Terrorist Training (SLATT) initiative.

VII. Conclusion

Financial crimes are about the money. The need to convert "dirty" cash into clean, untraceable funds is central to the success or failure of criminal enterprises. As detailed above, we have not kept pace with the innovations in money laundering practices nor adopted updated strategies to effectively identify and catch the beneficiaries of illegal activity. As a result, we are, as has been stated, a decimal point away from complete failure.

At the same time, the amounts of money lost are staggeringly high and growing — fueled by secrecy and misaligned incentives. The cost of inaction is already too high.

The above reforms provide a roadmap for change and challenge the status quo. If we are serious about the safety and security of our communities and our nation, the integrity of our financial system and the resulting impact on the broader economy, then it is time to admit the failures of our past efforts and consider new and better approaches to combat illicit finance.

About the Author

John A. Cassara

John A. Cassara is a former U.S. intelligence officer and Treasury Special Agent. Mr. Cassara retired after a 26-year career in the federal government intelligence and law enforcement communities. He is considered an expert in anti-money laundering and counter-terrorist financing, with particular expertise in the areas of money laundering in the Middle East and the growing threat of alternative remittance systems and forms of trade-based money laundering and value transfer. He invented the concept of international "Trade Transparency Units," an innovative countermeasure to entrenched forms of trade-based money laundering and terrorist financing. A large part of his career was spent overseas. He is one of the very few to have been both a clandestine operations officer in the U.S. intelligence community and a Special Agent for the Department of the Treasury.

His last position was as a Special Agent detailee to the Department of the Treasury's Office of Terrorism Finance and Financial Intelligence (TFI). His parent Treasury agency was the Financial Crimes Enforcement Network (FinCEN), the U.S. Financial Intelligence Unit (FIU). He worked at FinCEN from 1996–2002. From 2002–2004, Mr. Cassara was detailed to the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL) Anti-Money Laundering Section to help coordinate U.S. inter-agency, international, anti-terrorist finance training and technical assistance efforts

During his law enforcement investigative career, Mr. Cassara conducted a large number of money laundering, fraud, intellectual property rights, smuggling, and diversion of weapons and high technology investigations in Africa, the Middle East, and Europe for a variety of federal agencies. While assigned to the Office of the Customs Attaché in Rome, Italy, he directed the first truly international anti-money laundering task force, called Operation Primo Passo, ("First Step"). The innovative operation combated Italian/American organized crime by examining the movement of money between the two countries and represented an early use of financial intelligence to proactively initiate investigations. During his customs career, he also served two years as an undercover arms dealer. He began his career with Treasury as a Special Agent assigned to the Washington Field Office of the U.S. Secret Service.

Since his retirement, he has lectured in the United States and around the world on a variety transnational crime issues. He is a consultant for government and industry. Mr. Cassara has authored or co-authored several articles and books, including *Hide and Seek, Intelligence, Law Enforcement and the Stalled War on Terrorist Finance* (2006 Potomac Books) and *On the Trail of Terror Finance - What Intelligence and Law Enforcement Officers Need to Know* (2010 Red Cell IG). In 2013, his first novel *was released - Demons of Gadara. Trade-Based Money Laundering: The Next Frontier in International Money Laundering* (Wiley) was released in November, 2015.

Further information – including specific recommendations on how to improve AML/CFT enforcement – is available at *www.JohnCassara.com.*

About the FACT Coalition

Who We Are

Founded in April 2011, the Financial Accountability and Corporate Transparency Coalition (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.[61]

Our Goals

- End the use of anonymous shell companies as vehicles for illicit activity;
- Strengthen, standardize, and enforce anti-money laundering laws;
- Require greater transparency from multinational corporations to promote informed tax policy;
- Ensure that the U.S. constructively engages in global financial transparency initiatives; and
- Eliminate loopholes that allow corporations and individuals to offshore income and avoid paying their fair share of taxes.

Why It Matters

There is untold wealth hidden in secrecy jurisdictions around the globe. The wealth-stripping from corrupt practices and regimes, illegal activity, and legal-but-ethically-bankrupt tax avoidance schemes is larger than most can possibly imagine. Because of the secret nature of the financial flows, it is impossible to know precisely the amount of money, but economist Gabriel Zucman estimates at least $7.6 trillion is in tax havens and secrecy jurisdictions.[62] The Boston Consulting Group estimates $11 trillion.[63] And the Tax Justice Network estimates between $21 and $32 trillion dollars.[64]

Roughly $2.5 trillion is currently stashed offshore by the 500 largest U.S. companies, costing American taxpayers more than $700 billion in unpaid taxes.[65] Indeed, the annual cost of offshore tax avoidance by *multinational companies* is $94 billion to $135 billion,[66] while overseas tax evasion by *individuals* drains an additional $40 billion to $70 billion each year from the American public.[67]

We seek a larger conversation about how specifically certain interests are manipulating the tax system and undermining our ability to act collectively to solve problems. The secrecy, in particular, allows certain entities to play by a different set of rules than the rest of us. Internationally, the secrecy facilitates corruption and impoverishes developing countries. In the U.S., we are complicit in the draining of wealth of other nations and fueling the austerity movement in our own.

Learn More

Interested in learning more about the FACT Coalition or becoming a member? Visit our website at thefactcoalition.org or contact Jacob Wills at jwills@thefactcoalition.org or +1 (202) 827-6401.

References

[1] Eduardo Porter, *Numbers Tell of Failure in Drug War*, The New York Times, July 3, 2012. http://www.nytimes.com/2012/07/04/business/in-rethinking-the-war-on-drugs-start-with-the-numbers.html

[2] Ibid.

[3] Cheryl Hall, *You won't believe the level of distrust that people have in everything, Edelman survey shows*, The Dallas Morning News, January 24, 2017. https://www.dallasnews.com/business/business/2017/01/24/trust-drops-power-people-grows-edelman-survey-shows

[4] Roger Cohen, *The Age of Distrust*, The New York Times, September 19, 2016. https://www.nytimes.com/2016/09/20/opinion/the-age-of-distrust.html

[5] John A. Cassara, *In fight against money laundering and terror finance, 'the emperor wears no clothes,* The Hill, August 24, 2016. Available here http://thehill.com/blogs/congress-blog/judicial/292479-in-fight-against-money-laundering-and-terror-finance-the-emperor

[6] Bruce Zagaris, *Tax cooperation and cross-border tax crime: Roles of international organization and potential roles for the United Nations*, United Nations Economic and Social Council, November 22, 2005. Available at http://www.un.org/esa/ffd/tax/firstsession/ffdtaxation-tax%20cooperation.doc

[7] Financial Action Task Force, *Money Laundering*, Financial Action Task Force, 2016. Available at http://www.fatf-gafi.org/faq/moneylaundering/

[8] Thomas Pietschmann and John Walker, *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes,* United Nations on Drugs and Crime, October, 2011. Available at http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

[9] Ibid.

[10] Ywfyouthvoice, *Explaining Concept of Panama Papers and Why It's a Big Deal*, Ywfyouthvoice, 2016. Available at http://www.ywfyouthvoice.com/2016/04/explaining-concept-of-panama-papers-and.html

[11] International Monetary Fund, Revisions to the Financial Action Task Force (FATF) Standard—Information Note to the Executive Board, International Monetary Fund, July 17, 2012. https://www.imf.org/external/np/pp/eng/2012/071712a.pdf

[12] James Henry, *The Price of Offshore Revisited*, Tax Justice Network, July 2012. Available at https://www.taxjustice.net/cms/upload/pdf/Price_of_Offshore_Revisited_120722.pdf

[13] Dev Kar and Joseph Spanjers, *Illicit Financial Flows from Developing Countries: 2004-2013*, Global Financial Integrity, December 2015. Available at http://www.gfintegrity.org/wp-content/uploads/2015/12/IFF-Update_2015-Final-1.pdf

[14] Spanjers, Joseph, and Dev Kar. *Illicit Financial Flows from Developing Countries: 2004-2013.* Report. December 8, 2015. http://www.gfintegrity.org/wp-content/uploads/2015/12/IFF-Update_2015-Final-1.pdf

[15] Friedrich Schneider with Dominik Enste, *Hiding in the Shadows The Growth of the Underground Economy*, International Monetary Fund, 2016. Available at https://www.imf.org/external/pubs/ft/issues/issues30/

[16] Fidel Bafilemba and Sasha Lezhnev, *Congo's Conflict Gold Rush: Bringing Gold into the Legal Trade in the Democratic Republic of the Congo,* Enough Project, April 21, 2015. Available at http://www.enoughproject.org/files/April%2029%202015%20Congo%20Conflict%20Gold%20Rush%20reduced.pdf

[17] International Labour Organisation, *International Labour Standards on Migrant workers*, International Labour Organisation, 2016. Available at http://ilo.org/global/standards/subjects-covered-by-international-labour-standards/migrant-workers/lang--en/index.htm

[18] *Schneider, Friedrich, PhD. "Out of the Shadows: Measuring Informal Economic Activity." December 2016. http://www.heritage.org/index/book/chapter-4.*

[19] The World Bank, *Developing Countries to Receive Over $410 Billion in Remittances in 2013*, Says World Bank, The World Bank, 2013. Available at http://www.worldbank.org/en/news/press-release/2013/10/02/developing-countries-remittances-2013-world-bank

[20] Michael Dimock, *Global Migration's Rapid Rise*, The Magazine of the Pew Charitable Trusts, July 5, 2016. http://magazine.pewtrusts.org/en/archive/trend-summer-2016/global-migrations-rapid-rise

[21] Dilip Ratha, *Remittances: Funds for the Folks Back Home*, International Monetary Fund, 2012. Available at http://www.imf.org/external/pubs/ft/fandd/basics/remitt.htm

[22] The United States Department of State, *National Terrorist Financing Risk Assessment 2015*, The United States Department of State. Available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

[23] Simon Rogers, *Where does the money go? Remittances around the world visualised*, The Guardian, February 5, 2013. Available at https://www.theguardian.com/news/datablog/2013/feb/05/remittances-around-world-visualised

[24] United States Department of State, *Money Laundering and Financial Crimes*, United States Department of State, March 1, 2001. Available at https://www.state.gov/j/inl/rls/nrcrpt/2000/959.htm

[25] Swanson, Ana. "*How secretive shell companies shape the U.S. real estate market*." The Washington Post, April 12, 2016. https://www.washingtonpost.com/news/wonk/wp/2016/04/12/how-secretive-shell-companies-shape-the-u-s-real-estate-market/?utm_term=.8a4558c1877b.

[26] Bloomberg, *China's Money Exodus*, Bloomberg, November 2, 2015. Available at https://www.bloomberg.com/news/features/2015-11-02/china-s-money-exodus

[27] Financial Action Task Force, *Money Laundering,* Financial Action Task Force, 2017. Available at http://www.fatf-gafi.org/faq/moneylaundering/

[28] Internal Revenue and Services, *Money Laundering,* Internal Revenue and Services, March 2, 2017. Available at https://www.irs.gov/uac/overview-money-laundering

[29] United States Department of the Treasury, *National Money Laundering Risk Assessment 2015,* United States Department of the Treasury. Available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

[30] Analysis given to the author by Dr. John Zdanowicz via June 30, 2015 email

[31] Ibid.

[32] Commissioner of the U.S. Customs Service, Raymond Kelly, *The Black Peso Money Laundering System,* PBS Frontline. Available at http://www.pbs.org/wgbh/pages/frontline/shows/drugs/special/blackpeso.html

[33] United States Department of the Treasury, *National Money Laundering Risk Assessment 2015,* United States Department of the Treasury, 2015. Available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

[34] United States Government Accountability Office, *Report to Congressional Committees, Defense Acquisition Assessments of Selected Weapon Programs*, United States Government Accountability Office, March, 2016. Available at http://www.gao.gov/assets/680/676281.pdf

[35] J.R. Helming, *The Fight to Counter Illicit Finance,* Leverage Outcomes, May 15,2014. Available at http://pkm.com/wp-content/uploads/2014/05/Leveraged-Outcomes_Illicit-Finance.pdf

[36] The Economist, *Shell companies: Launderers anonymous,* The Economist, September 22, 2012. Available at http://www.economist.com/node/21563286

[37] Tax Justice Network, *Financial Secrecy Index,* Tax Justice Network, 2015. http://www.financialsecrecyindex.com/

[38] Dennis M. Lormel, *It's time to pry criminals out of their shell (companies): Dennis M. Lormel,* Cleveland, August 16, 2013. Available at http://www.cleveland.com/opinion/index.ssf/2013/08/its_time_to_pry_criminals_out.html

[39] Patrick Fallon cited in, *Dirty Little Secrets,* Fusion, 2016. Available at http://interactive.fusion.net/dirty-little-secrets/

[40] Ibid.

[41] United Nations Office on Drugs and Crime, *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes,* United Nations Office on Drugs and Crime, 2011. Available at https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

[42] Raymond Baker, *Capitalism's Achilles Heel: Dirty Money and How to Renew the Free-Market System,* New Jersey: John Wiley & Sons, Inc, 2005.

[43] John A. Cassara, *Hide and Seek: Intelligence, Law Enforcement, and the Stalled War on Terrorist Finance,* Washington D.C: Potomac Books, Inc, 2005.

[44] John Chalmers and Karen Lema, *For bank heist hackers, the Philippines was a handy black hole, Reuters,* March, 21, 2016 Available at http://www.reuters.com/article/us-usa-fed-bangladesh-philippines-idUSKCN0WM13B

[45] The United States Department of State, *Countries/Jurisdictions of Primary Concern - British Virgin Islands,* The United States Department of State, 2015. Available at https://www.state.gov/j/inl/rls/nrcrpt/2015/vol2/239060.htm

[46] Sheroma Hodge-Philip, *BVI Is Ranked Highest Offshore Jurisdiction,* Global Financial Centres Index, April 8, 2015. http://www.bvi.gov.vg/media-centre/bvi-ranked-highest-offshore-jurisdiction

[47] Ricardo Soares De Oliveira, *Cash-rich Angola comes to cash-strapped Portugal,* Politico EU, October 2, 2015. Available at http://www.politico.eu/article/cash-rich-angola-comes-to-cash-strapped-portugal-colony-oil-santos-luanda-lisbon/

[48] The United States Department of State, *2010 International Narcotics Control Strategy Report (INCSR)--Volume II: Money Laundering and Financial Crimes Country Database--Indonesia through Mongolia,* The United States Department of State, 2010. Available at https://www.state.gov/j/inl/rls/nrcrpt/2010/database/141519.htm

[49] The United States Department of State, *2016 International Narcotics Control Strategy Report Volume II: Money Laundering and Financial Crimes,* The United States Department of State, 2016. Available at https://www.state.gov/j/inl/rls/nrcrpt/2016/vol2/

[50] The United States Department of State, *2016 International Narcotics Control Strategy Report,* The United States Department of State, 2016. Available at https://www.state.gov/j/inl/rls/nrcrpt/2016/

[51] Ron Pol cited in Hamish Fletcher, *Dirty cash: The fight against money laundering - should NZ do more?,* The New Zealand Herald, September 10, 2015. Available at http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11510931

[52] International Monetary Fund, Revisions to the Financial Action Task Force (FATF) Standard—Information Note to the Executive Board, International Monetary Fund, July 17, 2012. https://www.imf.org/external/np/pp/eng/2012/071712a.pdf

[53] Hector X. Colon, Unit Chief/Director TTU, as quoted in March 26, 2015 email with John A. Cassara.

[54] For additional information, see: https://www.leiroc.org

[55] U.S. Money Laundering Threat Assessment, December 2015, available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf

[56] The 2007 National Anti-Money Laundering Strategy Report is available here: https://www.justice.gov/sites/default/files/criminal-afmls/legacy/2011/05/12/mlstrategy07.pdf

[57] National Money Laundering Risk Assessment 2015, available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

[58] For additional information, see: http://financialservices.house.gov/uploadedfiles/hhrg-114-ba00-wstate-jcassara-20160623.pdf

[59] See: RIN 1506-AB10; Docket Number FINCEN-2014- 0003; available at https://www.regulations.gov/docket?D=FINCEN-2014-0003

[60] Individual Accountability for Corporate Wrongdoing, Memorandum from Deputy Attorney General Sally Q. Yates, September 9, 2015, https://www.justice.gov/dag/file/769036/download

[61] FACT Coalition. *Coalition Members and Supporters*. http://thefact.co/cNXgh (accessed August 1, 2016).

[62] Zucman, Gabriel. 2015. *The Hidden Wealth of Nations: The Scourge of Tax Havens*. Chicago, IL: University of Chicago Press.

[63] Patrick, Margot, and Simon Clark. "'Panama Papers' Puts Spotlight on Boom in Offshore Services." *The Wall Street Journal*, April 6, 2016 (accessible at http://on.wsj.com/1q5Nmk8).

[64] BBC News. *Tax Havens: Super-Rich 'Hiding' at Least $21tn.* July 22, 2012. http://www.bbc.com/news/business-18944097 (accessed August 1, 2016).

[65] Phillips, Richard, Matt Gardner, Kayla Kitson, Alexandria Robins, and Michelle Surka. "Offshore Shell Games 2016: The Use of Offshore Tax Havens by Fortune 500 Companies." Washington, DC: *Citizens for Tax Justice, Institute on Taxation and Economic Policy, and U.S. PIRG Education Fund*, October 2016 (accessible at http://ctj.org/pdf/offshoreshellgames2016.pdf). http://ctj.org/pdf/pre0316.pdf (accessed August 1, 2016).

[66] Merle, Renae. *U.S. companies are saving $100 billion a year by shifting profits overseas, report says.* The Washington Post. May 10, 2016. http://wpo.st/glwp1 (accessed August 1, 2016).

[67] Guttentag, Joseph, and Reuven Avi-Yonah. "Closing the International Tax Gap." In *Bridging the Tax Gap: Addressing the Crisis in Federal Tax Administration*, edited by M. B. Sawicky, 99-110. Washington, D.C.: Economic Policy Institute, 2006.

FACTCOALITION

1225 Eye St. NW, Suite 600 | Washington, DC | 20005 | USA
+1 (202) 827-6401 | @FACTCoalition | www.thefactcoalition.org

LETTER SUBMITTED BY THE FACT COALITION

August 3, 2017

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Marco Rubio
United States Senate
284 Russell Senate Office Building
Washington, DC 20510

RE: Corporate Transparency Act (S.1717)

Dear Senators Wyden and Rubio,

On behalf of the Financial Accountability and Corporate Transparency Coalition (FACT Coalition), we thank you for your leadership in sponsoring the **Corporate Transparency Act (S.1717)**. The 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.[1]

This bill would create new tools to effectively combat terrorism and financial crimes by ending the incorporation of anonymous companies in the United States. Specifically, this legislation would enable law enforcement to more effectively and efficiently conduct investigations, enhancing safety by saving time and resources in pursuing complex money laundering operations. Anonymous companies formed in the U.S. have been used for a wide range of dangerous and illicit activities, including as fronts for rogue countries to evade sanctions,[2] to cloak arms dealers shipping weapons into conflict zones,[3] to fuel the opioid crisis in communities across the country,[4] to engage in human trafficking,[5] to rip off Medicare,[6] and to undermine the safety of our troops through the sale of faulty equipment.[7]

---

[1] For a full list of FACT Coalition members, visit https://thefactcoalition.org/about/coalition-members-and-supporters/.

[2] Julie Satow, "Seizing Iran's Slice of Fifth Avenue," *The New York Times*, September 24, 2013, https://nyti.ms/2nEDDUI.

[3] *Global Witness*, "The Great Rip-Off," http://greatripoffmap.globalwitness.org/#!/case/57988.

[4] Nathan Proctor and Julia Ladics. "Anonymity Overdose: Ten Cases that Connect Opioid Trafficking and Related Money Laundering to Anonymous Shell Companies" *Fair Share Education Fund*, August 1, 2016, http://www.fairshareonline.org/sites/default/files/AnonymityOverdose_Aug1_2016.pdf.

[5] *Global Witness*, "The Great Rip-Off", http://greatripoffmap.globalwitness.org/#!/case/57938.

[6] Joseph Kraus and Stefanie Ostfeld. "A Bill to End Secrecy Surrounding Shell Companies," *The Hill*, February 03, 2016, http://thehill.com/blogs/congress-blog/economy-a-budget/265401-a-bill-to-end-secrecy-surrounding-shell-companies.

[7] *The United States Attorney's Office, Eastern District of Virginia*, "Former America's Most Wanted Fugitive sentenced to 105 years for leading international conspiracy to defraud the military," https://www.dodig.mil/IGInformation/IGInformationReleases/RogerDayPR.pdf.

1225 Eye St. NW, Suite 600 | Washington, DC | 20005 | USA
+1 (202) 827-6401 | @FACTCoalition | www.thefactcoalition.org

The increased accountability made possible by the bill would make it much harder for these criminals to hide behind shell companies to perpetrate schemes to defraud legitimate businesses, investors, or taxpayers.

Your bill comes at a critical time. There has never been more momentum behind the effort to end anonymous companies than there is right now. We look forward to continuing to work with you and your staff on this legislation so that we can end the abuse of anonymous companies.

For additional information, please contact Clark Gascoigne at cgascoigne@thefactcoalition.org or +1 (202) 810-1334. Thank you again for your commitment to this important issue.

Sincerely,

Gary Kalman
Executive Director
The FACT Coalition

Clark Gascoigne
Deputy Director
The FACT Coalition

cc The Honorable Mike Crapo
The Honorable Sherrod Brown
Members of the U.S. Senate Committee on Banking, Housing, and Urban Affairs

STATEMENT SUBMITTED BY THE INDEPENDENT COMMUNITY BANKERS OF AMERICA

January 9, 2017

BSA Modernization Can Strengthen Law Enforcement and Ease Compliance

On behalf of the more than 5,700 community banks represented by ICBA, we thank Chairman Crapo, Ranking Member Brown, and members of the Senate Banking Committee for convening today's hearing on "Combating Money Laundering and Other Forms of Illicit Finance: Opportunities to Reform and Strengthen BSA Enforcement." We appreciate you raising the profile of this important issue, and we are pleased to offer this statement for the record.

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. We believe there are opportunities to modernize and reform the Bank Secrecy Act (BSA) so that it produces more useful information for law enforcement while alleviating community banks' compliance burden. Community bankers have consistently cited BSA as one of the most significant sources of compliance burden. Below are our recommendations for BSA modernization.

Update Reporting Thresholds

As the government combats money laundering and terrorist financing, ICBA strongly recommends an emphasis on quality over quantity for all BSA reporting. In this regard, 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. A higher threshold would produce more targeted, useful information for law enforcement. Suspicious activity reporting is the cornerstone of the Bank Secrecy Act (BSA) system and is a way for banks to provide leads to law enforcement. However, in the current regulatory environment, community banks are faced with an overly burdensome process to ensure they are protected and no mistakes are made when reviewed by examiners. As a result, bank employees often file SARs as a defensive measure, and community banks follow the same SAR procedure for every suspicious transaction alert no matter how minor the potential offense. This approach leaves community banks skeptical that SARs have real value real law enforcement.

ICBA recommends reform of the SAR process to a risk-based system with appropriate threshold increases. Similar to the CTR thresholds, the SAR filing thresholds have not been adjusted since becoming effective. Increasing those thresholds would enable community banks to provide more targeted and valuable information to law enforcement.

Improve Flexibility and Ease of Compliance

ICBA supports FinCEN's efforts to simplify certain BSA forms and encourages the government to continue streamlining other reporting requirements. The federal government should continue working with the banking industry to provide additional guidance—such as best practices, questions and answers, or commentary—that is understandable, workable and easily applied by community banks. ICBA encourages FinCEN to continue its outreach, investigation and adaptation of technology to assist banks with their BSA compliance requirements. ICBA also encourages the Office of Foreign Asset Control to streamline and simplify its lists for ease of reference and

application by bankers.

To ensure a consistent and balanced effort to combat money laundering and terrorist financing, the federal government should have consistent regulations across all financial services providers including nonbank entities. Additionally, the government should require reporting of only truly suspect transactions—and strive to balance those requirements against the need to respect customer privacy.

Incentives for Anti-Money Laundering and Anti-Terrorist Financing Efforts

As the Financial Crimes Enforcement Network (FinCEN) identifies additional high-risk transactions and accounts, it increases banks' requirements in these new areas. 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 financial (e.g., a tax credit) or regulatory incentives to offset the cost of BSA compliance. We believe this would help compensate community banks for their BSA compliance and encourage further investments in this area.

Beneficial Ownership

Beneficial ownership information should be collected and verified at the time a legal entity is formed. 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. 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. If such information is housed at a government entity, community banks should have access to it.

Closing

Thank you again for convening today's hearing. ICBA looks forward to working with this Committee to modernize the Bank Secrecy Act in a way that will strengthen critical law enforcement while rationalizing community bank compliance with this important law.

LETTER SUBMITTED BY THE CREDIT UNION NATIONAL ASSOCIATION

Credit Union National Association
CUNA

Jim Nussle
President & CEO

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

601 Pennsylvania Avenue NW
South Building, Suite 600
Washington, D.C. 20004-2601

January 9, 2018

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing
and Urban Affairs
United States Senate
Washington, DC20510

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 America's credit unions, thank you for holding the hearing entitled "Combatting Money Laundering and other Forms of Illicit Finance: Opportunities to Reform and Strengthen BSA Enforcement." The Credit Union National Association (CUNA) represents America's credit unions and their 110 million members.

Since the 2008 economic crisis and the resulting regulations that followed, credit unions have been required to devote more resources for regulatory and legal compliance particularly for mortgage loans and other consumer products, services, and protections. Given these new requirements, it has become difficult for credit unions to absorb their current total compliance burden. The new regulatory regime makes the Bank Secrecy Act (BSA)[1] and Anti-Money Laundering (AML) regulatory compliance even more daunting.[2]

We support efforts to track money laundering and terrorist financing, but also believe it is important to strike the right balance between the costs to financial institutions, like credit unions, and the benefits to the federal government from the BSA, AML, and Office of Foreign Assets Control (OFAC) regulations. As such, we support legislative and regulatory changes to address the redundancies, unnecessary burdens, and opportunities for efficiencies within the BSA/AML statutory framework. In particular, we support changes to (1) minimize the duplication of the same or similar information; (2) provide additional flexibility based on the reporting institution type or level of transactions; (3) curtail the continually enhanced customer due diligence requirements; (4) increase the currency transaction reporting (CTR) threshold; (5) reduce and simplify the reporting requirements of Suspicious Activity Reports (SARs) that have limited usefulness to law enforcement; and (6) allow for greater regulatory and examination consistency among regulators, including the National Credit Union Administration (NCUA) and state credit union regulators, in order to help with interpretations of BSA requirements and guidance and to minimize regulatory overlap.

BSA regulations, administered by FinCEN, are the foundation of all efforts by our government to stop criminal money laundering and terrorist financing. These have been strengthened through AML laws, which include part of the USA PATRIOT Act. These laws require financial institutions such as banks, credit unions, and non-depository financial institutions to keep records of events that could signal money laundering and terrorist financing. BSA/AML regulations require financial institutions to maintain records on cash sales of negotiable instruments of $3,000 - $10,000 and records of wire transfers of $3,000 or more, and to report cash transactions over $10,000 and any suspicious activity above a $5,000 threshold that might show money laundering, tax evasion, or another type of crime. The forms used by credit unions to report transactions are the Currency Transaction Report (CTR)[3] and the Suspicious Activity Report (SAR).[4] In addition, BSA requires the verification of member identity and response to the 314a information request lists provided by FinCEN. When financial

institutions fail to comply with these laws and regulations, they are subject to significant civil money penalties and risk damage to their reputation.

The reality is the cost of technology for monitoring and ensuring compliance with BSA/AML laws and regulations is disproportionately burdensome on smaller and less complex institutions, such as credit unions. Often, credit unions choose not to serve certain markets because of the complexities of compliance. Money Service Businesses are a prime example of where many credit unions have difficulty providing needed services because of the BSA and AML ongoing due diligence requirements associated with serving these businesses. Nevertheless, our government can ease the compliance burden for smaller or less complex financial institutions, such as credit unions, while maintaining the protections needed. The following technical changes would make a major difference in the compliance burden facing credit unions on these requirements.

SAR and CTR Forms Should Be Combined

It would be helpful to the industry if the SAR and CTR forms – the two forms used for reporting – were combined into one form and submitted to the same place. This form should be streamlined and consolidated so the same information can be populated for either form, or the form can simultaneously be used for either SAR or CTR (for example, with a check box on the form to specify for which report, CTR or SAR, the information is being provided). This minor change in paperwork would greatly ease compliance burden and ensure mistakes are not made during reporting, without compromising efforts to identify criminal activity.

Reporting Thresholds and Deadline to File Should Be Increased to Reflect Today's Environment

The threshold for a CTR has not been adjusted in many years for inflation. Credit unions support an adjustment to this $10,000 threshold to account for inflation and economic change over the past several years. This current amount was established in 1972, and would be over $58,400 if adjusted for inflation in today's world.[5] Furthermore, the current relatively low limit is now capturing routine cash transactions that are not necessary to report since such transactions will be reported via the SAR if there is suspicious activity. Credit unions support increasing the CTR threshold to a minimum $20,000 amount and at least doubling other key thresholds, such as the $5,000 threshold for filing a SAR.

Additionally, the deadline to file a SAR should be extended from 30 days to 40 days for more complex cases. The more complex the case, the longer it takes to research the facts, which places substantial pressure on the credit union to timely file a SAR.

"Beneficial Owner" and Beneficiaries Requirements

FinCEN finalized its beneficial ownership rule, which would extend Customer Due Diligence (CDD) requirements under BSA rules to the natural persons behind a legal entity, and require financial institutions to have risk-based procedures for conducting ongoing customer due diligence. The final rule creates a new § 1010.230 in Title 31 C.F.R. to require covered financial institutions to identify and verify the identity of beneficial owners of legal entity customers when a new account is opened, and conduct risk profiles and monitoring of customers. The requirements for identifying the true beneficial owner of various entities, which is effective on May 11, 2018, place an enormous burden on credit unions.

In addition, checking payable-on-death (POD) account beneficiaries against the OFAC list should only be required to occur if payout to the beneficiary is necessary. Payable-on-death beneficiaries do not have access to or control of the account in question, and may never have access, so there is no need to continually check them until they receive this access and control. Information on the beneficiaries is often not available for accurate checks because usually only the name of a beneficiary is collected, making this work difficult and time consuming to conduct. The OFAC checks are a substantial compliance burden and would be easier for institutions to conduct when ownership of the funds occurs. Again, this change would in no way limit efforts to prevent criminal activity.

Monetary Instrument Purchases

Under 31 C.F.R. § 1010.415, banks and credit unions are required to verify the identity of persons purchasing monetary instruments for currency in amounts between $3,000.00 and $10,000.00, and maintain documentation of such transactions. The requirement to maintain a separate documentation for these transactions is antiquated given today's systems that track every transaction that occurs in a financial institution. A credit union can trace any transaction on its core system if it is needed by law enforcement. Therefore, the separate documentation requirement should be eliminated.

Zero Tolerance for Unintentional Non-Compliance Should Be Reconsidered

The zero tolerance for non-compliance should be loosened so unintentional errors on SARs or CTRs, which can be complex and confusing to complete depending on the situation, do not result in an unfair penalty or violation in a supervisory examination. Intentional noncompliance or a pattern of negligence with the essential and substantive requirements should be subject to zero tolerance, but the occasional clerical error, such as failing to check a box on a complex form, should be afforded more leniency. In the current regulatory environment, even a substantially minor error, such as recording a P.O. Box as an address instead of a street address, can lead to a Document of Resolution (DOR) for the institution for non-compliance. If there is more than one error, for one or more consumers, the DOR by the financial regulator could be for a "systemic" violation, which would garner increased attention and be considered a greater violation. In today's complex regulatory environment, federal and state examiners are particularly conservative and will report institutions for a systemic violation even if only two similar errors were made. This reality increases the compliance burden for credit unions to conduct more checks than likely necessary and spend more resources on quality control. Furthermore, because the safe harbor for compliance only applies when a SAR is filed, credit unions tend to err on the side of caution and file a SAR even though law enforcement officials tell them not to file unless necessary. Finally, another reason why the burden is high for BSA/AML compliance is because now BSA officers can be held personally liable and be required to pay high civil money penalties out of their own pocket if they do not have a solid BSA/AML Program, as seen in some recent court cases. The penalties can be harsh and daunting, and can prevent individuals from becoming BSA officers or make these officers too expensive to hire.

Conclusion

Credit unions take compliance seriously and dedicate significant resources to it. However, when credit unions are spending their limited resources disproportionately on compliance, this means they are spending fewer resources on innovating and providing safe and affordable products and services. We recognize that regulatory agencies –whether it be the NCUA, the Consumer Financial Protection Bureau (CFPB), or bank regulators – have a renewed focus on BSA/AML compliance, particularly on issues such as cybersecurity and mobile payments. However, we encourage a regulatory regime that will recognize the time and effort that goes into good faith compliance with laws, and does not unduly punish financial institutions for unintentional technical or minor errors. The seemingly never-ending stream of regulatory

expectations for credit unions, often with small and stretched staffs, must be considered in agency examinations and when laws and requirements are enacted.

Thank you again for the opportunity to be a part of this process. We take our role in the credit union movement, and as part of the financial services industry, seriously. We believe we have an obligation to protect our members and the financial community from fraud and crime, and there can always be more that should be done. However, credit unions are first and foremost in the financial services business, and do not have the infrastructure for law enforcement. This is the reality they struggle with every day. The tough question that lawmakers must grapple with is how to balance the need for protection with the burden placed on financial institutions and consumers who ultimately pay the cost. The credit union industry is open to working with the government to protect against crime, and we look forward to being a resource as you develop processes and requirements that are streamlined and more manageable.

On behalf of America's credit unions and their 110 million members, thank you for your consideration of our views.

Sincerely,

Jim Nussle
President & CEO