S. HRG. 115–212

COMBATING MONEY LAUNDERING AND OTHER FORMS OF ILLICIT FINANCE: ADMINISTRATION PERSPECTIVES ON REFORMING AND STRENGTHENING 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 WAYS TO MODERNIZE THE UNITED STATES' ANTI-MONEY LAUNDERING AND COUNTERTERRORIST FINANCING REGIME AND EXPLORING WAYS TO STRENGTHEN THE ENFORCEMENT AND INTEGRITY OF THE U.S. FINANCIAL SYSTEM IN A NEW TECHNOLOGICAL ERA

JANUARY 17, 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

29–913 PDF WASHINGTON : 2019

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama	SHERROD BROWN, Ohio
BOB CORKER, Tennessee	JACK REED, Rhode Island
PATRICK J. TOOMEY, Pennsylvania	ROBERT MENENDEZ, New Jersey
DEAN HELLER, Nevada	JON TESTER, Montana
TIM SCOTT, South Carolina	MARK R. WARNER, Virginia
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts
TOM COTTON, Arkansas	HEIDI HEITKAMP, North Dakota
MIKE ROUNDS, South Dakota	JOE DONNELLY, Indiana
DAVID PERDUE, Georgia	BRIAN SCHATZ, Hawaii
THOM TILLIS, North Carolina	CHRIS VAN HOLLEN, Maryland
JOHN KENNEDY, Louisiana	CATHERINE CORTEZ MASTO, Nevada
JERRY MORAN, Kansas	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*
JAMES GUILIANO, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

C O N T E N T S

WEDNESDAY, JANUARY 17, 2018

WITNESSES

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

COMBATING MONEY LAUNDERING AND OTHER FORMS OF ILLICIT FINANCE: ADMINISTRATION PERSPECTIVES ON REFORMING AND STRENGTHENING BANK SECRECY ACT ENFORCEMENT

WEDNESDAY, JANUARY 17, 2018

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

The Committee met at 10:10 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. The hearing will come to order.

This morning, the Committee will receive testimony from Treasury and Justice Department witnesses on the potential for modernization of the United States anti-money laundering and counterterrorist financing regime. We look forward to hearing the Government's views on strengthening enforcement and protecting the integrity of the U.S. financial system in a new technological era.

The Committee held a hearing with industry stakeholders on this same topic last week. A clear bipartisan interest in modernizing the BSA/AML regime emerged from that hearing.

The hearing highlighted significant interest in several areas: beneficial ownership, information sharing, technology, and BSA reporting requirements. The hearing also highlighted the need to work with bank examiners to ensure that AML compliance is not just a "check-the-box" exercise.

There seems to be space to improve information and coordination between industry, regulators, and law enforcement. The breadth of each of these areas merit further consideration and discussion.

For example, today's technology promises new ways to catch criminals and facilitate compliance. But technology also poses challenges for law enforcement, such as the rise of cryptocurrencies and their potential to facilitate sanctions evasion and perhaps other crimes.

I appreciate the strong interest in this topic from my Banking Committee colleagues and others in the Senate. As this Committee looks deeper into the potential for reforms or modernization of the broader U.S. counter threat financing space, all stakeholders' interests must be critically examined to assure that financial institutions, among a myriad of other stakeholders, can work effectively

with the Government to efficiently provide information that results in a "high degree of usefulness" to combat crime and terrorism.

The Committee, in doing its work on this shared policy goal, must also be ever mindful of the potential for creating any new or different set of unintended consequences that may lead to inefficiencies and undue burdens.

Clearly, the United States cannot afford to allow criminals and terrorists to move illicit funds in furtherance of their criminal objectives.

At the same time, during last week's hearing, Mr. Baer shared an example of a community banker with a $100 million bank and three branches. This bank had seven AML compliance officers and only four lending officers. We cannot let AML compliance weigh disproportionately on the costs of community banks.

I look forward to working with my colleagues in helping to find a bipartisan path forward to a modernized, reformed BSA/AML regime that works for law enforcement, industry, and other stakeholders.

Under Secretary Mandelker and Mr. Day, I am eager to hear your thoughts today. Your testimony will help set the stage for taking BSA/AML compliance and enforcement into the future.

Senator Brown.

STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Thank you, Mr. Chairman, and we both welcome Senator Moran to the Committee. Welcome, Jerry. Nice to see you. The Chairman appropriately introduced you earlier.

Senator MORAN. I can almost see you from here.

[Laughter.]

Chairman CRAPO. Patience.

Senator BROWN. Thanks for calling this important hearing as a follow-up to our session last week as we begin to consider ideas to strengthen and reform our money-laundering and illicit finance laws.

I am pleased that today we will hear Administration views, including from Treasury Under Secretary for Terrorism and Financial Intelligence Mandelker, welcome, and Deputy Assistant Attorney General Day from the Criminal Division, welcome. They will both, I am sure, provide important law enforcement and counter-terrorism perspectives.

As I noted last week, we should keep in mind that we are operating against a backdrop where in recent years some of the world's largest banks and their foreign partners continue to run afoul of these laws. In some cases they had inadequate anti-money-laundering oversight and compliance regimes. In others, banks willfully and persistently violated U.S. bank secrecy, sanctions, and anti-corruption laws.

Though some have tried to minimize them, these were not simply paperwork missteps or administrative errors. In fact, the GAO concluded last year that over recent 6 years, approximately $12 billion was collected in fines, penalties, and forfeitures from financial institutions for violations of the Bank Secrecy Act, the Foreign Corrupt Practices Act, and the U.S. sanctions requirements—including $5 billion specifically assessed for Bank Secrecy Act violations.

Some of these banks violated U.S. anti-money-laundering and sanctions laws by knowingly facilitating illegal financial transactions for rogue regimes in Iran and Sudan and Libya and Syria and Burma, and in some cases for trying to conceal this activity by repeatedly stripping relevant information from transaction records. Some conducted transactions with individuals or entities affiliated with terrorist organizations and drug cartels directly in violation of U.S. law. Many violated the law for several years. I encourage my colleagues to read a sampling of these Deferred Prosecution Agreements on these banks; some will make your hair stand on end.

These are not victimless crimes. In addition to strengthening, for example, interdiction of the supply of drugs like fentanyl coming into the country through initiatives like my INTERDICT Act signed into law by the President last week, we also must cutoff the traffickers' money supply. Money laundering on behalf of drug cartels has a direct line to the opioid epidemic in my State, where Sinaloa cartel actors have been active, destroying thousands of families. Eleven people a day, more than any other State, die in my State. Every single day 11 people die.

Human traffickers exploiting the misery of runaways here or recruiting young women from overseas with promises of legitimate work in the United States use our financial system to launder their profits.

That is why these laws are so critical: they protect the integrity of our financial system; they provide critical intelligence to law enforcement to combat crime.

Even so, as last week's hearing made clear, we want to assess whether there are ways to responsibly update and strengthen the current anti-money-laundering framework, including through new measures to require beneficial ownership information when companies are formed in the United States, shedding once and for all the U.S. reputation for being a haven for anonymous shell companies. That must end.

Broadening information sharing may make sense, but there were good reasons that such sharing was limited to terrorism and money-laundering cases after 9/11. Important questions about privacy protections must be answered before considering any expansion.

And as we heard from witnesses last week, we should focus on sharpening suspicious activity reporting and bolstering efforts by law enforcement to give banks better guidance on what to look for, instead of on substantially raising currency reporting thresholds. Questions have been raised, including on how to enable banks to make better use of artificial intelligence, while retaining room for critical human judgments.

I know today's two distinguished Government witnesses have thought deeply for years about these issues. We welcome you both and look forward to hearing your perspectives.

Thank you.

Chairman CRAPO. Thank you, Senator Brown.

First, we will receive testimony from the Honorable Sigal Mandelker, who is the Under Secretary for Terrorism and Financial Crimes at the U.S. Department of Treasury. Following her, we will hear from Mr. Kendall Day, who is the Acting Deputy

Assistant Attorney General for the Criminal Division of the U.S. Department of Justice.

Under Secretary Mandelker, you may please proceed. I do remind the witnesses to try to follow the 5-minute clock that you have in front of you so we have time for questions and to remind our Senators to follow your own 5-minute clocks when it is time for your questions.

Please proceed.

STATEMENT OF SIGAL MANDELKER, UNDER SECRETARY, TERRORISM AND FINANCIAL INTELLIGENCE, DEPARTMENT OF THE TREASURY

Ms. MANDELKER. Thank you. Thank you, Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee. As the Under Secretary for Treasury's Office of Terrorism and Financial Intelligence, I am honored to once again appear before you today to discuss the critical work that we at TFI are doing to safeguard the United States and international financial systems.

The offices that I lead are tasked, as you know, with using our financial intelligence, expertise, and powerful economic authorities to combat terrorist financing, money laundering, weapons proliferators, rogue regimes, human rights abusers, cyber criminals, and other illicit finance and national security threats to the United States and in the international financial system to our allies.

TFI is actually the only office in the world that houses these unique authorities under one roof, and we are proactively integrating our authorities and expertise across components, deploying the best tools suited to each challenge and achieving significant impact.

The foundation of our economic authorities is a strong and robust anti-money-laundering/combating the financing of terrorism regime, and one of my top priorities as Under Secretary is to ensure that the AML/CFT framework remains strong and effective. Such a regime keeps illicit actors out of the financial system and allows us to track and target those who try to slip through. And that is exactly what we have been doing against a wide array of law enforcement and national security priorities.

Just as an example, we have been laser-focused on using our unique economic tools to identify and disrupt North Korea's use of covert representatives as well as front and trade companies to disguise, move, and launder funds that finance its weapons programs.

We are also targeting Iran's use of deceptive financial practices to generate revenue. As just one example, in November, we sanctioned an IRGC Quds Force network involved in a large-scale scheme to counterfeit bank notes to support its destabilizing activities.

In the past year, we have imposed sanctions, issued financial advisories, and undertaken diplomatic engagements to counter human rights abusers and the corrupt across the globe. Just last month, we sanctioned human rights abusers and corrupt actors under an Executive order that builds on the Global Magnitsky Act, which was passed by Congress just over 1 year ago.

We are also using our other economic tools and authorities, such as using geographic targeting orders and exercising other authorities against transnational criminal organizations, cyber criminals, human-trafficking networks, and other law enforcement priorities. And we are taking a hard look, as you are, at the Bank Secrecy Act and the broader AML/CFT regime.

We need to continuously upgrade and modernize our system, which was a statutory and regulatory construct that was originally adopted in the 1970s, and make sure that we have the right framework in place to take us into the 2030s and beyond.

In particular, we have to make sure that financial institutions are devoting their resources toward high-value activities and are encouraged to innovate with new technologies and approaches so that we in law enforcement are able to better address these threats. And we are working closely with our law enforcement and regulatory partners in this effort.

In recent years, financial institutions have been more proactive in their AML/CFT efforts, building sophisticated internal financial intelligence units, improving their ability to identify customers and monitor transactions by experimenting with new technologies, and working together to share information. We think these are good developments. These initiatives advance the BSA's underlying purpose and have been instrumental in assisting our efforts to identify and disrupt key streams of financing by illicit actors, including just as an example North Korea.

We have also been working with the financial community to understand their perspectives and achieve our shared objectives. They are on the front lines, detecting and blocking illicit financing streams, combating financial crimes, and managing risk.

Deploying our tools for maximum impact also requires proactive dialogue and information sharing with financial institutions. Enhancing public-private partnerships that reveal and mitigate vulnerabilities is a top priority of ours. That is why last month we launched FinCEN Exchange, a new public-private information-sharing program led by FinCEN.

FinCEN Exchange is bringing law enforcement, financial institutions, and FinCEN together to facilitate greater information sharing between the public and private sectors on issues like cases, typologies, and threats. This effort enables the private sector to better identify risks and provides FinCEN and law enforcement with critical information to disrupt money laundering and other financial crimes.

I want to thank the Committee for its leadership and support, both of which are truly essential to combating the threats that we face and ensuring our continued success. I look forward to working with this Committee on AML/CFT improvements and with other Members of Congress as we seek to fulfill our shared responsibilities to keep Americans safe and secure.

Chairman CRAPO. Thank you.

Mr. Day.

STATEMENT OF M. KENDALL DAY, ACTING DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Mr. DAY. Thank you, Senator. Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you for the opportunity to discuss our Nation's anti-money-laundering laws, including the Bank Secrecy Act.

The Department of Justice draws upon the resources and expertise of various components to combat money laundering, including the Criminal Division's money-laundering and asset recovery section, the U.S. Attorneys' Offices, the Federal Bureau of Investigation, the Drug Enforcement Administration, and other prosecution and investigating components and agencies. We work with partners across the country and around the globe to pursue complex, sensitive, multi-district, and international money-laundering and asset recovery investigations and cases. We devote significant resources to this problem because money laundering facilitates some of the most serious and significant threats to our security and our safety.

Transnational criminal organizations, kleptocrats, cyber criminal groups, terrorists, drug cartels, and alien smugglers alike must find ways to disguise and use their illicit proceeds. Money laundering, which best estimates peg at more than $2 trillion annually, is a global problem, but the threat it poses to the United States is acute and specific. Here we enjoy some of the deepest, most liquid, and most stable markets in the world. Those features of the U.S. financial system attract legitimate trade and investment, foster economic development, and promote confidence in our markets and in our Government. Those advantages—transparency, liquidity, and stability—also attract criminals. Through vigorous anti-money-laundering enforcement, we protect those hallmarks of our financial system, and we safeguard our citizens from the harms wrought by the underlying criminal conduct.

Unfortunately, however, criminals frequently seek to thwart or evade our efforts by exploiting gaps and vulnerabilities in the existing laws and regulations. As you are aware, the pervasive use of front companies, shell companies, nominees, and other means to conceal the beneficial owners of assets is one of the great loopholes in this country's anti-money-laundering regime. We constantly see bad actors using these entities to disguise the ownership of the dirty money they derive from their criminal activities.

The Bank Secrecy Act imposes a range of obligations on financial institutions, including reporting suspicious activity, performing customer due diligence, preventing transactions that involve the proceeds of criminal activity, and establishing effective anti-money-laundering programs. These requirements play a critical role in law enforcement's fight against money laundering. Effectively, they mean that financial institutions are often the front line of our Nation's efforts to prevent and detect such activity. Ensuring the ability of financial institutions to detect, investigate, and report illicit financial activity is of critical importance to law enforcement and the U.S. Government's fight to combat money laundering and prevent terrorist financing.

Compliance with the Bank Secrecy Act is fundamental to protecting the security of financial institutions and the integrity of the

financial system as a whole. In most cases financial institutions seek to do the right thing, implementing effective anti-money-laundering programs to detect and prevent money laundering through the U.S. financial system. In some cases, however, financial institutions have willfully failed to implement effective anti-money-laundering programs or failed to document suspicious transactions. In recent years the Department of Justice has resolved numerous anti-money-laundering and sanctions-based violations with major financial institutions, demonstrating that those institutions still struggle to create and incentivize anti-money-laundering and sanctions compliance programs.

The effectiveness of our current anti-money-laundering regime merits continued discussion among law enforcement, industry, and Congress as we strive to detect, target, and disrupt illicit financial networks that threaten our country. I am pleased to be with you talking about these important issues, and I thank the Committee for holding this hearing today to bring attention to the threat that money laundering poses to our financial system and our national security.

I will be pleased to take the Committee's questions. Thank you very much.

Chairman CRAPO. Thank you to both of you.

My first question is just to ask each of you to very briefly, if you could, tell me if there are reforms to our system that are gaining attention in your offices, of things in your office or in your work that you and your colleagues believe need to be fixed or changed. Ms. Mandelker?

Ms. MANDELKER. Thank you, Mr. Chairman. So what I can tell you is there are reforms and then there are actions that we can take independent of any legislative reforms, such as——

Chairman CRAPO. Yes, and I am referring to legislative fixes.

Ms. MANDELKER. Understood. So I do think that this is a very important time to take a look at the BSA framework that was stood up again in the 1970s. We have to look to see whether or not our reporting requirements are sufficiently meeting our needs. We have to look to make sure that we have a system in place that is harnessing all those financial crimes analysts that are sitting in the financial institutions and are very much on the front lines of what we are trying to accomplish through their reporting.

So we are taking a very hard look at that framework. We are looking at the thresholds. We are looking at the examination process. I think it is very important to study these issues carefully, to engage in conversations with law enforcement about what has been useful to them, what has been most useful, what has not been as useful so that we are getting the information that we need from the financial institutions in the right way, in the right form, and also so that we are incentivizing the financial institutions to prioritize work that is of high value to us.

I know that there was a lot of discussion, just as an example, about the examination process, so we need to take a look at the examination process and make sure, again, that it is tailored toward incentivizing the banks to do the difficult work of analyzing potential illicit activity in a way that is going to be more productive for us.

Chairman CRAPO. Rather than checking the box.

Ms. MANDELKER. That is right.

Chairman CRAPO. Thank you. Mr. Day?

Mr. DAY. Thank you, Chairman. I think in addition to the issues that Under Secretary Mandelker mentioned, I would like to flag beneficial ownership. That is an issue that continues to present challenges for law enforcement because it is no secret that one of the ways criminals try to obscure their conduct is by hiding behind shell companies and front companies.

Law enforcement has to devote enormous resources and time to piercing the corporate veil and amassing the evidence necessary to figure out who stands behind these companies and who is actually benefiting from the illicit financial flows. So that is another area that I think is ripe for consideration legislatively.

Chairman CRAPO. Well, thank you. And I appreciated the written testimony you both provided, and we will look forward to further information from you on helping to achieve these objectives as we move forward with legislative efforts here.

Back to something that you both referenced, there was a lot of discussion in our last hearing about this check-the-box notion, that we have an army of analysts out there, but the question that seemed to come through to me in the last hearing, or one of them was: Are they just, you know, mathematically looking at numbers and checking boxes as they report transactions? Or are they trying to analytically identify what is risky or dangerous behavior and help you find that? Could you both address the—do you see the objective that we want to get at and the objective we want to avoid? Could you address that for me?

Ms. MANDELKER. I want to just start by saying that we have a cadre of examiners that we work with that are in the Federal banking agencies that are, of course, very devoted and dedicated to make sure that financial institutions are complying with their AML/CFT obligations.

At the same time, I think that now is a very good opportunity to have a discussion with the Federal banking agencies that are conducting these exams to make sure that they are understanding what our priorities are from the Treasury Department, from law enforcement, to make sure that we are incentivizing financial institutions in the right way to devote their very substantial resources toward the high-value threats, toward identifying AML/CFT risks.

And so I have begun that process. We are discussing this very issue with the Federal banking agencies, and you will be hearing more from us on that front. I think this is a very important time to have that conversation.

Mr. DAY. Thank you, Mr. Chairman. I will say that the information we get from the existing regime is very helpful to law enforcement. Our job fundamentally is all about identifying crimes, catching criminals, putting them in jail. And we often initiate investigations based on that reporting as well as, if we have a preexisting investigation that started with other information, further an investigation with the intelligence we are able to glean from that reporting.

So I think that is very true, there is opportunity to consider this issue. It is just it should be done with an eye toward preserving what is already good about the system.

Chairman CRAPO. Thank you.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

Secretary Mandelker, let me start with you. I am sure you are familiar with the recent Clearing House Association report on these issues. One Clearing House recommendation is to have FinCEN's BSA oversight authority over large banks 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.

My questions are these, connected to that: Do you know what this change would require in terms of additional Federal funding and personnel? Why would we redo a system, an oversight system, that has worked reasonably well and put in place the kind of centralized examination teams suggested by the Clearing House when bank examiners already have extensive expertise and experience with these large entities on BSA issues and have been doing this job successfully for years? Tell us what you think.

Ms. MANDELKER. So I cannot tell you exactly what the numbers would look like if that authority—if we were to take back that authority. What I can tell you is that it is, again, very important, as we are with our partners charged with safeguarding the financial system, it is very important that we have continued conversations with the Federal banking agencies, with those examiners, so that they understand what law enforcement's priorities are and so that we continue to have an active discussion about how they are executing those responsibilities. So that is where our focus is, and, of course, we also have responsibility not just with respect to banks, but we have other responsibilities when it comes to executing our oversight responsibilities with money service businesses, in the virtual currency space, among a wide variety of areas. So we are very mindful of how we allocate our resources to make sure that we are not undertaking duplicative efforts.

Senator BROWN. Thank you.

Mr. Day, as recently as last September, in its quarterly report to the court on HSBC's Deferred Prosecution Agreement, which stemmed from the bank's unlawful moving of hundreds of millions of dollars for Mexican drug cartels and other AML violations, DOJ wrote the following: "The monitor has observed that HSBC is continuing to work toward the implementation of a reasonably effective and sustainable AML and sanctions compliance program." But despite progress in certain areas, the monitor had still identified "significant control deficiencies." It also noted that HSBC has successfully implemented a majority of the monitor's recommendations but has not implemented others. Even so, last month DOJ agreed to terminate its Deferred Prosecution Agreement with HSBC.

Has the monitor certified with no conditions or qualifications that HSBC has complied with the letter and the spirit of its obligation to effectively implement a sound AML compliance program? That is the first question. Second, if so, how do you reconcile that with recent statements by the monitor that HSBC still has those

control deficiencies I mentioned, it has not implemented all the monitor's recommendation? Why didn't DOJ simply extend the term of the DPA, as it has done with other DPAs in the past?

Mr. DAY. Thank you, Senator, for that question. I think it is important to highlight the Department's—the lens through which we view this type of conduct. Our role in this area is really to prosecute willful violations of the Bank Secrecy Act, so, in other words, when a financial institution understands its obligations and persists in choosing another course of conduct they know does not satisfy the law, that was the reason behind the initial deferred prosecution that we brought in 2012.

Since then, though, as we have reported to the court in regular filings, including the ones you mentioned, the bank had not engaged in that type of misconduct; rather, they had gone about a very lengthy process of taking the monitor's recommendations and implementing them. That is the lens that we have to apply when we are deciding whether or not to apply an additional sanction, extend a Deferred Prosecution Agreement, or let that document rest as it was originally intended.

So I cannot really comment about the specifics that are not public in that process, but I think that lens, the fact that the Department's perspective is focused on willful criminal violations and things that might fall short of that do not come to the Department's attention, can help explain why we take the steps in that case or any other.

Senator BROWN. But that lens, does that lens suggest allowing an incompleteness in complying? Because it seems that you acknowledge many ways they complied, some ways they did not. How does this encourage them to comply where they have fallen short?

Mr. DAY. Yes, Senator, so their obligations under the Deferred Prosecution Agreement they did comply with. Whether or not they at any given moment have satisfied all the monitor's recommendations is a different issue, but their obligations under the Deferred Prosecution Agreement are do not engage in any further violations of the law, implement a remedial program that at a given point satisfies the concerns the monitor has, even if it is not by an exact date. Those are the obligations, and that is why, because they had satisfied those obligations to the Government's satisfaction, we did not extend the DPA or take further action.

Senator BROWN. OK. Thank you.

Chairman CRAPO. Senator Sasse.

Senator SASSE. Thank you. Thanks to you both for being here, and thanks for really good written testimony. It was helpful.

Mr. Day, can you break down the $2 trillion number? What do we know by business type—type of crime business I mean—by geography, *et cetera*?

Mr. DAY. So I do not have those figures at hand, although I am happy to go back and see if we can further parse that figure. What I can say is that a substantial portion of it does impact the United States literally hundreds of millions of dollars. Part of that is because of the centrality of our financial system, right? Those strengths that I talked about attract criminals who wish to launder their proceeds, even if they did not generate them here in the United States.

Senator SASSE. So I would love to get any follow-up information on that. Thanks. I think your numbers say $300 billion is U.S. and $2 trillion is the global number, and I think tax evasion is not in that universe.

Of the $1.7 trillion—I know these are broad estimates, but setting aside the $300 billion that is in the United States and is going to use our financial system, of the $1.7 trillion outside the United States, does a third of it, most of it, does it touch the U.S. financial system somehow?

Mr. DAY. So I hesitate to give precise figures in part because I would need to go back and see if we have got any better data on that. But, yes, a large amount that is not included in the $300 billion would touch the U.S. financial system through U.S. dollar clearing or other services that our financial system provides essentially to the global economy. And that is why we have to be so vigilant in protecting against money-laundering crimes.

Senator SASSE. And so I guess—and this is for both of you two, not just you, Mr. Day. But I guess one thing I am trying to understand is the suspicious activity reports, we are not reading most of them, right? That is not your fault. It is that there is a huge flood of these things. Do we have anything like red zone statistics to have a kind of theory of the world and where the money-laundering crime is? And then where do we get reports, and how much of it ends up being aligned with the kinds of stuff we are trying to prevent? We would like to prevent, you know, all $2 trillion of illicit funds, but do we know that there is high-yield data that you are getting versus stuff that ends up just being noise in the system?

Ms. MANDELKER. So that is exactly what we are studying, you know, as we undertake this effort to examine whether or not we need to change these thresholds. What I can tell you is, yes, we get a lot of data, and there are review teams that are stationed all over the country who really take a very careful look at these SARs.

We also use technology, of course, to analyze the data so that while not every SAR may be reviewed, it certainly is targeted for analysis, which has been extraordinarily helpful. But as we continue our review, I am happy to share with you what we are learning.

Senator SASSE. Thanks. My team and I would love to not formally send you a letter on that but just learn your after-action reports. That would be really helpful.

Could you also walk us through a typical case, either as an agent or a field manager, where you used financial intelligence such as the suspicious activity reports and then ultimately catch criminals? What is the modal type of investigation that leads to successful prosecution?

Mr. DAY. I will give you an example, but I should say that there is no necessarily prototypical way because it is so useful. This type of information to prosecutors and agents can be used in a variety of ways. One way is to start a case. So, in other words, as Sigal mentioned, there are teams that regularly look through, setting criteria, the system to try to determine are there new financial crimes occurring in their district that they need to initiate an investigation into. In other instances, we might have started an investigation based on a cooperating witness or some completely

independent source of information. Then we go query the Bank Secrecy Act system that includes the SAR data in order to further the investigation, to learn more about what other things are these potential defendants into that we need to investigate. So it really is a very wide universe precisely because it is so useful to law enforcement.

Senator SASSE. I think lots of Americans would have a sense of how a drug cartel would need to use the financial system to launder their money. But in a case like human trafficking, give us an example of how a case would unfold where you get information and where does it yield something. Why and how are they abusing our system?

Mr. DAY. Sure. So human trafficking or really almost any other crime is all motivated by financial gain. So there has to be a way for the criminals, if they are going to engage in the crime, to use the proceeds that they glean from that, and that involves bringing the proceeds into the financial system; if they are successful, laundering those proceeds so that they can use them to purchase goods, reinvest in the criminal enterprise, create additional harms to the community.

So often the financial data is useful because it allows us to see the full human-trafficking network or other criminal networks, because the money goes out to the different parts of the network or it comes in from the different parts of the network that generate the illicit proceeds. It has to come in and be redistributed.

Senator SASSE. I am at time, but I will follow up with you both off-line. I would like to ask some specific questions about how we target specific organizations like MS–13, for example. So thanks.

Chairman CRAPO. Thank you.

Senator Reed.

Senator REED. Well, thank you, Mr. Chairman, and thank you both for your excellent testimony.

At page 5 of your testimony, Mr. Day, you say that one of the money-laundering threats is the purchase of real estate and other assets. And I understand, Secretary Mandelker, that there is a program in the Department of Treasury where you have identified certain areas of the country, and you are looking at these acquisitions of above a certain value and doing so through the title insurance companies. Can you explain how that is working?

Ms. MANDELKER. So we are using our geographic targeting order, which is an authority that was given to us by the Congress and expanded over the summer to extend to wire transactions. Essentially, what we are doing is we are telling the title insurance companies that they have to report to us who the beneficial owners are involved in transactions involving high-end real estate, in all-cash type of real estate, again, high-end real estate transactions.

Senator REED. Right.

Ms. MANDELKER. And then, of course, we are analyzing that data. We have already issued an advisory, which was a result not only of the data that we analyzed when we first issued the geographic targeting orders, but we also thought that it was very important to highlight to the real estate industry some of the red alerts, some of the risks that they should be identifying when they are taking in and working on this business.

Senator REED. And you have the legal authority, there is no question about the legal authority for you to do this.

Ms. MANDELKER. It is a legal authority that the Congress gave to us, yes.

Senator REED. One of the difficulties is finding who the ultimate beneficial owner is, so how insistent are you with these—it seems to me that title insurance companies typically do not do that, so how effective is this in terms of actually discovering the ultimate beneficial owner rather than the first phase of several phases of ownership?

Ms. MANDELKER. Again, they are required by law and required by our order to report that information to us, and we have been able to gather a great deal of information as a result.

Senator REED. Is that information available to the Congress and the public?

Ms. MANDELKER. That is not information that is available to the public. We are analyzing—it is submitted to us——

Senator REED. It is available to us, though?

Ms. MANDELKER.——pursuant to the Bank Secrecy Act authorities.

Senator REED. But it is available to us?

Ms. MANDELKER. We would be happy to work with you on any requests.

Senator REED. What type of beneficial owners trigger a response by the Treasury? Is it someone who has a criminal activity? Is it someone who has been sanctioned by the United States Government? What is the red line in terms of the beneficial owner is bad or good?

Ms. MANDELKER. Senator, that is really going to depend on the investigation. Of course, it is not just Treasury that is looking at the information that comes in through the Bank Secrecy Act and the SAR reporting. It is also a cadre of law enforcement agents all over the country that are taking a very careful look at it. Any particular economic authority that we deploy in connection with SAR activity or other information we receive in a variety of sources about illicit activity, again, what we decide to do with depend on the——

Senator REED. Have you made a referral to the Justice Department yet for enforcement action in any of these real estate transactions?

Ms. MANDELKER. Again, that information is likewise available to law enforcement through the Bank Secrecy Act. So as with all of the BSA data that comes into the Treasury Department, law enforcement has full access to any information. And, of course, we work closely with them to the extent they need our assistance to analyze the data.

Senator REED. I know Mr. Day wants to respond. I have one other question. Would you want a quick response, Mr. Day, now? And then I will go back to the Secretary.

Mr. DAY. Only to add that law enforcement is excited about the potential and is starting to see some of the fruits of this effort, because, remember, if you are talking about money laundering into real estate, you are talking a very large dollar money-laundering transaction. So those are big-time cases we need to bring.

Senator REED. All right. Switching gears slightly, your sanction activities against the North Korean regime, are you in any way able to impede the remissions that are paid by North Korean workers in Russia or other places?

Ms. MANDELKER. Senator, to the extent that we can use our sanctions authorities to target that kind of activity, we have done so. We have had designations connected to laborers. Of course, as you know, there are U.N. Security Council resolutions in place that specifically address, among other sources of revenue, laborers, and we expect that those countries will abide by their U.N. Security Council resolution obligations. And, of course, we continue to pressure them to do so.

Senator REED. But, unilaterally, are we pursuing them aggressively in terms of identifying any type of transmission mechanism and disrupting it?

Ms. MANDELKER. We continue to pursue North Korea's sources of revenue on a wide variety of fronts.

Senator REED. Thank you very much. Thank you.

Chairman CRAPO. Senator Tillis.

Senator TILLIS. Thank you, Mr. Chair. Thank you both for being here.

Madam Secretary, I had a question for you. It relates to some of the questions that I had in the hearing a couple of weeks ago. You have mentioned a couple of times that you think the financial institutions are engaged in a number of high-value activities, and I think that is a good thing. But when you see some of the numbers—Bank of America is headquartered in North Carolina—when you see 800 people focused on that, I have got to believe there are some low-value activities that are going on there, too. If you take a look at the fines, I think the GAO issued a report back in 2016 that said since 2009, $5.1 billion in penalties I guess have been paid by the financial institutions.

What work have we done to look at, you know, with that sort of exposure out there, how much of their work could actually be dedicated to doing nothing more to make sure they are compliant and not subject to a penalty versus focusing their resources on the higher-value activities that I think we all need to do? What are we looking at to try and make an objective assessment about the current status?

Ms. MANDELKER. Thank you, Senator. So, again, we do this in very close coordination with our regulatory partners and our law enforcement efforts. I do think we need to make sure that those resources are carefully calibrated toward producing the kind of financial crimes analysis that we need that really feeds into the cases that we are able to bring to tackle the threats, the money-laundering threats that we face. So we are, again, taking a very careful look at how we are incentivizing the banks to target their resources and efforts to the kinds of activities that provide higher value to us, and we are talking to the Federal banking regulators about that. We are talking to law enforcement about it as well.

Senator TILLIS. This is only conceptual. I am not offering this up as necessarily—thematically, it is more along the lines of offer them a bounty to identify bad actors versus subject them to a

penalty for not necessarily getting the paperwork right. It is just, I think, a mentality that we should look at.

Mr. Day, I had a question for you, and it relates to Secretary Mnuchin recently announcing that he is going to have a working group on digital currencies, and that kind of skates into the money-laundering lanes. If we are going to start looking at how to do a better job here and establish a working group, it seems that it would be helpful to have DOJ at the table since at the end of the day everything you put into place would be with the goal of ultimately having a successful prosecution. What is your view of that? And, Madam Secretary, you can weigh in as well.

Mr. DAY. I agree, but I should say, just as my colleague Sigal said, we already have a very good, robust working relationship, and so I fully expect—I saw that announcement as well, but I——

Senator TILLIS. So whether or not you sit on the working group, you feel like you will have adequate input into the process, Madam Secretary?

Ms. MANDELKER. I do not have any question. We actually do sit in working groups with the Department of Justice very specifically focused on virtual currencies. In fact, in a previous iteration, I supervised the section of the Justice Department that was focused on cryptocurrency and virtual currency. So we have a robust relationship. Of course, we need to work very much in concert with each other as we identify and regulate and enforce our laws to counter illicit uses of virtual currency.

Senator TILLIS. I had a couple of questions that I think add on to where Senator Sasse was going. If it is a $2 trillion aggregate market, $300 billion in the United States, does that mean if we solve our whole problem, we have still got an 80 percent problem to deal with out there? In other words, how do we go about this? I understand that we have to deal with our back yard, but how are we going about this to where we have just simply not made it an unfavorable jurisdiction but fundamentally the same activity is going to occur?

Ms. MANDELKER. Actually, we already do a great deal of work with our international partners in a wide variety of areas. So just as an example, we sit as the Vice President of the Financial Action Task Force, which is an international body that is focused on making sure that countries all over the world have the same kinds of standards that we do when it comes to AML/CFT regimes. We also work very closely with law enforcement and other agencies all over the world on tackling the threats at the Treasury Department. We likewise do that in the context of the G–7 and the G–20. I engage and I have a team of people at the Treasury Department who engage with our partners, again, all over the world to make sure that we are aggressively tackling illicit financing that is coming through the U.S. system and also that resides elsewhere.

Senator TILLIS. Madam Secretary, is the Treasury going to be on point to define other stakeholders and really set the priority? I always talk about the tip of the spear because we have got different people who are looking at—or different agencies who may be looking into this issue. Is Treasury at the tip? Are they going to kind of coordinate, engage the stakeholders, and be the one that the industry looks to for guidance going forward, and certainty?

Ms. MANDELKER. So we already do that. We have—among the mechanisms in which we engage with the private sector, we also—we chair the Bank Secrecy Act Advisory Group, which is an entity that brings together law enforcement, our interagency partners, as well as a wide spectrum of entities in the financial sector. So that is something that we do. It is something we will continue to do in that venue and in other fora as well.

Senator TILLIS. Thank you. Sorry I went over, Mr. Chair.

Chairman CRAPO. Thank you.

Senator Tester.

Senator TESTER. Thank you, Mr. Chairman. I want to thank both the witnesses for being here today.

Kind of going on with that, other countries that are tackling this issue, how effective have they been, number one?

Ms. MANDELKER. It is really going to depend on the country. It is something that, again, we monitor very carefully. So within, just as an example, the context of the FATF, the FATF conducts evaluations of other countries' AML/CFT regimes, and we play a very important role in that area. And where countries are not living up to their standards—Iran is a perfect example of that—we push very heavily to make sure that there are consequences to not having an AML/CFT regime in place that meets our standard.

Senator TESTER. All right. And of the money laundering that is done worldwide, can you give me any estimate how much of it is done in this country?

Ms. MANDELKER. I think Mr. Day spoke to that already.

Senator TESTER. Fine. Go ahead. Shoot quickly then.

Mr. DAY. Sure. Roughly $300 billion I believe is——

Senator TESTER. And what is that a percentage of the total?

Mr. DAY. So the best estimates I have seen are more than $2 trillion globally on an annual basis.

Senator TESTER. OK. So when it comes to money laundering in this country, is most of it done through the largest institutions, or is it done through regional or community banks?

Mr. DAY. I do not think you can actually pinpoint exactly where. The safe answer is criminals will go wherever they can with their illicit proceeds, so it happens at global financial institutions, national, regional, small banks.

Senator TESTER. Got you.

Mr. DAY. And even nonbanks like brokerage houses.

Senator TESTER. But you—and it is OK if you do not, I guess, but you do not know if most of it is going through the big guys or the small guys or the regional guys? I know I get it. They will go to the weakest link in the fence. But, currently, where is most of it happening?

Mr. DAY. It all depends on the case. That is a very case-specific question.

Senator TESTER. OK.

Mr. DAY. Sometimes it goes to the biggest institutions. Sometimes it does not. It just depends on how the criminals put together their——

Senator TESTER. So what I hear you say—unless I do not understand this issue properly myself. What I hear you say, of that $300

billion that is being laundered here, it is pretty much equal between small, medium, and large?

Mr. DAY. I would not want to put a percentage on it. I really do not know, Senator.

Senator TESTER. I do not want to be—but isn't that important to know? Isn't it important to know where the dough is going and how it is being laundered so that you can make the regulation fit the risk?

Mr. DAY. Well, you know, Treasury can speak to this even better than Justice, but the Bank Secrecy Act is a risk-based approach, and so you are exactly right. We are focused on identifying the largest risks, and we are constantly reevaluating and fine-tuning and training our investigative resources where we think is the largest threat.

Senator TESTER. OK.

Mr. DAY. But it would be a mistake to think of it as just happening in——

Senator TESTER. No, no. I am not saying that. I am just saying as we look at this from 30,000 feet, you are going to put the resources where most of the problems are having, and if you do not know where those problems are, that is a bit disturbing for me.

Mr. DAY. Well, I do not mean to suggest we do not know where those problems are. It is just that we never rest on our laurels in the sense that where the problems are today is not where they will be tomorrow.

Senator TESTER. I have got it. But today you cannot even tell me where the laundering——

Mr. DAY. Not as a percentage basis.

Senator TESTER. All right. Is there technology out there that can be—that you guys are recommending for banks of any size, but particularly the smaller ones, to be able to utilize to protect themselves?

Mr. DAY. So the Justice Department would not play that role.

Senator TESTER. Who does? Anybody?

Mr. DAY. I do not know if a regulator does or not.

Ms. MANDELKER. We do not recommend a particular vendor or type of technology for any particular kind of financial institution. We do provide guidance and training to——

Senator TESTER. OK. That is good, Sigal. So where do they go? Where do they go to get the information so they know where the threats potentially are coming from to be able to protect themselves and the consumers ultimately?

Ms. MANDELKER. I think there are a variety of places that they go. Of course, there is a whole AML/CFT compliance industry out there, of course, that they can talk to. But we are——

Senator TESTER. And where are they getting their instruction from?

Ms. MANDELKER. What we are focused on, Senator, is making sure that we are providing financial institutions of all types and sizes with critical information to help them identify risks and typologies. That is why, for example, in this initiative, FinCEN Exchange, which I mentioned at the beginning, we are going to be—we are going to and we have in the past, frankly—talking to not just the big banks but also local, regional, community banks so that

we can help them build their system, their red alerts, their algorithms to identify critical risk. And I think that kind of information is really critical to achieving the strong and effective regime that we want.

Senator TESTER. OK. We will have a few more for the record.

Senator TESTER. Thank you, Mr. Chairman.

Chairman CRAPO. Thank you, Senator.

Senator Kennedy.

Senator KENNEDY. Thank you, Mr. Chairman. Thank you both for being here.

Can we agree that you and your agencies could not do your job without the cooperation of our private sector financial institutions?

Ms. MANDELKER. The cooperation that we receive from financial institutions is critical to doing what we are trying to accomplish, which is to have a strong and effective regime.

Senator KENNEDY. In fact, it is mandated, is it not?

Ms. MANDELKER. Absolutely.

Senator KENNEDY. OK. How much do American financial institutions spend every year complying with the mandates?

Ms. MANDELKER. I am sure those figures are available. I do not have them before me. I think Clearing House, for example, might be able to provide you with some of those numbers. But it is a significant amount. There are a lot of resources that the banks, financial institutions, and other entities regulated by the Bank Secrecy Act are devoting to compliance.

Senator KENNEDY. Was it in the hundreds of millions?

Ms. MANDELKER. Again, I do not have those numbers, but they are substantial.

Senator KENNEDY. You have never looked at the cost?

Ms. MANDELKER. Again——

Senator KENNEDY. Have either of you ever looked at the cost?

Mr. DAY. I do not have those figures either, Senator.

Senator KENNEDY. OK. What is the dollar amount of money laundering that you stop every year?

Mr. DAY. I do not have those figures in front of me, but it is also significant, both in terms of actual money that is being laundered that we seize and forfeit, as well as conduct that we are able to prevent and deter from the prosecutions we bring. But I do not have a precise figure for you.

Senator KENNEDY. Do you know, Madam Secretary?

Ms. MANDELKER. So I cannot give you a number. What I can tell you is that we use a number of different economic authorities to stop illicit money from coming into this system. That is what we use our designations for. For example, we are sending out the message that if you are going to try—not only if you are a designated entity and you have money in the United States——

Senator KENNEDY. I get it. I am sorry to interrupt——

Ms. MANDELKER.——but your money is not welcome.

Senator KENNEDY.——but I have only got 5 minutes.

Ms. MANDELKER. Yes.

Senator KENNEDY. Don't you think it would make sense at some point to say, OK, here is the cost and here is the benefit? Is there anybody in your agencies that do that?

Ms. MANDELKER. Absolutely, Senator. I think that is a very important endeavor, and as we decide what rules and regulations roll out——

Senator KENNEDY. Can you get me that information?

Ms. MANDELKER.——in the future, we undertake that kind of—those kinds of exercises.

Senator KENNEDY. Can you get me that information?

Ms. MANDELKER. Again, some of that information is resident within the financial institutions in terms of what costs that they——

Senator KENNEDY. Yes, ma'am, but can you get it for me?

Ms. MANDELKER. I can provide to you what information we have. I do not know that I have an assessment of the total costs——

Senator KENNEDY. General, can you get it for me?

Mr. DAY. Senator, I do not know either that the Justice Department—remember, I guess our role is more narrow. We are ultimately focused on prosecuting——

Senator KENNEDY. I am going to take that as a no.

Mr. DAY. I am happy to take back any——

Senator KENNEDY. Yeah, if you could just ask, pretty please.

Mr. DAY. Of course.

Senator KENNEDY. This is our second hearing, and I have learned a lot, but I still have not heard what changes you are recommending. I understand we need to have more conversations. Tell me in the 2 minutes I have with specificity what changes you are recommending that we make, General.

Mr. DAY. Beneficial ownership is a problem we need to fix.

Senator KENNEDY. Do you have a suggestion on how we fix beneficial ownership?

Mr. DAY. We need to gather information about——

Senator KENNEDY. But in terms of a bill.

Mr. DAY. We do not have any proposed legislation, no, but we are more than happy to engage with you or your staff.

Senator KENNEDY. Well, I am engaging. Can you send to me with specificity the changes you need to make, you are recommending we make in beneficial ownership?

Mr. DAY. I would be happy to take that back, and there are some——

Senator KENNEDY. OK. Anything else?

Mr. DAY.——increased penalties for bulk cash smuggling.

Senator KENNEDY. OK.

Mr. DAY. So that is right now subject to a 5-year statutory maximum.

Senator KENNEDY. Can you send that to me with some specificity?

Mr. DAY. I would be happy to take that back, but increased statutory maximums.

Senator KENNEDY. OK. Anything else?

Mr. DAY. There are some additional tweaks to the money-laundering statutes that we would be——

Senator KENNEDY. All right. Can you send me those tweaks?

Mr. DAY. Yes, sir.

Senator KENNEDY. Madam Secretary, how about you, specificity?

Ms. MANDELKER. We would be happy to work with your staff. What I can tell you is—but I also want to, as I mentioned already, this is something that we have to do carefully, and we have to make sure that any fixes that we propose are supported by the analytics.

Senator KENNEDY. I want to be careful, and I appreciate all that. But what I am asking is at some point you have got to go from 30,000 feet to the ground. Are you ready to send to us with specificity suggested changes in the acts that we should make and why?

Ms. MANDELKER. Again, Senator, we are studying that issue very carefully. I want to make sure——

Senator KENNEDY. You are not ready? I mean, I am not trying to be rude.

Ms. MANDELKER. I understand.

Senator KENNEDY. This is the second hearing that we have sat through, and I have learned a lot, and I appreciate it. But I am ready—I understand the global perspective. I am kind of ready to get down out of La La Land down into the nuts and bolts. How do we fix the problem, and what is it going to cost?

Ms. MANDELKER. And, again, Senator, we are getting into the nuts and bolts. I want to make sure that whatever changes we recommend, those changes are supported by the data, the analytics, and the law enforcement community to make sure that we are doing this——

Senator KENNEDY. OK. When do you think you will have that?

Ms. MANDELKER. I cannot give you a timeframe, but I am happy to have further discussions about it.

Senator KENNEDY. Within 6 months?

Ms. MANDELKER. I would hope that we could have some recommendations within 6 months.

Senator KENNEDY. Three months?

Ms. MANDELKER. Again, you know, I want to make sure that we are doing this carefully, that any changes we are making are made—or we are recommending are made in very close cooperation with the law enforcement community, because it——

Senator KENNEDY. Well, I would just respectfully ask you, let us get down to it. OK?

Ms. MANDELKER. I appreciate that request.

Senator KENNEDY. You are raising problems. Let us look for solutions, and if you cannot tell us how to solve them, then point us in the right direction. And if you could get me that cost-benefit analysis, that would be—I will send you both a fruit basket. OK?

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Warner.

Senator WARNER. Thank you, Mr. Chairman. Let the record show that this is the second of one of these hearings. I have stayed until the end, and I am the last guy talking. Let me, first of all——

Chairman CRAPO. Duly noted.

Senator WARNER.——commend my friend, the Senator from Louisiana, for once again asking common-sense, practical, bottom-line questions. And I actually think this is one of those rare areas where, you know, I do not think there is a difference, Democrat and Republican, in terms of how we approach this. So I would love

to work with you on beneficial ownership. I think we need to look at areas where we could use technology. I think we heard in the last hearing, for example, literally tens of thousands of SARs reports, we do not really know how to sort through them, so how do we do this in a technology-friendly way that still protects consumer information?

I still think we have got a lot of work to do on cryptocurrencies to get ahead of this, and I think we have also heard both in this hearing and the other that, you know, a lot of the money laundering may have moved from traditionally through the banks particularly into real estate, and there is work there. So I appreciate very much the Senator's questions. I would look forward to those answers as well. But if the Administration cannot come up with some ideas, I think you and I and Members of this Committee and the leadership of the Chairman could.

Let me try to drill down on a couple of these. At the last hearing, I raised the issue around cryptocurrencies and what we are doing, and I know Senator Tillis raised the issue that Secretary Mnuchin has got a working group. But when we see just the notion that China said they were going to look a little bit more into this, and we saw a huge drop in value, for example, on one of these cryptocurrencies, on bitcoin, in the last couple weeks, do you feel like you have all the tools you need—and this is an area that is happening—moving so quickly. Do you have the tools you need and the technology analysis you need to make sure that we get ahead not just with bitcoin but any kind of blockchain-related technology to do this right?

Ms. MANDELKER. So this is an area of high focus for us, and, in fact, I think it is an area where the Treasury Department, in close coordination with our law enforcement partners, has been ahead of the game globally, and I will just walk you through some of the efforts that we have——

Senator WARNER. Fairly quickly, because I have got a series of questions.

Ms. MANDELKER. Sure.

Senator WARNER. Unless the Chairman wants to give me a couple extra minutes since I waited so long.

Ms. MANDELKER. And I would be happy to provide more information in another setting. But just as an example, in 2014 FinCEN issued guidance identifying virtual currency exchangers and administrators as entities that are regulated under the BSA. So those entities are now required, among other things, to file SARs. They are subject to examinations by FinCEN and the IRS, which we have been conducting. We have had enforcement actions. Both the Treasury Department and the Justice Department have gone after virtual currency——

Senator WARNER. Madam Secretary, could you get me that list? Again, because I want to get a couple more questions in.

Ms. MANDELKER. Yes, happy to do so.

Senator WARNER. I would love to see it and share it with the full Committee.

Senator WARNER. Again, talking about SARs, for example, one of the things that appears is we have got this massive amount of information, and it would seem to me that there may be technology

tools we could use that could show patterns that might not otherwise be evident. How do we do that and also a way where we protect—an issue Senator Warren and I have worked on—personal consumer financial information? How do we get that balance right between being able to see patterns but still protect consumers' information?

Ms. MANDELKER. So just in terms of detecting patterns, we have efforts underway to make sure that we are using technology to analyze the vast amount of information that is in the BSA. In fact, I have a council of folks at the Treasury Department that I have recently stood up who are working very collaboratively together to make sure that we are appropriately using the tools that we have and that we are identifying other areas or other tools that we can deploy to make sure that, again, we are detecting patterns, trends. And a lot of what we are able to obtain using those kinds of tools and analysis feed into authorities, the economic authorities that we use, the Justice Department authorities, but we also then loop that information back out into the financial sector.

Senator WARNER. If you could, again, get us a little more background on that.

Ms. MANDELKER. Happy to.

Senator WARNER. I have got a couple seconds left. You know, one of the issues I think we wrestle with as well is we have got to have strong anti-money-laundering procedures, but how do we get that right with also making sure that there are appropriate financial products for the underbanked, for example, the immigrant community that uses remittances a lot? Obviously, there is a ripe area for abuse, but there are wide swaths of our country that are underbanked that need to use these tools. How do you sort through and think through that notion?

Ms. MANDELKER. That is a very good question, and I think it is a complicated one. Again, I think it is important that we make sure that our financial institutions, including money services businesses, money transmitters, are appropriately regulated so that those avenues of transferring money are available and available in ways that are used licitly. And, of course, we also do outreach to those kinds of communities to make sure that they understand both the risks and the requirements that they have in place to have the kind of AML/CFT programs that we believe are appropriate.

Senator WARNER. Thank you, Mr. Chairman. I think there is a lot of work to be done here.

Chairman CRAPO. Thank you.

Senator Donnelly.

Senator DONNELLY. Thank you, Mr. Chairman. And I want to thank the witnesses for being here.

Mr. Day, in your testimony you highlight virtual currencies as an alternative to cash that criminals may use for illicit transactions. Cryptocurrencies such as bitcoin and ripple and ethereum provide anonymity and are lightly regulated, with limited AML controls. And this would be to both of you. To what extent do you believe criminal networks, terrorist groups, and rogue nations have utilized cryptocurrencies as a means for moving money? Mr. Day, if you would go first.

Mr. DAY. So we have seen criminal groups focus on digital currencies. There have been a number of prosecutions. Several years ago, the Justice Department prosecuted Liberty Reserve, and as Sigal mentioned, that was a coordinated effort where Treasury deployed anti-money-laundering authorities. At the same time we announced our prosecution, the estimates at the time were about $6 billion worth of money laundering through Liberty Reserve, so a very significant money-laundering problem, precisely because it offered anonymity to the criminals that were using it.

More recently, the Justice Department has prosecuted a digital currency exchange service in the Northern District of California for failure to have anti-money-laundering controls, and it is a problem where we are going to continue to devote significant additional resources.

We just hired a digital currency counsel whose job is to make sure that prosecutors and agents are up to speed on the latest evolving money-laundering threats in the digital currency space.

Senator DONNELLY. Ms. Mandelker?

Ms. MANDELKER. It is an area that we are tracking very carefully. We are concerned about the use of cryptocurrencies for illicit purposes all over the world, just as we are a number of other means that illicit actors use to transfer value.

I think one area that we are working on but that we have to really hone in on is the fact that while in the United States we have regulations over these virtual currency exchangers and administrators, those kinds of regulations are lacking in many different regions of the world. And so we have to encourage other countries to do what we, Japan, Australia, and some others have done to make sure that those industries are appropriately——

Senator DONNELLY. And I guess that follows up on my next question, which was: How can law enforcement and Federal authorities minimize—or monitor these transactions? As you move forward, what is the most important thing you need to do to be able to have success in that area?

Ms. MANDELKER. So we are monitoring the transactions. Because we do have AML/CFT requirements here in the United States, we actually get a lot of SAR reporting from the virtual currency exchangers. But we also have to send the message, which we have done throughout the world, that to the extent these virtual currency exchangers are engaging in illicit activity, we are going to go after them.

So just as a brief example, with the Justice Department we recently assessed a very significant monetary penalty of $100 million against a virtual currency exchanger that was resident and principally operating in a foreign jurisdiction.

Senator DONNELLY. There have been a number of reports that the United States is among the easiest countries to create anonymous shell companies in. Anyone can legally open bank accounts. Anyone can buy property. As a result, criminal networks, corrupt dictators, and terrorists can move money through the United States as a legal business entity.

I would like to know from both of you, what resources are available to you to identify the sources of illicit financing? And what

difficulties are presented by these weak corporate transparency rules where, in effect, almost anything goes?

Ms. MANDELKER. So I just wanted to start by pointing out that FinCEN did issue a rule in 2016, the customer due diligence rule, that actually now requires financial institutions to get information about the actual persons that are behind their customer accounts. I think that is a very important development. That rule is going to go into effect in May, and I know a lot of financial institutions are already gathering and collecting that information.

Of course, there has also been a lot of discussion about other mechanisms that we can put in place through legislation to gather additional beneficial ownership information, which is important in the context where you cannot just rely on the financial institutions to gather that kind of information.

Senator DONNELLY. Mr. Day?

Mr. DAY. Thank you, Senator, for your question on this issue. Law enforcement does view the lack of a systematic beneficial ownership regime in the United States as something that does cause us to expend a lot of additional time and effort in individual cases, piercing the corporate veil, trying to figure out who are the bad actors that are hiding these illicit proceeds. So we are able to do it through a lot of gumshoe traditional investigative work, but we would bring more cases more quickly with more impact if we had a better system in place to make that information available to law enforcement.

Senator DONNELLY. Thank you to both of you.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Cortez Masto.

Senator CORTEZ MASTO. Good morning, Under Secretary Mandelker, Mr. Day. Thank you for the conversation. A very important discussion we are having.

One of the things I want to shift just a little, though, and you will appreciate this. Besides the financial institutions—I come from the State of Nevada, and gaming is considered like those financial institutions. Qualified casinos are subject to the Bank Secrecy Act, so I have a couple questions around gaming in general, because I know the organizations within my State, and across the country, have suggested that gaming operators would welcome a review of the BSA requirements, like everyone else that we are talking about today, and they look forward to this Committee's thoughtful, bipartisan review of the 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.

So one of the top priorities of the gaming industry is to eliminate the requirement that a detailed factual narrative is required when filing a suspicious activity report form for structuring situations. What are the pros and cons of such a change? And I am going to ask both of you to answer that question.

Ms. MANDELKER. As with any SAR reporting, we do receive a great deal of benefit from the narratives that are provided in the context of—by the gaming industry, by financial institutions, among other areas. I understand that there have been some discussions about whether or not resources are well spent when it comes

to the structuring SARs. Of course, that is something that we will take into consideration and consider, and we welcome the thoughts of others in discussing——

Senator CORTEZ MASTO. You are willing to address it—listen to them and address some of the concerns, too?

Ms. MANDELKER. We are certainly happy to have a discussion with them.

Senator CORTEZ MASTO. OK. Mr. Day?

Mr. DAY. I would just second what Sigal said, which is the information that we glean from the narrative portion of a suspicious activity report can be very helpful in deciding to initiate a criminal investigation or furthering a preexisting case. So there probably is opportunity to at least discuss changes, but it should be, you know, at least leavened by the notion that there is a lot of benefit to law enforcement now, and what can we do to preserve that benefit going forward?

Senator CORTEZ MASTO. OK. And then the gaming industry and others have recommended—and I heard it at our last hearing—raising the currency transaction and suspicious activity reporting thresholds. Some have recommended increasing the rate roughly to about $60,000. Others say that is too high, but a lesser amount, from $5,000, $10,000, to $20,000 and $25,000, would be an improvement. Your thoughts on that, pros and cons? Or should we even be looking at that threshold amount?

Mr. DAY. Similar to the answer I gave a moment ago. There are crimes that do not involve a lot of money, and so I fear—or one potential disadvantage to raising the thresholds without substantial study, like Sigal is discussing, is that you risk losing visibility into those types of crimes. The classic example is the lone wolf terrorism example. That does not involve a lot of money and might not hit upon one of those thresholds, but might a lower threshold.

So it is obviously an opportunity for us all to have this discussion and make sure the thresholds are correct or, if they need to be tweaked, what should they be. But it should be balanced against this need to maintain visibility into those types of criminal activity.

Senator CORTEZ MASTO. OK. And what I have heard constantly is the lack of communication. So I appreciate and applaud the launch of FinCEN Exchange. Can you talk a little bit more about that? And how will that draw in industry that is being regulated and the discussion that we are having today and how they can talk to you directly about some of the concerns and whether those concerns can be addressed or not?

Ms. MANDELKER. I would be happy to. So this is actually something that we had piloted in the past and now we are accelerating. So what we have been able to do in these settings is bring together financial institutions of all different types and sizes across the country and, among other things, have discussions with them on particular cases. So we will provide them with information that they can then use——

Senator CORTEZ MASTO. And this would include nondepository institutions, like gaming and others?

Ms. MANDELKER. Right now we are focused on the financial institutions, but we are happy to have discussions about whether or not we would want to use it in other settings as well.

Senator CORTEZ MASTO. OK.

Ms. MANDELKER. But we also are very focused on doing, through FinCEN Exchange and through our financial advisories, among other ways of communicating, is providing financial institutions with typologies. What are the kinds of activity that they should be alert for? How can they continue to sophisticate their algorithms based on what our priorities are, the threats that we are seeing that are most troubling? So it is a mechanism to make sure that we are really significantly enhancing the private-public information sharing that is, I think, going to be so critical to ensuring that we are getting the kind of data from the financial institutions that we need to continue to be all the more effective in safeguarding our system.

Senator CORTEZ MASTO. I appreciate that. And is DOJ involved in the FinCEN Exchange?

Ms. MANDELKER. Absolutely.

Senator CORTEZ MASTO. So it is everybody that is involved with FinCEN that would be part of it.

Ms. MANDELKER. Exactly.

Senator CORTEZ MASTO. OK, all the agencies.

Ms. MANDELKER. These would be meetings with FinCEN, with law enforcement, and with the financial——

Senator CORTEZ MASTO. I would hope you would open it up to nondepository institutions as well, as you well know, because they are regulated—particularly, if we really want to address anti-money laundering, go after and target, then we need to bring all of the regulated agencies in to have this conversation.

One final thing. I do think that there needs to be more risk-based assessment, more targeted investigations, and everybody should be a part of that, not this check the box, "I have done what I had to do," and pass this form on and up the ladder to somebody else. I think we have got a lot of opportunity here, both in the compliance departments that exist in all of the agencies that are regulated along with our law enforcement and our Treasury to really have a targeted approach and streamline it and be effective when we are trying to address money-laundering issues and stop money laundering. So thank you for the conversation today.

Chairman CRAPO. Thank you.

Senator Warren.

Senator WARREN. Thank you, Mr. Chairman.

So at the last hearing on this topic, I focused on a few areas where we could update our money-laundering laws to make life easier both for law enforcement and for small financial institutions, including making reporting requirements more sensible and making sure we know who owns American corporations.

Today I want to focus on cracking down harder on the big banks that repeatedly violate anti-money-laundering laws. So think about Citigroup. Just this month, the OCC fined the bank $70 million for ignoring a 2012 order to beef up its anti-money-laundering controls. In May, Citi was fined by the Fed $97 million for letting Mexican drug cartels launder money through the bank. How many money-laundering operations are they assisting?

And Citi is not the only one. Other big banks break the law. They get caught. And then they shrug off fines that barely dent

their massive profits, while criminals and terrorists continue to move drug money and terrorist money all around the globe.

Under Secretary Mandelker, are you confident that the biggest financial institutions in the world are doing enough to comply with anti-money-laundering laws?

Ms. MANDELKER. I think that there is a lot of effort within the financial institutions to make sure that they have——

Senator WARREN. I am not asking if there is a lot of effort. It is a really simple question. I am asking, do you think they are doing enough to comply with the anti-money-laundering laws?

Ms. MANDELKER. Again, I think that there are very substantial efforts underway within the financial institutions to comply with the laws. To the extent that they are not complying with the laws, of course, we are going to be focused on those both through our——

Senator WARREN. So let me ask it again. Do you think they are doing enough?

Ms. MANDELKER. Again, Senator, that is a very broad question, and it is difficult for me to make a generalization. I think we are very vigilant in monitoring and making sure that they are doing enough, and where they are not, we and the Justice Department have and will continue to use our authority——

Senator WARREN. Well, I am concerned about the fact that we keep going back at them repeatedly, which kind of sounds like it is not working. You know, I am very concerned that big banks will continue to allow money laundering because the business is profitable and the penalties for violating the law are weak.

Let us take another example: HSBC. I think Senator Brown raised it. In 2012, the bank agreed to pay a fine of almost $2 billion for letting Mexican drug cartels and a Saudi bank linked with al Qaeda to launder money for years. It also admitted to moving money for customers in Iran, Libya, Sudan, and Burma, all of which were subject to U.S. sanctions. That was the largest penalty ever under the Bank Secrecy Act, and you know what? It was about 4 weeks' worth of income for HSBC. The bank's CEO swore that the bank would fix the problems. But it did not.

Last February, the court-imposed monitor told a judge that he had "significant concerns" about the bank's compliance program, and HSBC faces a new money-laundering investigation right now in the United Kingdom Still, the Department of Justice dismissed its case against the bank in December.

So let me ask, Mr. Day, do you think the fine in the HSBC case worked? Did it get HSBC to start following the law?

Mr. DAY. I think there are a number of parts about that prosecution that cumulatively had their desired impact. When you think——

Senator WARREN. So—let me just stop. It had the desired impact. Then how can it be that a court-installed monitor refused to certify that HSBC's anti-money-laundering compliance program was working? And in November, the United States just opened a new investigation evidently based on new evidence of money laundering? I do not understand how you can say that worked.

Mr. DAY. So that was a Justice Department-installed monitor, and that is another way of, I guess, thinking about the Deferred Prosecution Agreement, is that it included a range of measures,

including, for example, the decision by the Justice Department to impose a monitor to give us confidence that the various provisions of the agreement were being satisfied by HSBC.

Senator WARREN. Well, I am glad for you to have confidence, but I only want you to have confidence if it is actually working. And the monitor said it is not. So I am not clear how you can say that this is working.

You know, let me just make the point because I am running out of time here, and I have one more quick question I want to ask. It is never going to work so long as the consequences are lame fines and no accountability for individuals at the bank who are responsible for the illegal conduct. I promise you that if HSBC executives had been hauled out in handcuffs and were sitting in jail after their violations in 2012, they would have gotten the procedures in place pretty darn fast to make sure that that bank was in compliance with the law.

So I am over, but let me just ask a quick one. Mr. Day, doesn't the Bank Secrecy Act empower the Justice Department to go after individuals responsible for breaking the law?

Mr. DAY. Of course, Senator, and we are focused on bringing individual cases where the facts and the evidence merit such cases. And we have done so in the past and will continue to do so.

Senator WARREN. Well, if we want to stop money laundering, these giant banks really need to feel the penalties. And the people who are in charge who are making the decisions need to understand that if they are putting the American people at risk, they will go to jail. Until that happens, we are not going to fix anything here.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

And our final set of questions from Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Mr. Chairman. I thank both of you for your testimony today, and I do just want to add to what both the Chairman and the Ranking Member said and you have said in your testimony earlier about the importance of getting to this beneficial ownership issue. I believe that is going to be a major focus of the Committee's efforts.

Secretary Mandelker, when you were here for your nomination hearing, I asked you about FinCEN's geographic targeting order, and I think Senator Reed asked some questions regarding that. You did extend it to March 20th, I believe, of this year. Have you found that a useful tool? And I see that you did expand some of the geographic areas.

Ms. MANDELKER. Yes, we have found that it is a very valuable tool. It allows us the opportunity to get critical information to support our efforts and to support law enforcement's efforts.

Senator VAN HOLLEN. And do you have an expectation you will continue this beyond March 20th of this year?

Ms. MANDELKER. So I cannot—you know, as with any kind of tool, I cannot tell you what our forward plans are. We have extended that tool a number of times in the past.

Senator VAN HOLLEN. OK. Well, based on the past track record, I would hope that you would do that.

I know Senator Warner asked some questions about cryptocurrency, and I did want to follow up on some of those. Did you see the Reuters report January 8th headlined, "Cryptocurrency may be getting quietly channeled to North Korea University"? Did that hit your radar screen?

Ms. MANDELKER. I did not see that particular report, but I have seen similar reports linking cryptocurrency to the North Korean regime.

Senator VAN HOLLEN. Right, so I just want to follow up on that because I know we are all working hard on effective sanctions regimes and enforcement. A chief analyst at one of the South Korean cybersecurity firms, EST, was quoted in this article as saying that, "With economic sanctions in place, cryptocurrencies are currently the best way to earn foreign currency in North Korea's situation. It is hard to trace and can be laundered several times." They specifically mention the 13th largest cryptocurrency trader in the world, I guess Monero. Has that been on your radar screen? And what steps are you taking to make sure that North Korea cannot evade different sanctions regimes through use of cryptocurrency?

Ms. MANDELKER. So as you know, we are focused on illicit financing to North Korea in a wide spectrum of areas. Of course, cryptocurrency is one of them, but the North Korean regime has been able to finance itself through a number of different mechanisms, including through the financial system. So to put cryptocurrency to the side, we have to remain vigilant in making sure that North Korea is not using the international financial system, as they have repeatedly in the past, to finance their weapons program. So cryptocurrency, of course, will be an effort of focus for us, but as is the many different ways in which the North Korean regime has been able to buildup to the place where we find ourselves today.

Senator VAN HOLLEN. Absolutely. I think we have got to make sure we cover all of those sources of financing. It appears that to the extent that we are more successful at shutting down conduits through the normal financial system, they may turn to these cryptocurrencies, increasingly do that.

So with respect to these exchanges for cryptocurrencies, do you think that they should be held to the same standards as we do banks?

Ms. MANDELKER. So here in the United States they are. They are subject to the same AML requirements that—they are characterized under our laws as a "money transmitter," and so they are required to have an AML/CFT regime. We do examine them, just as we examine other financial institutions. We have brought enforcement actions not just here in the United States but also against a virtual currency exchanger overseas. We assessed a $100 million penalty over the summer, and the Justice Department has brought even stronger penalties against those kinds of exchangers.

I think the real vulnerability that we all have to address is that while we have regulatory authorities in place here in the United States and we do enforce those authorities, we need other countries to do the same. So countries like Japan and Australia are very much in line with us in regulating virtual currency exchangers, but we have a focused effort on encouraging other, many different

countries to make sure they have the regime in place to keep this type of currency from being manipulated and used by illicit actors.

Senator VAN HOLLEN. Got it. And that brings me to my last question, which I know Senator Tillis raised earlier, and other Members of the Committee, which is we are doing our best to defend our own financial system, and encourage others through international efforts that you testified about earlier. What at the end of the day is our—are we looking at tools to make sure that we strengthen penalties and the costs for those overseas that are not complying with our efforts? Because we can do everything we can here, but if you have got, as others have said, 75 percent of these money-laundering efforts going on overseas, we are just plugging one hole out of a whole lot of them. So what is the plan going forward to make sure we use our leverage in the financial system to make sure that other people are complying?

Ms. MANDELKER. Absolutely. So as I just mentioned, for example, in the virtual currency space we brought an enforcement action against a virtual currency exchanger that was resident overseas. A lot of the work that we do is focused on these kinds of cross-border illicit transactions, and I know many of the cases, just as an example, the Justice Department brings, I know from my days at the Justice Department and just looking at the work that they are doing now, there is a very, very big focus on bringing criminal penalties against illicit actors no matter where in the world that they operate. We do that. We do that through FinCEN, OFAC, and the Justice Department does it as well.

Senator VAN HOLLEN. And you have all the authorities that you think you need to do that effectively now?

Ms. MANDELKER. Yes.

Senator Van Hollen. OK. Thank you.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you, Senator.

For those Senators who want to ask questions for the record following the hearing, they will be due by January 24th, and our witnesses, I ask you, as you get follow-up questions, to respond promptly.

Senator MENENDEZ. Mr. Chairman, if I may?

Chairman CRAPO. Well, that was close. We will give you your 5 minutes.

Senator MENENDEZ. Thank you very much. This is important. Especially as someone who has been one of the architects of our sanctions, I would like to hear some of the answers to some of these questions. So thank you both for your appearance.

As someone who has been the architect of sanctions laws impacting Iran and Russia and North Korea, I understand how important it is to prevent criminals and sanctioned individuals from anonymously accessing the financial system. Therefore, it is critical that we improve beneficial ownership information to understand exactly who benefits in a legal entity, and I think there has been some discussion about that from what I gathered before, and ensure that information is quickly available to law enforcement.

In May, Treasury's new customer due diligence requirements for financial institutions are going to go into effect. There has been some testimony here about the nature of that in terms of banks

having to identify and verify beneficial owners owning 25 percent or more of a legal entity as well as an individual on the management team. Some witnesses expressed concern about Treasury's implementation of these regulations. Some suggested that if there is not an actual 25 percent or more stake, there would be no one to list as a beneficial owner.

Ms. Mandelker, can you address these concerns and provide some additional detail on how Treasury plans to implement this new regulation?

Ms. MANDELKER. Well, again, as you mentioned, Senator, the rule is going to go into effect in May. I know a lot of financial institutions have been taking steps underway to make sure that they are complying with the rule.

In addition to the 25 percent beneficial ownership mandate, companies are also going to have to identify a controlling person that is resident within a particular entity. So it is not just the ownership trigger. It is also the controlling person that needs to be identified.

Senator MENENDEZ. So whether or not it is sufficient to establish 25 percent, the controlling person will have to be identified?

Ms. MANDELKER. A control person will have to be identified as well.

Senator MENENDEZ. Do you think that that will give you the breadth and scope necessary to make sure that we know who is the beneficial entity?

Ms. MANDELKER. I think it is a very important step. Of course, that is information that is going to go to the banks, so it is a requirement that the banks identify and verify who the beneficial owners are and who a controlling person is. And, of course, to the extent—and it will have the ability to obtain information as necessary and in the right circumstances from the banks.

Senator MENENDEZ. All right. Let me follow up on both Senator Warner's and Senator Donnelly's questions on cryptocurrencies. I am interested in your view on the use of virtual currencies by foreign sovereign states, like Russia and Venezuela, to evade sanctions. In recent months both Venezuela and Russia have expressed interest in state-backed virtual currencies. In December, Venezuelan President Maduro announced he is launching a virtual currency backed by the nation's oil reserves for the explicit purpose—this is what he stated—or circumventing sanctions imposed by the United States.

Now, perhaps lack of technological sophistication will delay or hamper this plan, but we know full well that Maduro will use every tool at his disposal to perpetuate his authoritarian objectives, so it is critical that we understand the risk here.

Do you believe that the Treasury Department is monitoring these developments? And do you have the technical tools and enforcement mechanisms to combat the use of cryptocurrencies to evade U.S. sanctions?

Ms. MANDELKER. So we are monitoring the developments. As I am sure you are aware, we have had a very active portfolio in the context of what Venezuela is doing. In addition to a very strong Executive order that the President issued in August, we have also been designating individuals who have enabled the Maduro regime

and committed what we think are a variety of different types of offenses.

When it comes to the resources and tools to make sure that we are monitoring virtual currency and cryptocurrency, we do have a dedicated team of individuals at Treasury who have the expertise to monitor these activities very carefully and closely. We are regulating this industry, which is very important. We are examining virtual currency exchangers along with the IRS——

Senator MENENDEZ. So my question is—OK, so now I appreciate and am glad to hear that you are monitoring it, but do you believe you have the tools and mechanisms necessary in place to combat the use of cryptocurrencies to evade U.S. sanctions?

Ms. MANDELKER. We do have tools and authorities in place to make sure that we are staying very much on top of this burgeoning industry.

Senator MENENDEZ. Nothing that you need?

Ms. MANDELKER. At this time, no, Senator.

Senator MENENDEZ. OK. Fair enough. Glad to hear that.

Finally, I am sure you are aware that FinCEN issued guidance in 2014 to clarify Bank Secrecy Act expectations and set the rules of the road for banks and financial institutions seeking to provide services to legitimate marijuana-related businesses in States that have legalized, and what I have heard, including from New Jersey institutions for which medical marijuana is legalized and now the State is considering the possibility of passing—legalizing the essence of recreational marijuana, is that there is a concern that, according to the Pew Charitable Trust, since the guidance was issued, the number of banks and credit unions serving businesses in the industry has more than tripled to nearly 400. Regardless of my views on this, if it is going to be legal in any State, I think it should be bankable and transactionable and we should be able to have eyes on it and understand revenues and how the money is flowing.

FinCEN's guidance has been critical to alleviating some of the public safety risks as well in terms of accumulation of large quantities of cash at dispensaries and businesses. And I worry that any steps to walk back this guidance only serves to undermine public safety.

So can you commit that this guidance is going to stay in place?

Ms. MANDELKER. We are reviewing the guidance in light of the Attorney General's recent decision to revoke a Justice Department memorandum on this issue. What the guidance did was it provided guidance to financial institutions with respect to what kinds of SARs they should file in different circumstances. The laws with respect to the Controlled Substances Act, of course, remain on the books. Those have not undertaken any changes. That would have to be done by the Congress.

Senator MENENDEZ. But when you are saying you are reviewing, does that mean that you find a conflict with FinCEN having the standards for banking transactions in States where the law permits these sales to take place or uses to take place, and that you see there is a conflict that would lead you to say, no, you cannot bank them anymore?

Ms. MANDELKER. I am not suggesting that there is a conflict or not a conflict. The guidance remains in place, and we are taking a look at it in light of the Justice Department's——

Senator MENENDEZ. Well, would you let us know if you move to change it?

Ms. MANDELKER. Yes, of course we would let you know.

Senator MENENDEZ. Thank you, Mr. Chairman, for your courtesy.

Chairman CRAPO. Thank you. And that is the last questioning. I have already given instructions on follow-up questions from Senators, and, again, I urge the witnesses to respond. I am sure we will be engaging with you as we move forward on this issue.

Thank you for testifying today, and that concludes our hearing.

[Whereupon, at 11:46 a.m., the hearing was adjourned.]

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

PREPARED STATEMENT OF SIGAL MANDELKER

UNDER SECRETARY, TERRORISM AND FINANCIAL INTELLIGENCE, DEPARTMENT OF THE TREASURY

JANUARY 17, 2018

Introduction

Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee, as the Under Secretary for Treasury's Office of Terrorism and Financial Intelligence (TFI), I am honored to appear before you today to discuss the critical work that TFI does to safeguard the United States and international financial systems.

The offices I lead are tasked with deploying our financial intelligence, expertise, and economic authorities to combat terrorist financing, money laundering, weapons proliferators, rogue regimes, human rights abusers, and other national security threats to the United States and our allies.

In 2004, Congress and the executive branch had the tremendous vision to combine under one roof a broad range of powerful economic tools, including sanctions, anti-money laundering (AML) measures, enforcement actions, foreign engagement, intelligence and analysis, and private sector partnerships, among others. We are the only country that combines these economic authorities within one office, which has proven invaluable in combating some of the most serious illicit finance and national security threats we face today.

Terrorist groups such as ISIS, al Qaeda, Hezbollah, and others seek to infiltrate the financial system to finance their activities and threaten our national security.

Rogue regimes in Iran, North Korea, and Venezuela continue to assault the integrity of the financial system, including by using deceptive financial practices to advance their corrupt, criminal, or terrorist aspirations. Russia continues to occupy Crimea and destabilize Ukraine, in violation of international norms of sovereignty.

These regimes, and many more, engage in human rights abuses and corruption, putting their own interests above the well-being of their people. That is why we are also targeting human rights abusers and the corrupt through authorities like the Global Magnitsky Human Rights Accountability Act. Simply put, the United States will not allow our financial system to be compromised by human rights abusers and corrupt actors who exploit innocent people around the world.

Transnational criminal organizations, drug kingpins, cyber criminals and others likewise seek out vulnerabilities in the global financial system, including by looking to use emerging technologies such as virtual currencies to launder their ill-gotten gains and advance their malicious enterprises.

These and other malign actors cannot operate without funding. Cutting off their access to the financial system requires calibrating our economic tools in strategic and complementary ways. TFI integrates our authorities and expertise across components, deploying the tools best suited to each challenge and achieving significant impact. The foundation of our economic authorities is a strong and robust anti-money laundering/combating the financing of terrorism (AML/CFT) regime.

Many of our efforts to identify and disrupt terrorist financiers, weapons proliferators, rogue regimes, and other illicit finance threats depend on financial institutions implementing the laws and regulations designed to protect the financial system. Financial intelligence reported to us by financial institutions serves as a key component of our efforts to target illicit actors.

One of my top priorities as Under Secretary for TFI is to ensure that the AML/CFT framework remains strong and effective. My testimony today will focus on both the threats that we face and the efforts we are undertaking to strengthen the AML/CFT framework in order to counter those challenges.

Threats to Our Financial System

We bring enormous economic power to bear against an array of law enforcement and national security threats. Below are just a few of the challenges we have been combating.

For example, North Korea uses covert representatives as well as front and trade companies to disguise, move, and launder funds that finance its weapons programs. The regime's illicit financial activity is not just conducted in dollars, nor is it limited to a handful of jurisdictions. Once a North Korean trade or financial representative successfully accesses a nation's financial system, illicit funds can flow indirectly through global banks, who may be unwittingly conducting currency clearing operations for North Korea.

We are laser-focused on detecting and disrupting these networks as part of the Administration's strategy to impose maximum pressure on North Korea. We are

deploying the full range of our economic authorities to combat the North Korean threat. Treasury has a cadre of analysts, including in the Office of Intelligence and Analysis (OIA) and the Financial Crimes Enforcement Network (FinCEN), who are mapping out these networks so that we can target and disrupt them.

There are now six North Korea-related executive orders, in addition to robust congressional authorities, that we use to target key North Korean financial middlemen and others who support the regime. Over the last year, Treasury's Office of Foreign Assets Control (OFAC) designated over 100 individuals and entities related to North Korea as part of our concerted effort to pressure the regime. Our recent action under Section 311 of the USA PATRIOT Act against Bank of Dandong, a Chinese bank facilitating North Korean money laundering and sanctions evasion, highlights our resolve to target key nodes of financial support for North Korea.

We are also warning financial institutions both here and abroad about the deceitful ways in which North Korea abuses the international financial system. In November 2017, FinCEN issued an advisory to alert financial institutions about North Korea's attempts to use front companies to launder money and evade sanctions. This information helps the private sector detect and report such activity, which in turn supports our efforts to target those persons and entities that help the regime fund its weapons program.

Our focus on depriving North Korea of its ability to earn and move revenue through the international financial system means that we must work with other countries to achieve this goal. Not only do we work bilaterally with key partners to coordinate our domestic sanctions programs, the Secretary, myself, and others within TFI engage with leaders across the world to stress the importance of implementing United Nations Security Council Resolutions (UNSCRs). We also work bilaterally with governments and through the Financial Action Task Force (FATF) and the G7 Financial Experts Group to ensure that countries have the regulatory framework in place to detect and freeze assets linked to North Korea. I raise these concerns in virtually every engagement I have with my foreign counterparts and with many financial institutions, and will do so again in my upcoming trip to Asia next week.

Iran is another rogue regime that seeks to subvert the financial system. It is the leading state sponsor of terrorism and finances terrorist groups such as Hezbollah and Hamas, the brutal regime of Bashar al-Assad, and a host of Shi'a militant groups in Bahrain, Iraq, Syria, and Yemen.

Like North Korea, Iran uses deceptive financial practices to generate revenue. As just one example, in November, we sanctioned an Islamic Revolutionary Guards Corps-Qods Force (IRGC–QF) network involved in a large-scale scheme to counterfeit Yemeni bank notes to support its destabilizing activities. This network employed deceptive measures to circumvent European export control restrictions and procured materials to print counterfeit bank notes potentially worth hundreds of millions of dollars.

In addition to Iran's financing of terrorism and other destabilizing activities, the IRGC has an extensive presence in Iran's economy, including in the energy, construction, mining, and defense sectors. In our engagements both here in the United States and abroad, we have made clear that companies doing business in Iran face substantial risks of transacting with the IRGC or IRGC-linked entities.

This risk is heightened by the lack of transparency in the Iranian economy, which is one of the least transparent in the world. Indeed, Iran is on the FATF's blacklist precisely because it has failed to address such systemic deficiencies in its controls to combat terrorist financing and money laundering. This has led the FATF to highlight for the past decade the terrorist financing risk emanating from Iran and the threat that it poses to the international financial system. Thus far, Iran has failed to fulfill its commitments to the FATF in addressing its weak controls.

We will continue to take action to protect the international financial system and to combat Iran's relentless campaign to support terrorism, destabilize the region, and abuse its own people. Over the last 2 weeks, OFAC designated 19 individuals and entities in connection with serious human rights abuses and censorship in Iran, and for assisting designated Iranian weapons proliferators. As Secretary Mnuchin stated when announcing last week's sanctions, the United States will not stand by while the Iranian regime continues to engage in human rights abuses and injustice.

In Venezuela, the Maduro regime's systematic destruction of democracy, as well as its endemic corruption, also pose a threat to the international financial system. Under Maduro, embezzlement, graft, and fraud have become the regime's de facto economic policy, aimed at maintaining the loyalty of the security apparatus to keep Maduro and his cronies in power. In August 2017, the President issued an Executive order carefully calibrated to deny the Maduro dictatorship a critical source of financing to maintain its illegitimate rule and protect the U.S. financial system from

complicity in Venezuela's corruption and in the impoverishment of the Venezuelan people, while still allowing for the provision of humanitarian assistance.

In September, FinCEN issued an advisory to alert financial institutions of widespread public corruption in Venezuela and the methods that senior political figures and their associates may use to move and hide proceeds of their ill-gotten gains, at the grave expense of the Venezuelan people. Combined with our powerful sanctions, this advisory put financial institutions on watch for possible illicit fund flows.

Endemic corruption also undermines the U.S. and international financial systems, perpetuating violent conflict and damaging economic markets. In the past year, we have imposed sanctions, issued financial advisories, and undertaken diplomatic engagements to counter corruption across the globe. Building on the Global Magnitsky Act, which Congress passed just over 1 year ago, the President signed an Executive order on December 20, 2017, declaring a national emergency with respect to human rights abuses and corruption globally and enabling Treasury to impose financial sanctions on malign actors engaged in these activities.

In this Executive order, the President imposed sanctions on 13 serious human rights abusers and corrupt actors, and OFAC simultaneously imposed sanctions on an additional 39 affiliated individuals and entities under the newly issued Order. Since this action, we have seen public reports regarding the notable impact of these sanctions, with some of the designated individuals being cutoff from lucrative business arrangements, while others face investigation by their home governments.

TFI has also been deploying its authorities against transnational criminal organizations, fraud, cybercriminals, human trafficking networks, and other law enforcement priorities in which our economic tools have had a meaningful impact. In recent years, for example, we have issued geographic targeting orders (GTOs) aimed at combating tax refund fraud and sophisticated trade-based money laundering schemes orchestrated by drug trafficking networks and their money launderers.

To mitigate the money laundering vulnerabilities associated with luxury real estate, in 2016 we issued GTOs to identify the beneficial owners behind shell companies used to pay all-cash for high-end residential real estate in certain U.S. cities. In 2017, following the enactment of the Countering America's Adversaries through Sanctions Act, FinCEN revised the GTOs to capture a broader range of transactions and include transactions involving wire transfers. The information gathered from the GTOs supports law enforcement and helps inform our broader approach to mitigating the money laundering vulnerabilities in the real estate sector.

Strengthening the AML/CFT Framework

As we employ our economic tools to address these challenges, we must continue to increase the transparency and accountability in the financial system, which underpins much of our economic statecraft. A strong and effective AML/CFT framework keeps illicit actors out of the financial system, and allows us to track and target those who nonetheless slip through. This framework must address the evolving forms of illicit finance threats that we face.

As such, we are taking a hard look not only at the Bank Secrecy Act (BSA) but also at the broader AML/CFT regime. We need to continuously upgrade and modernize our system—a statutory and regulatory construct originally adopted in the 1970s—and make sure that we have the right framework in place to take us into the 2030s and beyond.

Incentivizing Innovation

In particular, we must make sure that financial institutions are devoting their resources toward high value activities and are encouraged to innovate with new technologies and approaches. In recent years, for example, financial institutions have become more proactive in their AML/CFT approach, in some cases building sophisticated internal financial intelligence units devoted to identifying strategic and cross-cutting financial threats. Financial institutions have been improving their ability to identify customers and monitor transactions by experimenting with new technologies that rely on artificial intelligence and machine learning. Institutions are also working together to share information on suspicious activities, enabling them to identify and report activity that would not otherwise be visible or concerning to a single institution.

We laud and encourage these innovations. These initiatives advance the BSA's underlying purpose. We are working closely with our counterparts at the Federal Banking Agencies (FBAs) to discuss ways to further incentivize financial institutions to be innovative in combating financial crime. We have also been speaking with many in the financial community to understand their perspectives.

Public-Private Partnerships

Deploying our tools for maximum impact requires proactive dialogue and information sharing with financial institutions. They are on the front lines, detecting and blocking illicit financing streams, combating financial crimes, and managing risk. The safeguards employed by the private sector, and the information reported about terrorist financiers, weapons proliferators, human rights abusers and traffickers, and cyber and other criminals, help prevent malign actors from abusing our financial system.

Enhancing public-private partnerships that reveal and mitigate vulnerabilities is one of our top priorities. To make these partnerships work, we are arming the private sector with information that enhances their ability to identify and report suspicious activity. We have also been issuing advisories to warn financial institutions about illicit finance risks.

I have heard from my outreach with financial institutions here and abroad how this information helps them better prioritize targets and utilize their limited resources. That is why last month I announced the launch of FinCEN Exchange, a new public-private information sharing program led by FinCEN.

FinCEN Exchange brings financial institutions, FinCEN, and law enforcement together to facilitate greater information sharing between the public and private sectors.

Information sharing should be a two-way street. As part of FinCEN Exchange, we are convening regular briefings—at least once every 6–8 weeks—with law enforcement, FinCEN, and financial institutions to exchange targeted information on priority illicit finance threats. In close coordination with law enforcement, our goal is to provide information to support specific matters through Section 314(a) of the USA PATRIOT Act and other authorities, and also to provide financial institutions with broader typologies to help them identify illicit activity. These types of exchanges enable the private sector to better identify risks and provide FinCEN and law enforcement with critical information to disrupt money laundering and other financial crimes.

I have seen firsthand the immense value of this public-private partnership. Information provided by financial institutions in connection with public-private briefings has helped us map out and target weapons proliferators, sophisticated global money laundering operations, human trafficking and smuggling rings, and corruption and trade-based money laundering networks, among others. This also creates a positive feedback loop in which we can share with the broader financial community the typologies learned from these exchanges, enabling other financial institutions to identify and report similar activity.

Through FinCEN Exchange, we are increasing public-private information sharing, which will include financial institutions of all types and sizes across the country.

We are also discussing BSA reform with the private sector, including in the Bank Secrecy Act Advisory Group (BSAAG). The BSAAG, chaired by FinCEN, is comprised of members from financial institutions, trade groups, and State and Federal regulators and law enforcement. The topics addressed in the BSAAG include identifying metrics for determining effective financial reporting, streamlining the reporting of money laundering "structuring" transactions, and more efficient ways for industry to report cash transactions.

Promoting Information Sharing Among Financial Institutions

Public-private partnerships are even more effective when financial institutions share information with each other. Money launderers are sophisticated. They move across borders and financial institutions, and financial institutions are better able to keep pace and effectively combat them when they communicate with each other.

Some institutions have started forming consortia to share information more dynamically under Section 314(b) of the USA PATRIOT Act, which provides safe harbor for financial institutions to voluntarily share information related to money laundering or terrorist activities. We are highly encouraged by, and supportive of, the private sector's willingness to engage in this type of exchange. By working together, these groups of financial institutions are directly assisting our efforts to identify and disrupt streams of financing for North Korea and other top illicit finance threats.

Evolving Threats

Part of our effort to update the AML/CFT regime includes staying ahead of evolving threats. We lead the world in mitigating the illicit finance risks of emerging technologies, such as the use of virtual currencies. We stand at the regulatory and supervisory forefront of this emerging industry. Currently, the United States, Japan, and Australia are among the few countries regulating virtual currency

payments/exchange activities, including in particular decentralized convertible virtual currency, for AML/CFT purposes.

To ensure that virtual currency providers and exchangers know the rules and follow them, FinCEN has prioritized engagement with—and examination of—these entities, focusing both on the approximately 100 that have registered with FinCEN as money transmitters as required, as well as those that have not. As part of the examination process, FinCEN, working with delegated Internal Revenue Service (IRS) examiners, has recommended virtual currency providers and exchangers take certain actions to improve their compliance activities.

The effectiveness of this structure depends on compliance by the regulated entities, and so we aggressively pursue virtual currency exchangers and others who do not take these obligations seriously. In July 2017, for example, FinCEN assessed a $110 million fine against BTC–e, an internet-based, foreign-located money transmitter that exchanges fiat currency as well as the convertible virtual currencies Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash. At the time of our action, it was one of the largest virtual currency exchanges by volume in the world and facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. FinCEN also assessed a fine against Russian national Alexander Vinnik, one of the operators of BTC–e, for his role in the violations.

This action sends a very powerful message that we will hold accountable virtual currency exchangers that violate our AML laws, wherever they are located. We will do so in conjunction with our law enforcement partners and foreign counterparts.

We understand that the European Union is finalizing its amendments to its anti-money laundering directive, which will put in place a requirement for EU members to regulate virtual currency exchangers, a significant step. Even with these advancements, there is still a major gap in regulating these entities globally and we are actively engaged with other countries, bilaterally and multilaterally, to encourage them to apply international AML/CFT standards to virtual currency payments.

We also prioritize increasing the transparency of shell companies in the U.S. financial system. To that end, we have strengthened one of the fundamental components of our AML/CFT regime: customer due diligence. Treasury's customer due diligence rule, which takes effect this May, requires covered financial institutions to identify and verify the identity of the beneficial owners of companies at the time of account opening. We look forward to working with Congress on the important issue of enhancing the transparency of beneficial owners.

As we call upon the private sector to enhance its systems, we at TFI are doing the same. Financial intelligence is central to our efforts to combat the national security threats I outlined above. As such, I have directed my staff to work innovatively on employing new tools to analyze and use information more effectively. Last month, I established a Technology Council, which, among other things, is implementing new technologies to further enhance our analytic capabilities.

Conclusion

I am grateful for this Committee's leadership and support, both of which are essential to combating the threats we face and ensuring the continued success of TFI. I look forward to working with this Committee and other Members of Congress as we seek to fulfill our shared responsibility to keep Americans safe and secure. I look forward to your questions.

PREPARED STATEMENT OF M. KENDALL DAY

ACTING DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

JANUARY 17, 2018

Chairman Crapo, Ranking Member Brown, and Members of the Committee. Thank you for the opportunity to discuss our Nation's anti-money laundering (AML) laws. They constitute one of the pillars of our national security strategy, while also serving as a critical element of our transparent and robust financial system.

As economies and financial systems become increasingly global, so too do the criminal organizations and other bad actors who attempt to exploit them. Transnational criminal organizations, kleptocrats, cybercriminal groups, terrorists, drug cartels, and alien smugglers alike must find ways to disguise the origins of the proceeds of their crimes so that they can use the profits without jeopardizing their source. These criminal actors and their illicit proceeds—which best estimates peg at more than $2 trillion annually are a global problem. But this is a global problem with acute and specific effects here in the United States, where we enjoy some

of the deepest, most liquid, and most stable markets in the world. Those features of the U.S. financial system attract legitimate trade and investment, foster economic development, and promote confidence in our markets and in our Government. Those same advantages, however, also attract criminals and their illicit funds as they seek to launder their proceeds to enjoy the fruits of their crimes, or to promote still more criminal activity.

One of the most effective ways to deter criminals and to stem the harms that flow from their actions—including harm to American citizens and our financial systems—is to follow the criminals' money, expose their activity, and prevent their networks from benefiting from the enormous power of our economy and financial system. Identifying and disrupting illicit financial networks not only assists in the prosecution of criminal activity of all kinds, but also allows law enforcement to halt and dismantle criminal organizations and other bad actors before they harm our citizens or our financial system. More broadly, money laundering undermines the rule of law and our democracy because it supports and rewards corruption and organized crime, allowing it to grow and fester. Our efforts to combat money laundering thus directly affect the safety and security of the American public, and the stability of our Nation.

The Department of Justice (Department), in coordination with our colleagues from other agencies—one of whom is here today—as well as our international law enforcement partners, has had numerous recent successes in thwarting criminals who sought to move, hide, or otherwise shelter their criminal proceeds using the U.S. financial system. Despite our successes, criminals continue to exploit gaps and vulnerabilities in existing laws and regulations to find new methods to conduct their illicit transactions and abuse and weaken our financial system and economy, causing real harm to our country and its citizens. Thus, it is imperative that domestic and international law enforcement, policymakers, regulators, and industry continue to work together to implement and enforce strong AML laws to detect, target, and disrupt illicit financial networks that threaten our country.

I. Background

Crime is big business. The U.N. Office on Drugs and Crime estimates that annual illicit proceeds total more than $2 trillion globally. Here in the United States, proceeds of crimes, excluding tax evasion, were estimated to total approximately $300 billion in 2010, or about 2 percent of the overall U.S. economy at the time. Of that $300 billion, drug trafficking sales in the United States generate an estimated $64 billion annually. Fraud, human smuggling, organized crime, and public corruption also generate significant illicit proceeds.

For any illegal enterprise to succeed, criminals must be able to hide, move, and access the proceeds of their crimes. And they must find ways to do so without jeopardizing their ongoing criminal activities. Without usable profits, the criminal activity cannot continue. This is why criminals resort to money laundering.

Money laundering involves masking the source of criminally derived proceeds so that the proceeds appear legitimate, or masking the source of monies used to promote illegal conduct. Money laundering generally involves three steps: placing illicit proceeds into the financial system; layering, or the separation of the criminal proceeds from their origin; and integration, or the use of apparently legitimate transactions to disguise the illicit proceeds. Once criminal funds have entered the financial system, the layering and integration phases make it very difficult to track and trace the money.

II. Specific Money Laundering Threats

Criminals employ a host of methods to launder the proceeds of their crimes. Those methods range from well-established techniques for integrating dirty money into the financial system, such as the use of cash, to more modern innovations that make use of emerging technologies to exploit vulnerabilities. Some of the more well-known methods of money laundering are described below.

Illicit cash. Cash transactions are particularly vulnerable to money laundering. Cash is anonymous, fungible, and portable; it bears no record of its source, owner, or legitimacy; it is used and held around the world; and is difficult to trace once spent. Additionally, despite its bulk, cash can be easily concealed and transported in large quantities in vehicles, commercial shipments, aircrafts, boats, luggage, or packages; in special compartments hidden inside clothing; or in packages wrapped to look like gifts. Criminals regularly attempt to smuggle bulk cash across the United States' borders using these and other methods.

Cash-intensive sources of illicit income include human smuggling, bribery, contraband smuggling, extortion, fraud, illegal gambling, kidnapping, prostitution, and tax evasion. Drug trafficking, however, is probably the most significant single source of

illicit cash. Customers typically use cash to purchase drugs from street-level drug dealers, who in turn use cash to purchase their drug supply from mid-level distributors. Mid-level distributors purchase drugs from wholesalers using cash, and wholesalers often make payment to their suppliers in cash. Mexican drug trafficking organizations responsible for much of the United States' drug supply commonly rely on multiple money laundering methods, including bulk cash smuggling, to move narcotics proceeds across the U.S.-Mexico border into Mexico.

Trade-based money laundering. Drug trafficking organizations also use money brokers to facilitate trade-based money laundering. In complex trade-based money laundering schemes, criminals move merchandise, falsify its value, and misrepresent trade-related financial transactions, often with the assistance of complicit merchants, in an effort to simultaneously disguise the origin of illicit proceeds and integrate them into the market. Once criminals exchange illicit cash for trade goods, it is difficult for law enforcement to trace the source of the illicit funds.

This particular method of money laundering harms legitimate businesses. For example, the U.S. Department of Treasury's (Treasury) National Money Laundering Assessment (2015) notes that transnational criminal organizations may dump imported goods purchased with criminal proceeds into the market at a discount just to expedite the money laundering process, putting legitimate merchants at a competitive disadvantage.

Illicit use of banks. U.S. banks handle trillions of dollars of daily transaction volume. Most Americans use depository financial institutions—such as commercial banks, savings and loan associations, and credit unions—to conduct financial transactions. Those who do not have access to these institutions, or who choose not to use depository financial institutions, may conduct financial transactions using money services businesses such as money transmitters, check cashers, currency exchangers, or businesses that sell money orders, prepaid access devices, and traveler's checks. Some money services businesses themselves may also engage the services of depository financial institutions to settle transactions. Banks may also hold accounts with other banks, including foreign banks, to facilitate domestic and cross-border transactions. For example, some banks establish correspondent relationships with other banks to enable them to conduct business and provide services to clients in foreign countries without the expense of establishing a presence in those foreign countries.

The sheer volume of business that banks handle on a daily basis exposes them to significant money laundering risks. In fact, in most money laundering cases, criminals employ banks at some point to hold or move illicit funds.

Because they play such a significant role in the U.S. financial system, financial institutions are often the front line in AML efforts. Compliance with the Bank Secrecy Act and sanctions laws is fundamental to protecting the security of financial institutions and the integrity of the financial system as a whole. These laws impose a range of obligations on financial institutions, including filing of transaction reports, reporting suspicious activity, performing customer due diligence, preventing transactions that involve the proceeds of crimes, and establishing effective AML programs.

Effective AML programs play a critical role in the fight against criminal activity. For example, effective AML programs help financial institutions detect efforts to launder illicit proceeds, which can, in turn, prevent those funds from ever entering the U.S. financial system.

Accurate and timely suspicious activity reporting can be a critical source of information for law enforcement investigations. Further, domestic collection of AML information improves the United States' ability to respond to similar requests from foreign law enforcement for investigative assistance, thus increasing our ability to fight financial crime on the global stage.

The Bank Secrecy Act's requirements are designed to help ensure that banks avoid doing business with criminals. However, criminals frequently seek to thwart or evade these requirements. For example, criminals may structure cash deposits to avoid threshold reporting requirements, or seek out complicit merchants who will accept their illicit proceeds without reporting the transactions. Criminals may also misuse correspondent banking services to further their illicit purposes. Because U.S. banks may not have a relationship with the originator of a payment when they receive funds from a correspondent bank, banks may face additional challenges in evaluating the money laundering risks associated with those transactions. When criminals successfully deploy these techniques, they are one step closer to "cleaning" their illicit proceeds—with significant consequences for our financial system.

Obscured beneficial ownership. Increasingly, sophisticated criminals seek access to the U.S. financial system by masking the nature, purpose, or ownership of their accounts and the sources of their income through the use of front companies,

shell companies, or nominee accounts. Front companies typically combine illicit proceeds with lawful proceeds from legitimate business operations, obscuring the source, ownership, and control of the illegal funds. Shell companies typically have no physical operations or assets, and may be used only to hold property rights or financial assets. Nominee-held "funnel accounts" may be used to make structured deposits in multiple geographic locations and corresponding structured withdrawals in other locations. All of these methods obscure the true owners and sources of funds. And without truthful information about who owns and controls an account, banks may not be able to accurately analyze account activity and identify legitimate (or illegitimate) transactions.

Misuse of money services businesses. While many money services businesses engage in legitimate business activities, they, too, can serve as a means for criminals to move money. Although money services businesses have customer verification requirements above certain thresholds and other Bank Secrecy Act obligations, individuals who use money services businesses may do so in a one-off fashion, without establishing an ongoing relationship that banks maintain with their customers, which can make it more difficult to identify money laundering. While money services businesses are subject to Bank Secrecy Act compliance requirements, some money services businesses fail to register with the proper authorities, making it more likely that AML violations at those money services businesses go undetected.

Prepaid access cards. Prepaid access cards, also known as stored value cards, may be used as an alternative to cash. Prepaid access cards provide access to funds that have been paid in advance and can be retrieved or transferred through an electronic device such as a card, code, serial number, mobile identification number, or personal identification number. They function much like traditional debit or credit cards, and can provide portable and absent regulation, potentially anonymous ways to access funds.

Prepaid access cards may be used by criminals in a variety of ways. Criminals can direct Federal or State tax authorities to issue fraudulent tax refunds on prepaid debit cards. Drug traffickers, meanwhile, may convert drug cash to prepaid debit cards, which they may then use to purchase goods and services or send to drug suppliers, where they can use the cards to withdraw money from a local ATM.

Virtual currencies. Virtual currencies offer yet another alternative to cash. Criminals seek to use virtual currencies to conduct illicit transactions because they offer potential anonymity, since virtual currency transactions are not necessarily tied to a real world identity and enable criminals to quickly move criminal proceeds among countries. Some of those countries, unlike the United States, do not currently regulate virtual currencies and therefore have limited oversight and few AML controls.

Purchase of real estate and other assets. Criminals may also convert their illicit proceeds into clean funds by buying real estate and other assets. Foreign government officials who steal from their own people, extort businesses, or seek and accept bribery payments, in particular, have used this method to funnel their illicit gains into the U.S. financial system. Recent investigations and prosecutions have revealed that corrupt foreign officials have purchased various U.S. assets to launder the proceeds of their corruption, from luxury real estate and hotels to private jets, artwork, and motion picture companies. The flow of kleptocracy proceeds into the U.S. financial system distorts our markets and threatens the transparency and integrity of our financial system. For example, when criminals use illicit proceeds to buy up real estate, legitimate purchasers—businesses and individuals—are foreclosed from buying or investing in those properties. Moreover, kleptocracy erodes trust in Government and private institutions, undermines confidence in the fairness of free and open markets, and breeds contempt for the rule of law, which threatens our national security.

Those are only a few of the methods criminals use to launder ill-gotten gains through the U.S. financial system. New methods are always being devised, as the criminal underworld seeks to take advantage of emerging technologies and to outpace the development of new detection and investigation tools by law enforcement.

III. The Department's Efforts to Combat the Threat

To keep pace with and disrupt the evolving threats of money laundering, the Department draws on the full complement of its law enforcement tools. The Criminal Division's Money Laundering and Asset Recovery Section (MLARS) leads the Department's AML efforts. MLARS works in parallel with U.S. Attorneys' Offices around the country, other Government agencies, and domestic and international law enforcement colleagues to pursue complex, sensitive, multi-district, and international money laundering and asset forfeiture investigations and cases. MLARS' Bank Integrity Unit, for example, investigates and prosecutes criminal cases involv-

ing financial institutions and their employees or agents who violate Federal criminal statutes, including the Bank Secrecy Act, the Money Laundering Control Act, and economic and trade sanctions authorized by the International Emergency Economic Powers Act and the Trading with the Enemy Act. MLARS' Money Laundering and Forfeiture Unit investigates and prosecutes professional money launderers who provide their services to criminal organizations, such as Mexican drug cartels, and, in partnership with U.S. Attorneys' Offices, litigates criminal and civil forfeiture cases.

In addition—and as part of its efforts to fight global corruption and money laundering on the international stage—MLARS leads the Department's Kleptocracy Asset Recovery Initiative. Large-scale corruption by foreign government officials who steal from their people and seek to invest those funds in the U.S. financial system erodes citizens' trust in Government and private institutions alike, undermines confidence in the fairness of free and open markets, and breeds contempt for the rule of law. When kleptocracy is allowed to take root, organized criminal groups and even terrorists are soon to follow. Accordingly, this initiative seeks to protect the U.S. financial system from the harmful effects of large flows of corruption proceeds, and, whenever possible, to return stolen or illicit funds for the benefit of the citizens of the affected countries.

Also instrumental in the Department's AML efforts are the Criminal Division's Fraud Section, Computer Crimes and Intellectual Property Section, Narcotic and Dangerous Drug Section, and Organized Crime and Gang Section; the Tax Division; the Civil Rights Division's Human Trafficking Prosecution Unit; and their U.S. Attorneys' Office partners. These prosecutors lend critical expertise in the predicate offenses involved in money laundering. They work in tandem with a host of domestic law enforcement partners—among them, the Federal Bureau of Investigation (FBI); the DEA; the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Department of Homeland Security, U.S. Immigration and Customs Enforcement-Homeland Security Investigations (HSI); U.S. Secret Service; and the Internal Revenue Service-Criminal Investigations (IRS–CI)—as well as State, local, tribal, and international law enforcement partners. Agents investigate a range of financial fraud schemes, including health care fraud, false claims for Federal income tax refunds, and identify theft and other internet-related schemes. They also investigate drug trafficking organizations and organized crime groups responsible for alien smuggling, extortion, illegal gambling, prostitution, and racketeering, among other crimes.

In July 2017, for example, Attorney General Jeff Sessions and the Department of Health and Human Services (HHS) announced the largest-ever healthcare fraud enforcement action by the Medicare Fraud Strike Force. Investigating agencies included the FBI, and HHS–Office of the Inspector General, with the assistance of the DEA, U.S. Department of Defense-Office of Inspector General-Defense Criminal Investigative Service, and State Medicaid Fraud Control Units. The Criminal Division's Fraud Section, with its strike force partners, led a series of coordinated actions that charged 412 defendants across 41 Federal judicial districts with crimes stemming from their participation in health care fraud schemes involving $1.3 billion in false billings.

Interagency task forces, including those that fall under the umbrella of the Organized Crime Drug Enforcement Task Forces program, similarly play a critical role in the Department's investigation and prosecution of the money laundering of drug traffickers. They draw upon the resources of Federal, State, local, and tribal law enforcement partners to identify, target, and dismantle drug trafficking organizations that seek to launder illicit drug proceeds through the U.S. financial system.

U.S. law enforcement wields a number of powerful tools in the fight against criminals who engage in money laundering:

First and foremost, criminal money laundering charges are of course essential to the Department's efforts to disrupt and dismantle criminal organizations' financial networks. Federal prosecutors have secured, on average, more than 1,200 Federal money laundering convictions each year, and have successfully investigated and prosecuted complex, global, and high-value money laundering cases.

For example, in June 2017, MLARS and the U.S. Attorney's Office for the Eastern District of New York secured the guilty plea of Jorge Luis Arzuaga, a private banker formerly employed by several Swiss banks on money laundering conspiracy charges stemming from the distribution and receipt of millions of dollars of bribes paid to high-ranking soccer officials. Arzuaga furthered the bribery conspiracy by opening a bank account in the name of a shell company ostensibly established on behalf of a sports marketing company, when in fact, the true beneficial owner of the account was a high-ranking soccer official. In exchange for facilitating more than $25 million in bribe payments to the soccer official through this account, Arzuaga received more than $1 million in bonus payments.

In 2016, moreover, MLARS and the U.S. Attorney's Office for the Southern District of California successfully prosecuted a drug trafficking and money laundering organization based primarily in Tijuana and Culiacan, Sinaloa, Mexico. The organization smuggled cocaine, heroin, methamphetamine, and marijuana from Mexico to the United States for distribution and arranged for the proceeds to be smuggled from the United States to Mexico, where a portion was laundered through money exchange houses in Culiacan and Tijuana. The remaining currency was sent back to the United States, deposited at banks, and wire transferred to bank accounts controlled by the organization in Mexico. The total amount laundered by the organization is believed to have exceeded $100,000,000. That figure included approximately $45,000,000 wired from U.S. bank accounts to accounts in Mexico and at least another $28,000,000 smuggled through Southern California ports of entry into Mexico.

Criminal charges against financial institutions complicit in money laundering are likewise a component of the Department's AML strategy. In considering how a criminal enterprise was able to move illegal proceeds through the financial system, prosecutors and agents necessarily ask: Were the criminals just lucky, or did a financial institution fail to implement an effective AML program? Today's investigations often look at which companies processed the payments, which banks held the relevant accounts, whether any automated alerts or Suspicious Activity Reports were (or should have been) filed in connection with the movement of funds, and who served as the financial advisors, the tax preparers, and the accountants. In appropriate cases, prosecutors have brought actions against financial institutions for criminal violations of the Bank Secrecy Act and anti-fraud statutes.

For instance, in 2017, a global money services business admitted to criminal violations, including willfully failing to maintain an effective AML program and aiding and abetting wire fraud, through agreements with the Department, the Federal Trade Commission, and four U.S. Attorneys' Offices. Specifically, the money services business admitted to processing payments between 2004 and 2012 for fraudsters who posed as family members in need or who had promised prizes or job opportunities and directed victims of their scams to send money through the business. Some of the money services business's employees were complicit in the schemes, processing the fraud payments in return for a cut of the proceeds. And the money services business knew of the agents' involvement, yet failed to take corrective action against them.

Beyond criminal charges, civil penalties and forfeiture are additional tools in the Department's AML efforts. Civil forfeiture gives law enforcement the ability to go after what criminals value most—the money and property motivating their crimes—and to remove the proceeds of crime and other assets used to perpetuate criminal activity. It is a critical tool when prosecutors have no jurisdiction over culpable persons but have jurisdiction over property obtained through their criminal activity because it is located in the United States.

The Department also uses targeted financial sanctions in conjunction with criminal and civil prosecutions. The Department works closely with Treasury and other agencies to impose financial sanctions where appropriate-measures that are particularly useful when criminals have evaded arrest or are otherwise outside the jurisdiction of the United States. For example, Treasury's Office of Foreign Assets Control (OFAC) may level significant economic sanctions against individual drug traffickers under the Foreign Narcotics Kingpin Designation Act, and against transnational criminal organizations under Executive Order 13581. Section 311 of the USA PATRIOT Act authorizes Treasury, through its Financial Crimes Enforcement Network (FinCEN), to require domestic financial institutions and agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern. Special measures include, among other actions, enhanced recordkeeping and reporting requirements, the collection of beneficial ownership information, or prohibitions on banks from opening or maintaining in the United States any correspondent account or payable-through account for or on behalf of a foreign financial institution. Such economic sanctions can help freeze money launderers' financial accounts, block their U.S. properties, and deny them access to the U.S. financial system.

Forfeiture and sanctions authorities have been deployed in a number of recent money laundering prosecutions. In August 2017, the Department announced the filing of two complaints seeking the imposition of a civil money penalty and the civil forfeiture of more than $11 million from companies that allegedly facilitated financial transactions for North Korea. These companies did so by brokering the sale of North Korean coal, transferring the proceeds of those sales to front company accounts, and using those front companies and the coal proceeds to purchase goods and services for North Korea. The complaints allege that the front companies

supported OFAC-sanctioned North Korean entities, including North Korean military and North Korean weapons programs—direct threats to our national security.

In 2016, the Department announced the filing of criminal charges and civil forfeiture actions against four Chinese nationals and a China-based trading company for conspiring to evade U.S. economic sanctions and violating the Weapons of Mass Destruction Proliferators Sanctions Regulations (WMDPSR). Simultaneously, OFAC imposed sanctions on the defendants for their ties to the government of North Korea's weapons of mass destruction proliferation efforts. The defendants used front companies to facilitate prohibited transactions through the United States on behalf of a sanctioned entity in North Korea with ties to sanctioned weapons of mass destruction proliferators.

Similarly, in the Liberty Reserve case in 2013, the Department's filing of criminal charges against the web-based money transfer system was coupled with regulatory action by Treasury. FinCEN announced that, in coordination with the unsealing of the criminal indictment, Liberty Reserve had been named as a financial institution of primary money laundering concern under Section 311, effectively blocking its access to the U.S. financial system.

Civil forfeiture has also been critical to the success of the Kleptocracy Asset Recovery Initiative, which has seized or restrained $3.5 billion worth of corruption proceeds to date and has filed complaints seeking the restraint of assets in a range of other high-profile matters. These include actions seeking to recover more than $1.7 billion in assets allegedly associated with a Malaysian sovereign wealth fund, more than $850 million allegedly related to bribe payments made by the world's sixth-largest telecommunications company and other firms, and more than $140 million allegedly obtained through corrupt oil contracts awarded by Nigeria's former Minister for Petroleum Resources. These cases demonstrate that the Department will not let corruption undermine and destabilize our markets, the rule of law, or democracy.

In the Malaysia matter—the largest single action ever brought under the Initiative—the Department filed a complaint in 2016 to forfeit and recover assets associated with an international conspiracy to launder more than $4.5 billion stolen from the country's sovereign wealth fund, known as 1Malaysia Development Berhad, or 1MDB. The Malaysian government created 1MDB to promote economic development through international partnerships and foreign direct investment, with the ultimate goal of improving the lives of the Malaysian people. However, corrupt 1MDB officials treated this public trust as a personal bank account.

Between 2009 and 2015, those corrupt officials and their associates took more than $4.5 billion from the development fund in four phases. These funds were laundered through a complex web of opaque transactions and fraudulent shell companies with bank accounts in countries around the world, including Switzerland, Singapore, Luxembourg, and the United States. The funds were then used to purchase approximately $1.7 billion in assets that the Department seeks to recover, including a $261 million, 350-foot yacht; a $35 million jet; masterpieces by Van Gogh, Picasso, and Monet; and a motion picture company that used the funds to finance, among other things, the production of the films "The Wolf of Wall Street," "Daddy's Home," and "Dumb and Dumber To." MLARS and the U.S. Attorney's Office in Los Angeles filed civil complaints targeting assets that, according to court documents, were misappropriated and diverted by Malaysian officials and their associates from 1MDB. In June 2017, the Department announced additional steps to forfeit and recover assets, bringing the total assets subject to forfeiture in this case to more than $1.7 billion. If the United States is successful in court, we will forfeit this more than $1.7 billion in property, liquidate it, and, ultimately, return as much as possible to the citizens of Malaysia.

IV. Challenges in Pursuing and Prosecuting Money Laundering Cases

Notwithstanding the Department's many successes, Federal prosecutors and investigators continue to face significant challenges in bringing to justice those who threaten our financial system and national security by laundering the proceeds of their crimes.

A. Opaque Corporate Structures

The pervasive use of front companies, shell companies, nominees, or other means to conceal the true beneficial owners of assets is one of the greatest loopholes in this country's AML regime. Except in very narrow circumstances, current Federal laws do not require identification of beneficial owners at account opening. Although banks are required to obtain certain types of customer account information during the account-opening process, those requirements do not address the conduct of bad actors who make misrepresentations to banks to achieve their illicit purposes.

The Financial Action Task Force (FATF), the inter-governmental body responsible for developing and promoting policies to protect the global financial system against money laundering and other threats, highlighted this issue as one of the most critical gaps in the United States' compliance with FATF standards in an evaluation conducted last year. FATF noted that the lack of beneficial ownership information can significantly slow investigations because determining the true ownership of bank accounts and other assets often requires that law enforcement undertake a time-consuming and resource-intensive process. For example, investigators may need grand jury subpoenas, witness interviews, or foreign legal assistance to unveil the true ownership structure of shell or front companies associated with serious criminal conduct. Moreover, the failure to collect beneficial ownership information also undermines financial institutions' ability to determine which of their clients pose compliance risks, which in turn harms banks' ability to comply with their legal obligation to guard against money laundering.

A recent case involving Teodoro Nguema Obiang Mangue, the Second Vice President of Equatorial Guinea, highlights the challenge of successfully prosecuting money laundering schemes when parties have concealed the true ownership of bank accounts and assets. In that case, Nguema Obiang reported an official government salary of less than $100,000 a year during his 16 years in public office. Nguema Obiang, however, used his position and influence to amass more than $300 million in assets through fraud and corruption, money which he used to buy luxury real estate and vehicles, among other things. Nguema Obiang then orchestrated a scheme to fraudulently open and use bank accounts at financial institutions in California to funnel millions of dollars into the United States. Because U.S. banks were unwilling to deal with Nguema Obiang out of concerns that his funds derived from corruption, Nguema Obiang used nominees to create companies that opened accounts in their names, thus masking his relationship to the accounts and the source of the funds brought into the United States. The Department ultimately reached a settlement of its civil forfeiture actions against assets owned by Nguema Obiang. However, the Department needs effective legal tools to directly target these types of fraudulent schemes and protect the integrity of the U.S. financial system from similar schemes.

The Treasury Department's recent Customer Due Diligence Final Rule (CDD rule) is a critical step toward a system that makes it difficult for sophisticated criminals to circumvent the law through use of opaque corporate structures. Beginning in May 2018, the CDD rule will require that financial institutions collect and verify the personal information of the beneficial owners who own, control, and profit from companies when those companies open accounts. The collection of beneficial ownership information will generate better law enforcement leads and speed up investigations by improving financial institutions' ability to monitor and report suspicious activity, and will also enable the United States to better respond to foreign authorities' requests for assistance in the global fight against organized crime and terrorism.

Important as it is, however, the CDD rule is only one step toward greater transparency. More effective legal frameworks are needed to ensure that criminals cannot hide behind nominees, shell corporations, and other legal structures to frustrate law enforcement, including stronger laws that target individuals who seek to mask the ownership of accounts and sources of funds.

B. Evidence Collection Involving Foreign Entities

The assistance of our interagency and international partners is an important element of the Department's success in its AML efforts. Because money often moves across multiple countries in the global economy, U.S. law enforcement depends on the cooperation of foreign counterparts to aggressively investigate money laundering cases touching the United States. Domestic and international law enforcement partners must work together to obtain evidence and to trace, freeze, and seize assets wherever they are located. The ability to pursue investigative leads in transnational criminal investigations and terrorist financing cases using foreign bank records is vital to successful AML efforts on the international stage.

Recent cases reinforce this need. The Department's 2017 complaints against the companies that sought to help North Korea circumvent the U.S. sanctions—noted above—allege that sanctioned North Korean entities were able to send financial transactions in U.S. dollars through U.S. correspondent banks without detection and thereby avoided being blocked under the WMDPSR program. In these and similar cases, foreign bank records may be of great benefit in demonstrating potentially illicit conduct.

Under the existing authority in Title 31 U.S.C. § 5318(k), however, foreign banks are not required to produce records in a manner that would establish their authenticity and reliability for evidentiary purposes. The statute also does not contain any

anti-tip-off language, meaning that banks who receive subpoenas could disclose the subpoenas to account holders or others, thereby compromising an ongoing investigation. The only sanction provided under current law is the closure of the correspondent account, which, in most cases, will not result in the production of the records, and may in fact impede law enforcement investigations. There is no procedure to seek to compel compliance with subpoenas to foreign banks, nor any explicit authority to impose sanctions for contempt. Finally, the current statute provides that no effort can be taken by the Attorney General or the Secretary of Treasury to close the correspondent account or a foreign bank when the foreign bank has brought proceedings to challenge enforcement of the subpoena.

C. Practical Problems in Prosecutions of Money Laundering Cases

Several specific areas of the current legal framework have in practice served as loopholes or obstacles in the investigation and prosecution of money laundering cases.

For instance, current law in at least two Federal circuits may prevent the Government from pursuing money laundering charges under Section 1957 in cases in which some or all of the illegal proceeds were moved through accounts that mask the source of funds by commingling illegal proceeds with the proceeds of legitimate businesses. Supreme Court precedent requiring proof that a defendant knew not only that cash was being transported in secret, but that the cash was being transported in secret specifically to conceal its criminal nature, has created an enforcement gap when it comes to charging certain culpable intermediaries, like couriers or persons who agree to engage in transactions or transportation as directed for cash, with concealment money laundering. Prosecutors are hampered in pursuing entities like check cashers, which do not transmit money, because the money laundering statutes govern unlicensed money transmitting businesses, as opposed to the broader category of unlicensed money services businesses. This may present challenges for bringing cases against emerging technologies that fall within the broader category, but not the narrower one. On these and other points, there remains room for streamlining and updating our money laundering laws to enhance the Department's efforts to combat money laundering.

V. Conclusion

I thank the Committee for holding this hearing today and bringing attention to the threat that money laundering poses to our financial system. In conjunction with our domestic and international law enforcement partners, the Department looks forward to working with Congress in the global fight against money laundering.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN CRAPO FROM SIGAL MANDELKER

Q.1. During our recent hearings, the Committee heard the BSA regulators being criticized for taking a "check-the-box" approach to compliance. How can we encourage regulators and examiners to allow more innovative approaches to BSA/AML compliance that go beyond a "check the box" exercise? How can we encourage regulators and examiners to allow more innovative approaches? What are the obstacles and challenges here?

A.1. Treasury is taking a hard look at both the Bank Secrecy Act (BSA) and the broader AML/CFT regime. We need to continuously upgrade and modernize our system—a statutory and regulatory construct originally adopted in the 1970s—and make sure that we have the right framework in place to take us into the 2030s and beyond. In particular, we must make sure that financial institutions are devoting their resources toward high value activities and are encouraged to innovate with new technologies and approaches. In recent years, for example, financial institutions have become more proactive in their AML/CFT approach, in some cases building sophisticated internal financial intelligence units devoted to identifying strategic and cross-cutting financial threats. Financial institutions have been improving their ability to identify customers and monitor transactions by experimenting with new technologies that rely on artificial intelligence and machine learning.

We encourage these innovations. These initiatives advance the BSA's underlying purpose. We are working closely with our counterparts at the Federal Banking Agencies (FBAs) to discuss ways to further incentivize financial institutions to be innovative in combating financial crime, including through the examination process. We have also been speaking with many in the financial community to understand their perspectives.

Q.2. Moving forward, it is important to hear the voices of all stakeholders in the BSA/AML compliance space. In your testimony, you noted that Treasury uses the Bank Secrecy Act Advisory Group (BSAAG) to communicate with the private sector and provide guidance. Please provide formal recommendations from the BSAAG.

A.2. The Bank Secrecy Act Advisory Group (BSAAG) provides a key forum for Treasury to receive feedback on Bank Secrecy Act requirements from a broad, diverse representation of the financial industry, law enforcement, and regulatory communities. As such, BSAAG generally does not provide consensus formal recommendations, but rather provides a forum for Treasury to understand views from different impacted constituencies in order to balance diverse stakeholder needs. In addition to BSAAG, we regularly engage with financial institutions through a variety of forums, including the FinCEN Exchange, outreach efforts, and other

engagements. We value the importance of proactive dialogue and information sharing with financial institutions. The safeguards employed by the private sector, and the information reported about terrorist financiers, weapons proliferators, human rights abusers and traffickers, and cyber and other criminals, help prevent malign actors from abusing our financial system.

Q.3. The Clearing House report on "A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement" includes an assertion that "the examination and enforcement regimes for the Bank Secrecy Act have incentivized financial institutions to exclude (or "de-risk") accounts from any customer, industry, or country that has relatively higher potential to engage in criminal activity." We need to ensure a fair and proper regulatory framework that balances the policy goals of stopping criminals while not overburdening banks and causing the unintended consequences of unbanking small, main street businesses.

- What is Treasury currently doing to address de-risking?
- Moving forward, how do we ensure our policy approaches do not create incentives to de-risk?

A.3. Protecting the integrity of the U.S. financial system and preventing its use for criminal purposes is of paramount importance. It is our responsibility at Treasury and within the law enforcement community to detect and prevent illicit use of the U.S. financial system. Financial institutions play a critical role in safeguarding the international system from abuse by illicit actors, which at times includes making risk-based decisions about with whom, where, and how they conduct business.

At the same time, we take concerns about de-risking seriously. We value the importance of preserving access to the U.S. financial system to support economic growth, financial inclusion, and financial transparency while continuing to enforce U.S. laws and regulations. Financial inclusion and financial transparency are complementary and mutually reinforcing objectives. Keeping legitimate transactions in the regulated financial systems improves financial transparency. Treasury has worked with the Federal regulators to issue guidance and clarify the importance to financial institutions of implementing risk-based approaches that assist in preventing overcorrections that might exclude legitimate banking customers.

In the last few years, Treasury has led the U.S. Government's efforts related to de-risking. These efforts have included Treasury-led engagements and dialogues with stakeholders from the public sector and industry, in addition to Treasury's ongoing open line of communication with U.S. financial institutions. Further, Treasury's work on this issue involves close coordination with global bodies and multilateral organizations, including the Financial Action Task Force, the Financial Stability Board, the World Bank, and the IMF.

Treasury recognizes that financial institutions' decisions on whether and how to maintain customer relationships are driven by multiple factors, including: profitability and business strategy motives; current global economic conditions; and real concerns about suspicions of illicit financial activity, including money laundering and the financing of terrorism.

An important way to ensure financial inclusion while increasing transparency is by making sure financial institutions are devoting the resources they have to high value activities. As discussed in my testimony, financial institutions have been improving their ability to identify customers and monitor transactions by experimenting with new technologies that rely on artificial intelligence and machine learning. We laud and encourage these innovations, which advance the underlying purposes of the BSA. We are working closely with our counterparts at the Federal Banking Agencies to discuss ways to further incentivize financial institutions to be innovative in combating financial crime.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM SIGAL MANDELKER

Q.1. Can you describe from your previous experience in the Department of Justice and your current position with Treasury the role that BSA-generated financial intelligence plays in counterterrorism and other law enforcement investigations—in developing investigative leads, sharpening focus on certain criminal players and their banks, or otherwise?

A.1. I know from my prior experience at the Justice Department and in my current role that financial intelligence is a vital source for law enforcement, counterterrorism, and other national security investigations, as we work to follow the money used by illicit actors. This includes our investigations related to North Korea, terrorist financing, drug trafficking, fraud, tax evasion, cybercrime, corruption, sanctions evasion, among other areas. We work closely with Federal, State and local law enforcement across the country to provide access to FinCEN's data to support their investigative efforts including those who are part of SAR Review Teams and financial crime task forces. This includes SAR Review Teams covering the 94 Federal judicial districts, as well as 55 task forces led by IRS–CI. In the last 5 years, regulatory and law enforcement partners, and FinCEN's Intelligence Division made over 10 million queries of the FinCEN database.

Two recent examples that highlight the importance of BSA data include weapons proliferation and cyber threat investigations. On the former, law enforcement used a high volume of financial intelligence from 7 different financial institutions with a transaction value totaling over $17.7 billion in a multi-year investigation into a criminal organization moving hundreds of millions of U.S. dollars to support foreign nuclear and ballistic missile programs. Foreign authorities took action against several of the targets, while the United States is prosecuting others.

Similarly, a multi-year, multi-agency investigation, led by IRS–CI, focused on several targets selling narcotics on the dark web and distributing them throughout the United States through the U.S. Postal Service. BSA reporting by six different financial institutions included over 2.5 million in transactions and provided details of the financial and personal information of the subjects of the investigation and the use of Bitcoins to conceal the illicit proceeds. The targets were arrested, indicted, and pled guilty to various drug and money laundering charges. This was the first case in this

particular Midwest district where money laundering charges were approved based on Bitcoin transactions.

Q.2. What financial intelligence tools are currently most useful to prosecutors, sanctions overseers and others who combat money laundering, and where do we need to strengthen Treasury's and DOJ's tool kit?

A.2. Treasury has broad access to financial intelligence tools and related data as well as information systems and facilities to conduct its mission. Our Office of Intelligence and Analysis, one of the 16 U.S. Intelligence Community agencies, provides expert analysis of financial networks and illicit actors, identifying key nodes that enable us to take disruptive action and build impactful strategies. Likewise, FinCEN continually collects and analyzes BSA and other financial intelligence, including information provided by Geographic Targeting Orders, Foreign Financial Agency rules, and the BSA, and works closely to support law enforcement. Treasury uses this information to inform our strategies, effectively deploy our tools, ensure our actions are calibrated for maximum impact, and measure our effectiveness and inform follow-on strategies and actions. For example, the Office of Foreign Assets Control (OFAC) uses this information to inform our sanctions targeting, and to track, trace, and disrupt illicit financial flows. Likewise, FinCEN uses this information in actions it takes pursuant to section 311 of the USA PATRIOT Act.

I defer to my colleagues at the Department of Justice as to their views on what tools or resources are most useful and needed to strengthen their toolkit.

Q.3.a. Current law allows bank information-sharing only in cases of terrorism or money laundering. Some have advocated for expanding banks' ability to share information, and to broaden the current liability safe harbor to cover a range of other suspected violations of law. Others—including witnesses who have come before the Committee—have sounded an alarm about the need to strengthen privacy safeguards around bank-to-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.

With this in mind, what additional steps do you think 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?

A.3.a. Effective information-sharing between financial institutions is a critical element of our fight against illicit financing. Money launderers are sophisticated. They move across borders and financial institutions, and financial institutions are better able to keep pace and effectively combat them when they communicate with each other.

Some institutions have started forming consortia to share information more dynamically under Section 314(b) of the USA PATRIOT Act, which provides safe harbor for financial institutions to voluntarily share information related to money laundering or terrorist activities. We are supportive of the private sector's

willingness to engage in this type of exchange. By working together, these groups of financial institutions are directly assisting our efforts to identify and disrupt streams of financing for North Korea and other top illicit finance threats.

We also recognize the critical issues of data protection and privacy. We believe existing controls on SAR confidentiality and information-sharing sufficiently protect the privacy interests of consumers and would not be significantly degraded if information-sharing was expanded. Greater information-sharing among financial institutions is expected to improve financial institutions' risk management processes overall. Better risk management is an important element in combating the de-risking phenomenon.

Q.3.b. In particular, should we consider implementing a system of redress or information correction for such individuals, and if so how would you envision that process working?

A.3.b. Creating systems for individuals to access and correct information connected with a financial institution's compliance with its SAR obligations could undermine the purpose of SAR confidentiality and Congress's explicit prohibition of notifying "any person involved in the transaction that the transaction has been reported." (31 U.S.C. 5318(g)(2)). SAR confidentiality is a foundational element of the BSA framework. Without SAR confidentiality, financial institutions may be less open in what they report, omitting information critical to national security or public safety. Further, a SAR is just one part of a broader investigation and law enforcement does not rely exclusively on a SAR when building a case.

Q.4.a. As financial institutions have sought to comply with Know Your Customer (KYC) rules and other important protections against terrorist financing, in recent years many 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 and elsewhere. Whether we are talking about family remittances, or funds transfers for humanitarian purposes, this de-risking has presented hurdles to efforts to get resources to some of the most at-risk populations on Earth. I worked for many months with your predecessor Under Secretary Adam Szubin to address these issues.

Can you describe Treasury's current efforts to mitigate this problem, and to provide technical assistance to Somalia's central bank to strengthen their control systems?

A.4.a. Treasury recognizes the importance of remittances to the Somali economy and to the many American citizens whose families depend on the flow of these funds. Estimates indicate that between 25 to 40 percent of Somalia's GDP comes from remittances from abroad, with the single largest source of this money coming from the United States. Despite banking access challenges, we understand that remittances continue to Somalia.

However, we have seen a number of terrorist financing cases from the United States to Somalia involving companies that provide remittances to Somalia, which presents an ongoing and serious terrorist financing risk. In addition, Somalia's weak regulation and supervision of financial institutions and the continuing lack of

security and governance in many regions elevate the risk of money transfer to Somalia. We carry out regular engagement with external stakeholders, including financial institutions, remittance companies, representatives of the Somali-American community, Federal banking agencies, the Somali government, and technology firms to better understand the drivers of the bank risk aversion toward money transmitters serving the Somalia corridor and potential ways to mitigate the risks related to the transfer of funds to Somalia.

Treasury is also engaged in technical assistance and outreach to enhance the regulation and supervision of financial institutions, including money transmitters, in Somalia. The development of a well-regulated and supervised financial system in Somalia will reduce the risks of fund flows to and from Somalia and reduce banks' risk aversions related to fund transfers and Somalia. Treasury's primary effort is a multi-year capacity-building program sponsored by the Department of State and run by Treasury's Office of Technical Assistance (OTA) to support the Central Bank of Somalia (CBS) in strengthening its capacity to supervise the banking sector. To date, OTA has conducted eight training sessions for the CBS on the regulation and supervision of commercial banks and expects to conduct another session this summer. Due to security conditions in Somalia, to date the training seminars have been held at the Kenya School of Monetary Studies in Nairobi, Kenya. Treasury also participates in the World Bank-led Somalia Remittances Stakeholders Advisory Council, a forum for engagement and coordination of work on this issue, which includes the Somali government. Finally, Treasury has provided assistance in other areas on an ad hoc basis. For example, last year we gave the Somali government advice on the drafting of financial provisions of a new counterterrorism law, following similar work on their anti-money laundering laws, to help them create a legal framework for regulating and supervising financial institutions. This program led to the completion of onsite supervisory exams of the largest money transmitters in Somalia in 2018, among other improvements, which we hope will improve the long term outlook for both safeguarding the financial system from abuse and promoting financial inclusion.

Q.4.b. How can U.S. banks better ensure compliance with important protections against terrorism, while still enabling the flow of legitimate family remittances, and the legitimate work of charities and humanitarian organizations abroad?

A.4.b. Remittances, and the money transmitters that many senders use, play an essential role in financial inclusion. However, the unfortunate reality is that money transmitters have been abused in the past by human traffickers, drug traffickers, fraudsters, and even terrorists.

Treasury recognizes and strongly supports the essential role of charities and humanitarian organizations in communities worldwide. Nonetheless, charities and humanitarian organizations delivering critical assistance in conflict zones abroad have been, in some cases, exploited by terrorist organizations and their support networks in the past. As a result, for money transmitters, Treasury has helped develop international standards on AML/CFT that help

to mitigate the risks of funds transfers. We have also worked at the Financial Action Task Force (FATF) to improve the standards relating to supervision of financial institutions, including those that provide money transfer services, and engaged with charities so they can better understand the terrorist financing risk and appropriate, risk-based mitigation measures. More broadly, we have worked both domestically and at the FATF to convey the importance of both safeguarding the financial system from abuse and promoting financial inclusion.

Q.5.a. The Panama Papers and other similar document leaks revealed the widespread systematic use of shell corporations by wealthy bad actors seeking to not only evade lawful tax collection, but also to facilitate all kinds of financial crime.

How would you characterize the urgency of the threat to the U.S. financial system posed by anonymous shell companies, and by the lack of a coherent national framework for identifying beneficial ownership at the point of company formation?

A.5.a. There is no question that vulnerabilities exist in corporate formation without the disclosure of beneficial ownership information. Illicit actors may more easily hide illicit funds and avoid detection through business entities because the true owner is masked. The collection of beneficial ownership information is critical both at the time of account opening and when a company is being incorporated. FinCEN's Customer Due Diligence (CDD) rule, which is set to be implemented by covered financial institutions in May 2018, requires those institutions to identify and verify the identity of the beneficial owners of their legal entity customers. This change will assist financial institutions in managing risks and law enforcement in pursuing criminals who launder illicit proceeds through legal entities. This is an important step forward.

We are committed to further increasing the transparency and accountability in our financial system, and we look forward to working with Congress to support legislation that addresses this issue.

Q.5.b. Can you give us concrete examples you have seen in your work of bad actors using shell companies for money laundering, terror finance and other illicit purposes?

A.5.b. U.S. companies with hidden beneficial owners have been used by arms dealers, narco-traffickers, proliferators of weapons of mass destruction, and facilitators of massive health care and mortgage frauds, among other abuses. Viktor Bout, a Russian arms dealer used at least 12 companies incorporated in the United States to carry out his arms dealing. In February 2017, Tareck El Aissami, the current Venezuelan executive vice president was designated pursuant to the Foreign Narcotics Kingpin Designation Act by the Office of Foreign Assets Control (OFAC) for playing a significant role in international narcotics trafficking, and his frontman, Samark Lopez Bello, was designated for providing financial and material support to El Aissami. Five companies blocked by OFAC in Florida were used to hold real estate and other assets in Lopez Bello's name. These cases illustrate the importance of obtaining and verifying beneficial ownership information both at the time of company formation and account opening, so that we can be even more effective in countering these threats.

Q.5.c. 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, including with respect to beneficial ownership?

Who should we be looking at that we are not currently regulating—real estate firms, escrow agents, company formation lawyers, others?

A.5.c. We are constantly working to maintain our understanding of the money laundering risks that exist in different sectors. One sector we continue to monitor is real estate. Starting in 2006, we have published assessments of the money laundering risks in the real estate sector. In 2012, to address our assessment of money laundering vulnerabilities, FinCEN extended BSA coverage to resident mortgage lenders and originators. Currently, we continue to collect information and assess the risks in this sector. FinCEN has issued Geographic Targeting Orders (GTOs) that focus on all-cash luxury residential real estate purchases by legal entities. The GTOs require U.S. title insurance companies in seven metropolitan areas to identify the natural persons behind the companies used to buy high-end real estate when certain forms of payment are used.

In 2017, following the enactment of the Countering America's Adversaries through Sanctions Act, FinCEN revised the GTOs to capture a broader range of transactions and include transactions involving wire transfers. FinCEN is analyzing the findings from the GTOs to understand the extent of the vulnerability associated with the misuse of legal entities to acquire real estate and whether additional regulation should be considered. Based partially on findings from the GTO, on August 22, 2017, FinCEN issued an advisory to financial institutions and real estate firms and professionals highlighting risks in the real estate industry, including the use of shell companies to reduce transparency in transactions. In March 2018, FinCEN extended the GTO in response to the useful information that we have been receiving under the new authority to include wire transfers, and we continue to define methods to address the vulnerabilities of this sector. Although real estate professionals do not currently have an obligation to report suspicious activity to FinCEN, FinCEN is using FinCEN advisories and industry outreach to encourage real estate professionals to report voluntarily.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR SASSE FROM SIGAL MANDELKER

Q.1.a. In your testimony you referenced the Treasury Department's ongoing evaluation of when anti-money laundering (AML) measures, particularly Suspicious Activity Reports (SARs), are most helpful to law enforcement.

Has the Treasury Department identified information from SARs or other AML measures that are consistently valuable for law enforcement purposes? If so, what?

A.1.a. We know through our own analysis that SARs and other BSA data are a vital source of financial intelligence for law enforcement investigations of North Korea, terrorist financing, drug trafficking, fraud, tax evasion, cybercrime, and sanctions evasions,

among other crimes. I am committed to better understanding the value of individual elements of the SAR data to inform our overall view of changes that may be necessary to modernize the BSA. To that end, Treasury is issuing an RFP to conduct a thorough, data-driven analysis of BSA reporting requirements to inform its decisionmaking processes. We would be pleased to brief the Committee and its Members as that analysis progresses.

Q.1.b. Has the Treasury Department identified information from SARs or other AML measures that are consistently not valuable for law enforcement purposes? If so, what?

A.1.b. See above.

Q.1.c. Does the Treasury Department expect to recommend altering the reporting requirements for SARs or other AML measures? Do you expect that any of the changes will require legislative authorization?

A.1.c. As discussed in my testimony, I am taking a careful look at the current regulatory and statutory construct surrounding the BSA and AML/CFT regime, which was originally adopted in the 1970s. Treasury is prepared to pursue changes, whether regulatory or statutory in nature, upon completion of our analysis. However, it is premature to predict any specific changes at this time.

Q.1.d. Will you commit to keeping me informed of any conclusions reached by the Treasury Department regarding the scope of AML measures such as SARs?

A.1.d. Yes. Treasury would be happy to brief the Committee and its Members as our analysis progresses.

Q.2.a. I'd like to understand better the law enforcement context for the United State's efforts to fight money laundering.

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

A.2.a. Human traffickers, like other criminals, move their illicit proceeds using a number of methods and vectors: through cash movements, through trade, and through the U.S. and global financial system. Human traffickers are often particularly difficult to stop because their fund transfers tend to be very low-value and their networks are often small and/or decentralized.

Treasury is engaged in both domestic and international efforts, to combat human traffickers and their illicit flows. FinCEN published an advisory on human trafficking to assist financial institutions in identifying the movement of human traffickers' funds and supports law enforcement investigations that use financial intelligence generated as a result of this advisory. In 2017, FinCEN launched a human trafficking project with their global counterparts through the Egmont Group of FIUs. The human trafficking project team applies existing, as well as new approaches/processes/tools for enhanced bilateral information sharing to produce actionable information and disrupt the financial movement related to human trafficking across borders.

We continue to use our intelligence capabilities to identify and track the activities of human traffickers. This includes information from the intelligence community as well as data made available through the Bank Secrecy Act and the USA PATRIOT Act.

In addition, OFAC works to designate human traffickers and other transnational criminal organizations pursuant to Executive Order 13581 (Blocking Property of Transnational Criminal Organizations). For example, on April 18, OFAC designated Syrian national Nasif Barakat and the Barakat Transnational Criminal Organization (TCO) pursuant to Executive Order 13581. The Barakat TCO is a human smuggling organization based in Homs, Syria, that facilitates the smuggling of Syrian and Lebanese nationals to the United States border using a variety of travel routes. Since 2013, the Barakat TCO has facilitated the smuggling of hundreds of individuals to the Southwest border of the United States.

Q.2.b. Last, Treasury's Office of Terrorist Financing and Financial Crimes (TFFC) is leading U.S. involvement in a global typology study of the problem at the Financial Action Task Force. If so, how?

A.2.b. See above.

Q.2.c. What about terrorism, such as organizations like Hezbollah?

A.2.c. The U.S. Government's efforts to counter the financing of terrorism (CFT) are focused on disrupting the monetary and material support terrorist groups need to sustain themselves and to plot and carry out attacks against innocent civilians. This approach focuses on the interrelated objectives of (1) cutting off terrorists and terrorist organizations from their sources of revenue and (2) denying them access to the international financial system so they cannot use their money.

Given Hezbollah's global presence, our efforts to cutoff financing for Hezbollah have focused on imposing costs on its main financier—Iran—as well as taking actions within Lebanon. These actions include constraining Hezbollah financially through extensive cooperation with Lebanese authorities and banks, centering on its procurement agents, facilitators, and financiers in Europe, Latin America, Asia, and the Middle East, including by identifying and sanctioning Hezbollah's Iranian sponsors, and enabling law enforcement and foreign partner actions.

Treasury has demonstrated a relentless commitment to targeting Hezbollah, designating over 120 Hezbollah-linked individuals and entities, including 13 individuals and entities as recently as February 2, 2018, and using Section 311 of the USA PATRIOT Act to identify as entities of primary money laundering concern three Lebanese financial institutions engaged in illicit activity.

Treasury has also targeted Hezbollah's supporters, including Iran, which is the largest state sponsor of terrorism. We have sanctioned over 100 targets in the Middle East, Africa, Asia, and Europe in connection with the Islamic Revolutionary Guard Corps and Iran's support for terrorism, ballistic missile programs, human rights abuses, censorship, cyberattacks, counterfeiting, and transnational criminal activity.

Q.2.d. What about drug cartels and violent gangs such as MS–13?

A.2.d. As noted in the 2015 National Money Laundering Risk Assessment published by Treasury, the size and diversity of our financial sector makes our system attractive to drug cartels and gangs looking for ways to move and store their illicit proceeds.

Treasury oversees a number of efforts to combat TCOs and also actively provides support to law enforcement efforts to identify, target, and dismantle this activity. Using all-source intelligence analysis and in partnership with law enforcement, Treasury maps out the financial networks of cartels and uses its unique authorities to combat those threats. This includes personnel from FinCEN, with access to unique datasets of BSA and PATRIOT Act-derived information, and the Office of Intelligence Analysis.

In addition, OFAC works continuously to target and designate TCOs and their facilitators under its unique authorities, including E.O. 13581 and the Foreign Narcotics Kingpin Designation Act. For instance, on December 22, 2017, OFAC designated the "Thieves-in-Law" TCO, a crime syndicate operating in Russia, Europe, and the Unites States, along with 10 associated individuals and two entities for their involvement in serious transnational criminal activities, including money laundering, extortion, robbery and bribery. Likewise, on April 18, 2018, OFAC designated Syrian national Nasif Barakat and the Barakat TCO pursuant to Executive Order 13581. The Barakat TCO is a human smuggling organization based in Homs, Syria, that facilitates the smuggling of Syrian and Lebanese nationals to the United States border using a variety of travel routes. Since 2013, the Barakat TCO has facilitated the smuggling of hundreds of individuals to the Southwest border of the United States.

In addition to its contribution of intelligence, FinCEN also acts through its role as a regulator to impose and supervise AML/CFT obligations in the United States that help to narrow vulnerabilities that criminals use. FinCEN has published advisories to help financial institutions detect and stop criminal activity and used its authority under the USA PATRIOT Act to take 311 actions against institutions and jurisdictions that criminals use to launder money.

Q.2.e. How can law enforcement officials use anti-money laundering tools to target specific groups such as MS–13 or Hezbollah?

A.2.e. Treasury actively uses its existing authorities and engages with foreign partners to create a hostile operating environment for Hezbollah by denying Hezbollah access to the U.S. and international financial systems, disrupting and exposing its activities around the world, and isolating the group from its support network.

OFAC has designated more than 120 Hezbollah-linked individuals and entities, including 13 individuals and entities as recently as February 2, 2018, pursuant to our counterterrorism authorities and authorities to counter the Assad regime. OFAC uses its sanctions authorities to aggressively target Hezbollah leadership, operatives, and facilitators around the world. We have also aggressively targeted Hezbollah's financiers and commercial investors as well as key procurement networks. These actions are often conducted jointly with law enforcement in order to ensure an effective whole-of-Government approach to countering Hezbollah. Treasury has also targeted Hezbollah's supporters, including Iran, which is the largest state sponsor of terrorism. We have sanctioned over 100 targets in the Middle East, Africa, Asia, and Europe in connection with the Islamic Revolutionary Guard Corps and Iran's support for

terrorism, ballistic missile programs, human rights abuses, censorship, cyberattacks, counterfeiting, and transnational criminal activity.

FinCEN has also used Section 311 of the USA PATRIOT Act to identify Lebanese financial institutions that facilitate money laundering activities as foreign financial institutions of primary money laundering concern. This included the Lebanese Canadian Bank (2011), Rmeiti Exchange (2013), and Halawi Exchange (2013). These actions served to further expose Hezbollah's involvement with and benefiting from illicit activities.

In December, Treasury participated in a workshop on law enforcement approaches to countering Hezbollah. The workshop was hosted by Interpol and more than 25 governments participated in this session, along with Europol. This session built on a similar workshop that Treasury hosted in May, where participants from over 20 governments discussed approaches to combating Hezbollah's financial, commercial, and procurement activities and how financial information and measures can support law enforcement action. FinCEN is also providing direct support to law enforcement officials focused on gang-related activity such as that pertaining to MS–13.

Q.2.f. Are there particular criteria of suspiciousness associated with transactions conducted for the benefit of groups such as MS–13 or Hezbollah?

A.2.f. Treasury uses financial intelligence to map the networks of organizations such as Hezbollah and create typologies for specific underlying activities of individual actors or transaction types. By doing so, we understand that Hezbollah receives the majority of its funding, estimated at $700 hundred million annually, from Iran, as well as millions of dollars from a global network of supporters and businesses, many of which transact through the international financial system. Hezbollah also uses a global network of companies and brokers to procure weapons and equipment and launder funds, many of which Treasury has publicly identified and designated. For example, Hezbollah-affiliated individuals and companies facilitate commercial investments on behalf of Hezbollah.

Types of activities include individual commercial investors and fund managers, organized fundraising from diaspora communities, donations from individual diaspora supporters, and networks to transfer funds and launder money. Procurement activities identified include purchase of weapons and military equipment and purchase of technologies, including electronics for communications, surveillance, and weapons development. These networks have historically operated in the Middle East, West Africa, and South America.

Q.2.g. Can you walk me through a typical case where law enforcement officials used financial intelligence, such as suspicious activity reports, to fight terrorism or transnational criminal organizations such as MS–13?

A.2.g. Financial intelligence is a regular component of all law enforcement investigations. Multiple law enforcement agencies use Bank Secrecy Act reporting, FinCEN analytical reports, and other financial intelligence to initiate and support criminal investiga-

tions. FinCEN regularly publishes examples of how Federal, State, and local law enforcement use the financial intelligence that FinCEN collects. In one example, BSA reports from 26 financial institutions assisted law enforcement in uncovering a criminal network in the United States and Canada with proceeds of $100 million to $300 million annually. Law enforcement liaised with fraud investigators at several banks to investigate suspected money laundering activity being conducted through a series of businesses and trust accounts located in several countries. This investigation, supported by financial intelligence, identified a major money launderer for a transnational organized crime syndicate known as the Black Axe Group. Working closely with foreign and domestic law enforcement partners, authorities arrested and indicted the targets on various money laundering, fraud, and conspiracy charges. Several suspects pled guilty, while others were convicted at trial.

Q.3.a. 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 healthcare 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 identity money laundering and how much more progress can be made in this front?

A.3.a. Technological innovation holds great promise for both financial institutions and Government agencies. We have recently been engaged in extensive outreach with the financial community to better understand trends in this area as well as identify any appropriate changes to the AML regulatory framework to better encourage the use of technological advances.

Q.3.b. Outside of AI and machine learning, how can recent FinTech innovations such as blockchain fight money laundering?

A.3.b. At Treasury, we are exploring ways to work more closely with financial institutions, in particular to foster innovation or leverage financial or regulatory technology (FinTech/RegTech) to fight money laundering. Treasury has been conducting extensive outreach with financial institutions and innovators in the FinTech/RegTech space to solicit their perspectives and suggestions.

The financial services sector continues to drive a range of innovations in FinTech that could help combat money laundering. Blockchain is being applied in fields as diverse as finance, health care, and logistics. FinTech startups have promoted the use of blockchain, and large financial institutions in a variety of partnerships and consortia are actively exploring this technology. These groups continue to test different blockchain implementations that could have varying implications for AML/CFT programs. For example, blockchain could allow financial institutions to more effectively share data and allow better identification of suspicious activity spread across many institutions through a real-time distributed ledger. Such a system could create a much larger dataset spanning participating institutions that would allow AI and machine learning technologies to be even more effective.

Q.3.c. How much does bitcoin, blockchain, and other crypto-currencies facilitate money laundering?

A.3.c. Virtual currency payments present money laundering, terrorist financing, and sanctions evasion risks that must be assessed and mitigated. Absent effective regulation and supervision, virtual currencies are vulnerable to abuse by illicit actors because they may provide for anonymity by users, instantaneous and borderless reach, and irrevocable settlement, and because they may not require the involvement of an institution or intermediary, and lack decentralized records. We remain concerned about its use by illicit actors, such as Venezuela and terrorist organizations. For this reason, we are making it a top priority to encourage global regulation of virtual currency, including through efforts at the G–20 and during our term as President of the FATF beginning in July 2018.

Q.3.d. How can law enforcement officials best stop this newer form of money laundering?

A.3.d. Treasury closely tracks digital currency financial services-particularly virtual currency payments products and services and related technology innovations, and aggressively targets bad actors who exploit them for illicit purposes. We also work in close partnership with law enforcement officials, including collaboration with law enforcement officials on dozens of cases at all levels, and we have seen that traditional investigative techniques combined with expert knowledge and appropriate tools can be highly effective in detecting and prosecuting this type of money laundering.

Critical to Treasury's efforts are the regulatory framework and enforcement authorities we have in place to govern the use of digital currencies or other emerging payments systems. Through FinCEN, Treasury regulates convertible virtual currency exchangers as money transmitters and requires them to abide by a range of Bank Secrecy Act obligations. Virtual currency businesses are subject to comprehensive, routine AML/CFT examinations, just like U.S. financial institutions. Treasury also leverages its enforcement authorities to target illicit actors who do not meet their AML/CFT responsibilities. Further, OFAC uses sanctions in the fight against rogue regimes and criminal and other malicious actors abusing digital currencies and emerging payments systems as a complement to exiting tools, including diplomatic outreach and law enforcement authorities.

The development of digital fiat currencies by rogue regimes such as Venezuela further present money laundering, terrorist financing, sanctions evasion, and other illicit finance risks that must be assessed and mitigated. We are focused on providing industry as well as law enforcement partners detail and clarity to help them in their respective compliance and law enforcement efforts. To that end, we regularly issue FAQs, advisories, and guidance on key sanctions and AML developments, including related to virtual currency. Recently, we issued additional guidance on virtual currency and on prohibited sectoral transactions in our Venezuela program. Additionally, the President issued an Executive order that prohibits, as of the effective date of the order, all transactions related to, provision of financing for, and other dealings in, by a U.S. person or within the United States, any digital currency, digital coin,

or digital token, including the Venezuelan Petro on or after January 9, 2018.

We also convey our expectations through enforcement actions. Each of our actions, whether by FinCEN, OFAC, or other departments, provides an opportunity for industry to gain insight into our compliance and enforcement priorities and often demonstrate our close cooperation with interagency and law enforcement partners. In the last year, for example, Treasury has pursued actions against a number of non-U.S. companies and individuals for violating U.S. laws related to economic sanctions and money laundering, many of which occurred in conjunction with our DOJ and law enforcement partners. FinCEN assessed a $110 million fine against BTC-e, an internet-based virtual currency exchanger located outside the United States, which did substantial business in our country.

We are also making it a top priority to encourage global regulation of virtual currency, including through efforts at the G–20 and during our term as President of the FATF.

Q.4.a. I'd like to discuss Today, around 2 million Suspicious Activity Reports (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.4.a. FinCEN automatically searches the filings it receives, targeting specific risks and challenges to support law enforcement, as well as analyze them for patterns and trends. FinCEN has created business rules and various automated tools that search every filing and assist analysts and law enforcement in identifying those records that are related to or may be associated with open cases or support pattern or trend analysis to identify subjects or areas of interest. The greatest value in SAR data is often not found in a single SAR, but in the aggregation of this critical information that can demonstrate connections, patterns, and trends. That said, there are more than 10,000 FinCEN Query users who conduct more than 30,000 searches each day whose investigations and analysis are augmented by these technological tools.

Financial intelligence, including SARs, serves as a vital resource for law enforcement investigations of North Korea, terrorist financing, drug trafficking, fraud, tax evasion, cybercrime, and sanctions evasion among other things. Federal, State, and local agencies have access to FinCEN's database, this includes SAR Review Teams covering the 94 Federal judicial districts, as well as 55 task forces led by IRS–CI.

As an example of how law enforcement uses data, over 24 percent of IRS–CI's investigations are initiated from (not just supported by) a BSA source.

Q.4.b. How often do financial institutions receive feedback from law enforcement officials as to the utility of their SAR filing?

A.4.b. Law enforcement is better suited to respond to a specific question about feedback they are providing to financial institutions. However, the Treasury Department actively encourages greater law enforcement feedback to financial institutions through initiatives such as FinCEN's Law Enforcement Awards program to recognize successful investigations and provide greater feedback on these success stories to the financial industry. We have also recently launched FinCEN Exchange, an initiative led by FinCEN that brings law enforcement together with financial institutions to facilitate greater information sharing between the public and private sharing. As I discussed in my testimony, FinCEN Exchange convenes regular briefings to exchange targeted information on priority illicit finance threats and uses our authorities under Section 314(a) of the USA PATRIOT Act to provide financial institutions with broader typologies to help them identify illicit activity.

Q.4.c. Some have proposed reducing the number of SARs and CTR 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 we resolve this conflict?

A.4.c. We know through our own analysis that SARs and other BSA data are a vital source of financial intelligence for law enforcement investigations of North Korea, terrorist financing, drug trafficking, fraud, tax evasion, cybercrime, and sanctions evasions, among other crimes. We also need to ensure that financial institutions are devoting their resources toward high value activities. I am committed to better understanding the value of individual elements of the SAR data to inform our overall view of changes that may be necessary to modernize the BSA. To that end, Treasury is issuing an RFP to conduct a thorough, data-driven analysis of BSA reporting requirements to inform its decisionmaking processes. We would be pleased to brief the Committee and its Members as that analysis progresses.

Q.4.d. 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.4.d. I believe that public-private information sharing is critical to enhancing our ability to safeguard the financial system and combat illicit financing activity. For that reason, we recently launched FinCEN Exchange. FinCEN Exchange is a public-private information sharing program in which FinCEN, in consultation with law enforcement as appropriate, provides information to financial institutions to efficiently focus their resources on priority areas. This information sharing provides financial institutions with better insight into the Government priorities and, in some cases, how the Government utilizes information received from financial

institutions. Another key element is to foster responsible innovation to better harness technological innovation.

Q.4.e. 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.4.e. We are happy to consider the matter and review it in consultation with our law enforcement partners.

Q.5. Often, financial institutions will de-risk 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.

Q.5.a. Are there instances in which de-risking is actually unhelpful for law enforcement purposes, because it drives these criminals underground and makes it more difficult to track them?

Q.5.b. At the moment, do the regulators that evaluate and enforce financial institutions compliance with our Federal money laundering take this into account?

Q.5.c. 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 de-risk?

Q.5.d. 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.5.a.–d. Protecting the integrity of the U.S. financial system and preventing its use for criminal purposes is of paramount importance. It is our responsibility at Treasury and within the law enforcement community to detect and prevent illicit use of the U.S. financial system. Financial institutions play a critical role in safeguarding the international system from abuse by illicit actors, which at times includes making risk-based decisions about with whom, where, and how they conduct business.

At the same time, we take concerns about de-risking seriously. We value the importance of preserving access to the U.S. financial system to support economic growth, financial inclusion, and financial transparency while continuing to enforce U.S. laws and regulations. Financial inclusion and financial transparency are complementary and mutually reinforcing objectives. Keeping legitimate transactions in the regulated financial systems improves financial transparency. Treasury has worked with the Federal regulators to issue guidance and clarify the importance to financial institutions of implementing risk-based approaches that assist in preventing overcorrections that might exclude legitimate banking customers.

In the last few years, Treasury has led the U.S. Government's efforts related to de-risking. These efforts have included Treasury-led engagements and dialogues with stakeholders from the public sector and industry, in addition to Treasury's ongoing open line of communication with U.S. financial institutions. Further, Treasury's work on this issue involves close coordination with global bodies

and multilateral organizations, including the Financial Action Task Force, the Financial Stability Board, the World Bank, and the IMF.

Treasury recognizes that financial institutions' decisions on whether and how to maintain customer relationships are driven by multiple factors, including: profitability and business strategy motives; current global economic conditions; and real concerns about suspicions of illicit financial activity, including money laundering and the financing of terrorism.

In terms of resource requirements within the financial institutions, I believe that we can be most effective in combating illicit finance and protecting the integrity of the banking system by making sure that financial institutions are devoting the resources they have to high value activities. As discussed in my testimony, financial institutions have been improving their ability to identify customers and monitor transactions by experimenting with new technologies that rely on artificial intelligence and machine learning. We laud and encourage these innovations, which advance the underlying purposes of the BSA. We are working closely with our counterparts at the Federal Banking Agencies to discuss ways to further incentivize financial institutions to be innovative in combating financial crime.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM SIGAL MANDELKER

Q.1.a. As we contemplate our current anti-money laundering system, it's critical that we also understand the unintended consequences of various policies. In a report issued last April, the World Bank found that for the first time in recent history, remittance flows to developing countries declined for two straight years. Last July, the Financial Stability Board issued a report which found that the number of correspondent-banking relationships fell in all regions between 2011 and 2016. Hardworking men and women throughout the United States, including many in my home State of New Jersey, use remittances to send critical economic support to their families abroad. In the United States and elsewhere, however, we've seen reports that certain banks are terminating the accounts of nonbank payment providers that offer these critical financial services to consumers. In many cases, we've seen banks end outright their relationships with firms, market segments, or countries that are viewed as higher risk, instead of analyzing risks on a case-by-case basis. The net impact of this behavior across multiple countries could have staggering effects on financial inclusion.

What are your views on the causes of this de-risking trend?

A.1.a. Protecting the integrity of the U.S. financial system and preventing its use for criminal purposes is of paramount importance. It is our responsibility at Treasury and within the law enforcement community to detect and prevent illicit use of the U.S. financial system. Financial institutions play a critical role in safeguarding the international system from abuse by illicit actors, which at times includes making risk-based decisions about with whom, where, and how they conduct business.

At the same time, we take concerns about de-risking seriously. We value the importance of preserving access to the U.S. financial

system to support economic growth, financial inclusion, and financial transparency while continuing to enforce U.S. laws and regulations. Financial inclusion and financial transparency are complementary and mutually reinforcing objectives. Keeping legitimate transactions in the regulated financial systems improves financial transparency. Treasury has worked with the Federal regulators to issue guidance and clarify the importance to financial institutions of implementing risk-based approaches that assist in preventing overcorrections that might exclude legitimate banking customers.

In the last few years, Treasury has led the U.S. Government's efforts related to de-risking. These efforts have included Treasury-led engagements and dialogues with stakeholders from the public sector and industry, in addition to Treasury's ongoing open line of communication with U.S. financial institutions. Further, Treasury's work on this issue involves close coordination with global bodies and multilateral organizations, including the Financial Action Task Force, the Financial Stability Board, the World Bank, and the IMF.

Treasury recognizes that financial institutions' decisions on whether and how to maintain customer relationships are driven by multiple factors, including: profitability and business strategy motives; current global economic conditions; and real concerns about suspicions of illicit financial activity, including money laundering and the financing of terrorism.

An important way to ensure financial inclusion while increasing transparency is by making sure financial institutions are devoting the resources they have to high value activities. As discussed in my testimony, financial institutions have been improving their ability to identify customers and monitor transactions by experimenting with new technologies that rely on artificial intelligence and machine learning. We laud and encourage these innovations, which advance the underlying purposes of the BSA. We are working closely with our counterparts at the Federal Banking Agencies to discuss ways to further incentivize financial institutions to be innovative in combating financial crime.

Q.1.b. What can FinCEN and the banking regulators do to encourage banks to conduct case-by-case analysis as opposed to wholesale termination of relationships with various market segments?

A.1.b. Treasury has been heavily engaged on the issue of de-risking over the last few years, including by focusing on encouraging that banks make decisions that effectively assess and manage risk on an individual, rather than indiscriminate basis. This is one of the reasons why we encourage financial institutions to share appropriate information under the Section 314(b) program, thereby allowing financial institutions to make better-informed risk decisions on individual customers.

To help improve the overall supervisory environment, we have taken an active role in supporting efforts to improve multi-State and State-Federal supervisory coordination, notably through State coordination vehicles like the multi-State Money Service Business examination Task Force and the Conference of State Banking Supervisors online system for streamlined data reporting. We have also worked to promote State-Federal coordination vehicles like the Federal Financial Institutions Examination Council and the 2014

Money Remittances Improvement Act. De-risking related work is also a major focus area at the Bank Secrecy Act Advisory Group.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR PERDUE FROM SIGAL MANDELKER

Q.1.a. Secretary Mandelker, Treasury is tasked with overseeing the BSA regime and it has subsequently delegated aspects of that authority—notably BSA exam authority—to various regulatory agencies.

How is Treasury ensuring that regulators' evaluations of financial institution AML programs are consistent with Treasury's view of what makes our country more secure?

A.1.a. Treasury is working with its counterparts in the Federal Financial Institutions Examination Council (FFIEC) to ensure Treasury's principles for an effective AML framework are integrated into their exam practices. I meet with the heads of the regulatory agencies to ensure that we are working closely together to make the exam process as effective and impactful as possible, and incorporates key law enforcement and national security priorities. Treasury also participates in regular calls with FFIEC counterparts, coordinates and cooperates on enforcement actions, and provides training and guidance to examiners through a variety of mechanisms, including through updates to the FFIEC AML exam manual. We also engage in a similar fashion with the SEC and CFTC and frequently engage with groups of State regulators.

Q.1.b. More generally, how do you oversee these industries?

A.1.b. While Treasury has delegated aspects of its exam authority to other Federal functional regulatory agencies, we retain the ability to examine financial institutions as needed. We partner with the IRS on examinations of financial institutions that are not under the jurisdiction of the Federal banking agencies, the SEC or the CFTC and often lead the examinations of virtual currency exchangers. We receive statistical information and reports of examination related to significant BSA deficiencies as well as referrals from examiners when significant BSA compliance issues are identified in examinations.

As part of a robust enforcement program, we also independently investigate and take enforcement action against financial institutions subject to the BSA. In addition to holding individuals and companies accountable, enforcement actions ensure that companies and financial institutions of all types and sizes understand their obligations and take them seriously. They serve as cautionary tales to inform the broader community about the risks of engaging in prohibited activity.

Q.1.c. As of today, what 2017 or 2018 AML/CFT exam priorities has the Treasury Department communicated to regulators?

A.1.c. I have been meeting with the heads of the regulatory agencies to discuss our priorities and work with them to be sure that the examination process reflects those priorities. FinCEN also meets monthly with the delegated supervisors to discuss areas of concern and examination focus related to BSA/AML. These meetings are excellent opportunities for FinCEN, as an expert on the

money laundering risks facing financial institutions, to engage and discuss priority areas with the delegated examiners that have expertise in the operations and risks specific to their covered entities. Also, FinCEN will communicate money laundering risks for a specific institution or geographic area to the appropriate regulator to incorporate in an institution's upcoming examination. The specific recommendations Treasury makes to its examiners are highly sensitive and not appropriate to discuss publicly.

Q.1.d. Could you please reference any memoranda or other evidence of that communication?

A.1.d. The referrals that Treasury makes to its delegated examiners often contain information that is law enforcement sensitive or considered confidential supervisory information. Treasury takes very seriously protecting information that is law enforcement sensitive to prevent any impact on ongoing investigations that often involve matters of national security. Additionally, Treasury and other regulatory agencies rely on the protection and nonpublication of confidential supervisory information as that ensures a high-level of candor between the financial institutions and Treasury. Institutions would less readily share information if there were concerns that it could be made public.

Q.2. Secretary Mandelker, in your testimony you noted that Treasury uses the Bank Secrecy Act Advisory Group (BSAAG) to communicate with the private sector and provide guidance.

Q.2.a. Could you describe the membership of the group? Who sits on the board and how is it selected?

A.2.a. The BSAAG is a statutorily mandated advisory group that consists of representatives from Federal and State regulatory and law enforcement agencies, financial institutions, and trade groups with members' subject to the requirements of the Bank Secrecy Act. Once per year, FinCEN solicits nominations from the public for BSAAG membership in the Federal Register. In making selections for membership, FinCEN will seek to complement current BSAAG members in terms of affiliation, industry, and geographic representation.

Q.2.b. Were there actionable results this group has produced?

A.2.b. In the last few years, BSAAG member suggestions have contributed to several actions taken by FinCEN, including:

- Information Sharing between the Government and Financial Institutions: BSAAG discussions on the importance of two-way, iterative information informed FinCEN pilot information sharing sessions over the past few years that evolved into the recently announced FinCEN Exchange program.
- Information Sharing Between Financial Institutions: BSAAG feedback informed FinCEN actions to streamline the 314(b) information sharing process by creating a more user-friendly registration process and one-click renewal, and informed FinCEN's guidance on information sharing related to money laundering predicate offenses.
- FinCEN Advisories: BSAAG feedback informed improvements to FinCEN advisories to better communicate actionable

information and regulatory expectations. BSAAG feedback was particularly instrumental in FinCEN's development of an advisory on establishing a Culture of Compliance that highlighted general principles illustrating how financial institutions and their leadership may improve and strengthen compliance with the BSA.

Q.3.a. Secretary Mandelker, as a follow-up to the previous question, the BSAAG has a statutory mandate to provide the Treasury Secretary with "advice on the manner in which" BSA and certain Internal Revenue Code reporting requirements "should be modified to enhance the ability of law enforcement agencies to use the information provided for law enforcement purposes."

In the last few years, what formal recommendations has this group made on modifications to BSA reporting requirements to enhance its utility to law enforcement?

A.3.a. Given its broad, diverse representation of the financial industry, law enforcement, and regulatory communities, BSAAG generally does not provide consensus formal recommendations, but rather provides a forum for Treasury to understand views from different impacted constituencies in order to balance diverse stakeholder needs. As noted in my testimony, current topics under discussion within the BSAAG include identifying metrics for determining effective financial reporting, streamlining the reporting of money laundering "structuring" transactions, and more efficient ways for industry to report cash transactions.

Q.3.b. Did Treasury either fully or partially adopted any of the recommendations?

A.3.b. Although the BSAAG does not produce formal recommendations, ongoing discussions within BSAAG are directly contributing to Treasury's perspectives regarding potential modifications in reporting requirements, including potential opportunities to streamline the reporting of money laundering "structuring" transactions, and more efficient ways for industry to report cash transactions.

Q.4. Secretary Mandelker, in the previous hearing on BSA/AML, there was agreement amongst industry experts that regulators have imposed "check-the-box" AML/CFT compliance requirements on banks. I understand that some of this is driven by the Federal Financial Institutions Examination Council's (FFIEC) BSA/AML Examination Manual.

Q.4.a. Historically, how involved has Treasury been in writing the exam manual given it is published by the FFIEC?

A.4.a. Treasury had considerable input into the scoping and review of the first iterations of the manual and has since been working collaboratively with the banking agencies with respect to further updates. I have emphasized the importance of this effort during my meetings with the regulatory agencies and am ensuring Treasury's in-depth involvement in further development of the manual.

Q.4.b. Is the exam manual consistent with Treasury's AML/CFT priorities?

A.4.b. Treasury is working with its counterparts in the FFIEC to ensure that Treasury's principles for an effective AML framework are integrated into the updated manual.

Q.4.c. According to press reports, the manual is currently being updated as it was last published in 2014. Will the public be given the opportunity to comment on it?

A.4.c. The manual is published by the FFIEC. Treasury defers to the FFIEC member agencies on the decision to open the manual to public comment.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM SIGAL MANDELKER

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 de-activate and the relative benefits and drawbacks of each.

A.1. We defer this question to our colleagues in the CFPB or Federal Trade Commission.

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. We defer this question to our colleagues in the CFPB or Federal Trade Commission.

Q.3.a. 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.a. Financial institutions have been quite proactive over the last few years in their AML/CFT approach, in some cases building sophisticated internal financial intelligence units and experimenting with new technologies that rely on artificial intelligence and machine learning to identify strategic and cross-cutting financial threats. The Treasury Department lauds and supports these innovations and is exploring how innovative technology could potentially be used to improve the effectiveness and efficiency of the AML/CFT regime. We are engaging the private sector to better understand the potential of new and emerging technologies to support both private sector compliance and smarter, more effective Government regulation and supervision. These technologies include digital identity solutions, which could potentially facilitate compliance with Bank Secrecy Act requirements for customer identification and verification for onboarding and transaction monitoring and better enable law enforcement to identify, track, and target those who abuse the financial system and to trace and recover illicit proceeds.

Another promising area may be the emergence of innovative regulatory technology solutions that leverage big data, complex algorithms, and artificial intelligence/machine learning to strengthen transaction monitoring and suspicious transaction reporting while reducing compliance costs. We are paying close attention to these and other new technologies in the AML/CFT space, including their

potential use by Government to advance regulatory, supervisory, and law enforcement activities. In this regard, we will continue to engage the private sector to make sure that the regulatory regime keeps up with evolving technology and most effectively supports public and private efforts to achieve our shared objective of protecting the financial system from abuse.

Q.3.b. What are the barriers to either the Government or the private sector adopting these technologies?

A.3.b. We encourage financial institutions to innovate with new technologies and approaches to better target their resources toward high-value activities, while protecting the financial system from abuse. To help us better understand emerging technologies of relevance to our AML/CFT mission and the potential barriers to private sector adoption, Treasury staff is currently engaged in outreach to the private sector. Treasury is also working closely with our counterparts at the Federal Banking Agencies to discuss ways to further incentivize financial institutions to be innovative in combating financial crime.

Q.3.c. What can we be doing as legislators to ensure that we promote technological innovation in this sector?

A.3.c. We encourage Congress to continue outreach to the private sector to stay abreast of technological solutions that can improve efficiency of the financial system, enhance consumer choice, and protect the U.S. financial institutions. We do not have any recommendations at this time related to legislation and technological innovation.

Q.4. One proposal for modernizing the AML compliance regime involves increased information sharing among private sector entities.

Is there a way to increase private sector information sharing while protecting consumer financial information?

A.4. All information sharing by private sector financial institutions for AML purposes is already protected by Federal privacy laws such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Right to Financial Privacy Act (for sharing with the Federal Government), by Federal laws such as the Federal Trade Commission Act that can be used to protect privacy interests, and in many cases by State privacy laws as well. While any expansion of information sharing for AML purposes would have to take into account the requirements of this existing privacy framework, the framework would operate to protect from misuse the information that was in fact shared.

Q.5. The regulatory definition of "financial institution" has been expanded several times over the years, both by the Financial Crimes Enforcement Network rulemaking and by legislation by Congress.

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

A.5. We assess risks and vulnerabilities of the United States and international financial system on an ongoing basis. We are constantly assessing whether specific gaps could be remedied by expanding the definition of the term "financial institution."

Q.6. Could these changes be made via FinCEN rulemaking or should legislation be passed?

A.6. The statutory definition of "financial institution" under the BSA, 31 U.S.C. 5312(a)(2), includes a wide variety of entities touching all the major nodes of the international financial system. In addition, this provision gives the Secretary of the Treasury the authority to designate by regulation as financial institutions for purposes of the BSA any other agency or business that performs activities similar to, related to, or a substitute to any of the activities engaged in by enumerated financial institutions. The Secretary is also authorized to designate as a financial institution any other business whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters. This rulemaking authority has been delegated to FinCEN, and as noted above, Treasury continuously assesses whether specific gaps can be remedied by expanding the definition of financial institution.

Q.7. 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.7. Although real estate professionals do not currently have an obligation to report suspicious activity to FinCEN, we are using FinCEN advisories and industry outreach to encourage real estate professionals to report voluntarily. The advisory issued in August 2017, was not directed exclusively at real estate brokers but any person "involved in real estate closings and settlements," a group identified by Congress as "financial institutions" for purposes of the BSA. (31 U.S.C. 5312(a)(2)(U)). In that advisory, FinCEN outlined specific vulnerabilities and typologies applicable to real estate transactions. An example of industry outreach includes Treasury participation in a conference hosted by the National Association of Realtors in November 2017. Treasury served on a panel to educate real estate agents about the money laundering risks and vulnerabilities in their sector and to encourage industry to report suspicious activity voluntarily to FinCEN under a safe harbor provision. Treasury will continue to engage in this type of outreach.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM SIGAL MANDELKER

Q.1. Gaming and tourism are some of Nevada's top sectors. In my State, 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 my State have suggested that gaming operators would welcome a review of BSA requirements. 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 depository and nondepository regulated entities. I

wanted to follow up on my question in the Committee about the pros and cons of eliminating the requirement that a detailed factual narrative is required when filing a Suspicious Activity Report (SAR) form for structuring situations. In your responses, you mentioned that useful information is found in the detailed factual narrative more generally which I understand but wonder how useful this information is for structuring situations.

What are the pros and cons of eliminating the factual narrative for just structuring situations?

A.1. Eliminating the SAR narrative for certain structuring cases could significantly hamper important investigations. For example, if a financial institution files transactional information but does not include other related suspicious activity that may exist in the narrative, there is a risk that such additional and important information would not be available to law enforcement during the course of an investigation.

There are some significant investigations (in both financial institutions and law enforcement) that were triggered by simple structuring activity, where subsequent investigations that drew on the SAR narrative led to the discovery of more serious crimes. Eliminating the SAR narrative would hamper such investigations. Further, even if the narrative is not highly detailed, it could still help identify a network of individuals where law enforcement may have been previously unaware.

We also recognize that financial institutions expend tremendous amounts of resources each year on investigations and SARs for possible structuring transactions and that eliminating the narrative requirement would reduce these costs. Financial institutions would also have greater flexibility to utilize existing resources on more risk-relevant investigations that may be of higher interest to law enforcement.

We continue to look at this issue carefully and look forward to working with Congress on this topic.

Q.2. I wanted to follow up on my question about raising the Currency Transaction and Suspicious Activity Reporting thresholds. In the hearing, you mentioned concerns that small dollar amounts can be used for criminal activities so there are risks to raising the thresholds. Some recommend raising them to either inflation or a lesser amount—from $5,000/$10,000 for suspicious activity reports and $20,000 or $25,000 for currency transaction reports.

Please expand on what we should consider if the threshold amounts for CTRs and SARs were increased.

A.2. As part of a broader risk-based review of the efficacy and value of the current AML/CFT regime, we are evaluating the suspicious activity report (SAR) and currency transaction report (CTR) requirements, including reporting thresholds. In conducting this review, we are defining and measuring the value both quantitatively and qualitatively of the data derived through BSA reporting requirements.

We have identified some initial concerns, especially from our law enforcement partners, that significant increases in the respective thresholds could reduce the amount of valuable financial intelligence available to Treasury, law enforcement, and other key

domestic and international partners. For example, FinCEN recently reviewed CTR filings to assess how much of that financial intelligence we might lose if the threshold were doubled to approximately $20,000. In that circumstance, FinCEN would lose over 60 percent of CTR-based financial intelligence on which FinCEN and law enforcement, in particular, currently rely to support investigations and analysis. The more the threshold is increased, the more data would be potentially lost. For example, increasing the threshold to $30,000 would result in a loss of close to 80 percent of currently provided data—in this case the type of data points that enable the identification of illicit networks and the initiation or expansion of investigations. In addition, it is important to consider how changing practices can highlight the suspiciousness of a cash transaction, even in low amounts. For example, because customers often rely on wire transfers instead of cash deposits and withdrawals, a cash deposit of $10,000 can be a valuable source of information.

The value of the reporting that could be lost as a result of threshold increases is not simply a reduction in the number of SARs, CTRs, FBARs or other required BSA reporting. This reporting has significant tactical value that supports, among other efforts, existing law enforcement and sanctions investigations or provides new leads and information to start those efforts. This reporting also provides significant strategic value, ranging from studies of trends to identification of typologies associated with new illicit finance schemes, such as crypto-currencies, that are used to develop and implement risk mitigation responses. Financial reporting also supports operations, including through the sharing of information with international partners to support efforts related to terrorist financing, proliferation financing, political corruption, drug or human trafficking, human rights abuses and corruption, and many other important illicit finance and national security issues.

We continue to conduct a broader and deeper data-driven analysis of BSA reporting requirements to inform decisionmaking processes and recommendations. As we review the factors discussed above we may need to focus our attention on the relative value of the SARs and CTRs being filed, instead of merely on thresholds. We will also continue to discuss the threshold issue and BSA value with law enforcement and other relevant stakeholders within the BSAAG and other fora to consider their input.

Q.3. 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.

Do you think institutions are taking advantage of those red flags, in order to better assess whether their banks are being used to finance human trafficking?

A.3. Based on feedback received from our engagement with stakeholders, we do believe that financial institutions have benefited from relying on the red flags identified in the advisory to better assess such activity. In fact, according to FinCEN's internal metrics, the advisory focused on human trafficking red flags is one of its most viewed advisories.

Q.4.a. Secretary Mandelker, I believe the FinCEN Exchange is a great idea.

Following up on my question, will you provide similar occasional briefings for nondepository entities that also comply with BSA/AML?

A.4.a. We created FinCEN Exchange to provide a range of financial institutions with additional information about priority issues on a more regularized and frequent basis. In the past, FinCEN has invited nonbank financial institutions to similar discussions when it believes that the financial institution may have information relevant to an issue specific briefing or other ability to support the law enforcement priorities within the scope of the particular engagement. Such exchanges are important and we will work with our law enforcement partners to provide briefings for nondepository entities.

Q.4.b. Would you commit to hosting briefings at least bi-annually for gaming establishments, money services businesses, currency exchanges and others that are not currently included in FinCEN Exchange events?

A.4.b. We envision robust participation in FinCEN Exchange by a variety of private sector entities. The invitation list of participating private sector entities for a particular briefing will be driven by the specific illicit finance or national security threat topic as prioritized by FinCEN and law enforcement.

Q.5. In 2015, FinCEN signed a Memorandum of Understanding with the State Regulatory Registry/CSBS Board to obtain access to all State MSB licensing data contained in the Nationwide Multi-State Licensing System (NMLS).

What has FinCEN learned from the MOU regarding MSB registration data about the scope and risks within the MSB sector? Has this information been shared with the IRS, State regulators and Congress? Could you share any analysis with my office?

A.5. FinCEN has obtained information on money transmitter agents from the NMLS. FinCEN is using this data to identify higher risk agents that engage in MSB activity beyond their work as an agent and may need to be independently licensed. Under a new feature of NMLS and the ensuing data package, FinCEN will now also obtain information on transaction monetary volumes at the company and State-specific level, as well as volumes and destinations of transactions going to foreign jurisdictions. This will enhance FinCEN's ability to identify MSBs that need enhanced supervision of their money transmitting activities. FinCEN meets with State regulators regularly to discuss upcoming examinations and better ways to more effectively and efficiently manage the MSB sector.

Q.6.a. Since the Money Remittances Improvement Act (MRIA) became law, FinCEN has worked with the IRS and State examination authorities to coordinate exam scheduling.

How many States currently register in the NMLS system?

A.6.a. According to the NMLS, there are 40 States managing their MSB licensing through NMLS. Of these States, at least 28

mandate that MSBs use the NMLS system for registration and this number continues to grow.

Q.6.b. What has been the impact of MRIA and the coordination that resulted from the passage of that law?

A.6.b. The MRIA has improved FinCEN's collaboration and coordination with its State partners. As discussed in a prior answer, FinCEN uses information collected by the States through the NMLS system to partially evaluate potential risks in the MSB industry. FinCEN regularly communicates with the States on coordinating examinations and efficiencies in the supervision process. FinCEN has also coordinated directly with the States when crafting agreements between the State regulator and the institution to bring the institution into compliance.

Q.6.c. Which States permit Money Services Businesses to share certain State exam findings with banks or credit unions?

A.6.c. FinCEN is aware of certain States that allow financial institutions to share State examination findings based on specific conditions and consultations. However I would refer you to the Conference of State Bank Supervisors for more information on this issue.

Q.7. I served as Attorney General of Nevada for 8 years. I know that investigations of organized crime, terrorist financing and money laundering rely on collaboration with leaders and governments of other nations.

As the Under Secretary for Terrorism and Financial Crimes, how does your office collaborate with African nations to curb terrorist financing and money laundering?

A.7. Treasury's Office of Terrorist Financing and Financial Crimes heads the U.S. delegation to the Financial Action Task Force Regional Style bodies in Africa. Through both the Eastern and Southern Africa Anti-Money Laundering Group and the Inter-Governmental Action Group Against Money Laundering in West Africa, we collaborate with African nations to strengthen their anti-money laundering and countering the financing of terrorism regimes. Further, through other multilateral fora and the World Bank/IMF biyearly Bank Fund meetings and other bilateral engagements, we also share information critical to stemming illicit financial flows. Finally, when discrete matters arise, we engage with local embassies on a bilateral basis on issues related to terrorist financing and money laundering.

Q.8. Secretary Mandelker, Treasury's Office of Technical Assistance has been a critical resource to collaborate and strengthen other nations. I would like to better understand how the Office of Technical Assistance works.

Q.8.a. Which nations did the Office of Technical Assistance serve in 2016 and 2017? How many nations requested assistance but have been denied?

Q.8.b. Please detail why the assistance was denied: lack of U.S. funding, diplomatic considerations, another nation was better suited to provide the information, *etc.*?

Q.8.c. Please provide annual OTA funding levels from 2010 until today?

A.8.a.–c. Treasury's Office of Technical Assistance (OTA) falls under the Under Secretary for International Affairs. OTA provided the following information in response to your questions about its activities.

Please see OTA's 2016 and 2017 Operating Plans (attached) for a complete list of OTA projects.

In 2016 to 2017, OTA received 20 requests for assistance from jurisdictions that did not result in a new Treasury technical assistance engagement. There are many reasons that a request for assistance would not result in an engagement. Most commonly, OTA requires additional information prior to conducting an in-country needs assessment, such as more detailed information as to the type of assistance requested. If additional information is not received, OTA will not move forward with an in-country needs assessment.

For those engagements that do proceed to an in-country needs assessment, OTA management may determine that there is insufficient commitment to reform and/or the counterparts are not positioned at the time of the assessment to use OTA assistance well. In these circumstances, OTA communicates necessary pre-conditions for OTA assistance to have the best opportunity for success. Pre-conditions vary, but can include the requesting jurisdiction committing additional resources to or hiring of additional staff at the counterpart agency or the need for a demonstration of political will to implement reform through the issuance of a decree or regulations.

In rarer circumstances, OTA management may determine that other nations or international institutions are better positioned to provide the necessary technical assistance.

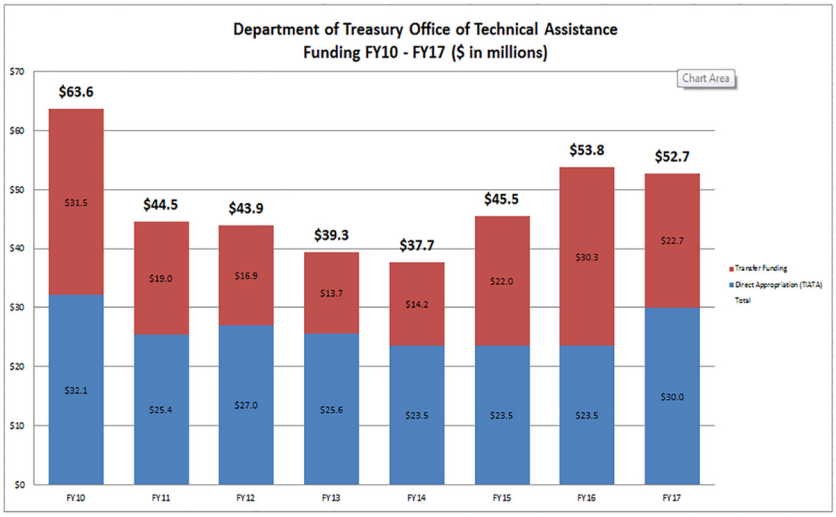
Q.9. For years, Treasury relied on supplemental fund transfers from the State Department, USAID and other Government agencies.

Q.9.a. How much did OTA receive from State and USAID in 2014, 2015, 2016, and 2017?

Q.9.b. How is the OTA working with the International Monetary Fund and the World Bank to prevent terrorist financing and money laundering?

A.9.a.–b. Treasury's Office of Technical Assistance falls under the Under Secretary for International Affairs. OTA provided the following information in response to your questions about its activities.

The chart below provides OTA's annual funding levels by source of funding from 2010 to 2017 (last complete fiscal year).



Notes:

1. FY10 TIATA figure includes $7.1 million supplemental appropriation for assistance to Haiti.
2. FY12 and FY13 TIATA figures include $1.5 million Overseas Contingency Operations (OCO) funding.
3. FY13 TIATA figure reflects 5% sequester.
4. FY15 Transfer Funding includes $6.75 million in multi-year funding for Ukraine from Dept. of State.

The table below provides the funding OTA received from State and USAID from 2014 to 2017.

Transfers from USAID and Dept. of State		
	USAID	STATE
FY14	$ 4,249,325.00	$ 6,672,409.00
FY15	$ 4,953,237.00	$ 12,766,385.37
FY16	$ 5,551,234.00	$ 23,846,336.15
FY17	$ 3,899,176.00	$ 18,784,682.00

OTA regularly coordinates its anti-money laundering/counter financing of terrorism assistance with other assistance donors and providers, including the International Monetary Fund (IMF) and the World Bank. This collaboration occurs both at headquarters in Washington, DC, and in the field with the goal of ensuring that assistance efforts are aligned and to prevent redundancy. OTA communicates with other providers about its current assistance efforts as well as prospects for future assistance. For example, in a country where more than one assistance provider may operate, these efforts prevent unnecessary overlap, identify synergies, and maximize absorptive capacity of recipient counterparts.

For example, as part of OTA's holistic approach to engaging the full range of AML/CFT stakeholders, OTA usually seeks to work

with supervisory as well as enforcement authorities. If the IMF plans to work with the banking sector supervisor to develop supervisory tools, OTA may seek to work in parallel with the supervisor of money remitters or may concentrate its activities on other parts of the framework, such as the financial intelligence and law enforcement authorities. Alternately, if the IMF concludes its supervision assistance with the drafting of a supervision tools such as an examination manual, OTA may provide follow-on assistance on the application and implementation of those tools.

Q.10. Kenya's M–Pesa is an electronic system that captures every transaction. All M–Pesa customers must identify themselves with their original identification document. There is three-factor authentication: SIM card, ID and the PIN. The Central Bank of Kenya receives regular reports on transactions.

What can we learn from Kenya and other nations about how to use mobile banking to provide access to financial services and also avoid terrorist and other forms of illicit financing?

A.10. Kenya's M–Pesa mobile payments system is often cited as an example of how innovative financial products and services can leverage technology and new business models to support financial inclusion. M–Pesa demonstrates the importance of encouraging responsible, regulated innovation in the financial sector that includes robust digital identification built into the FinTech product/service. M–Pesa's use of three-factor authentication, including the use of mobile phone technology (SIM card and other cell phone data), to supplement official Government identity documentation for customer identification and verification, and for transaction authorization, helps combat fraud and protect against abuse by money launderers and terrorists and their financiers.

Q.11. 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 de-risking has become epidemic in some communities, such as communities along the Southwest border, remittances providers serving fragile nations like Somalia and humanitarian groups. In your testimony, you mention Treasury's efforts to ensure humanitarian remittances reach Venezuela as you work to stem financial corruption in that nation.

Please explain what steps the Treasury Department is taking in Venezuela to stabilize humanitarian remittances?

A.11. We share your concern regarding the humanitarian and economic catastrophe in Venezuela. As part of our ongoing efforts to address this issue, Secretary Mnuchin hosted Finance Ministers from the Western Hemisphere, Europe, and Japan on April 19 to discuss the humanitarian situation, which has consequences that extend beyond Venezuela's borders, threatening regional stability and national security. Ministers reviewed population flows out of Venezuela to destination countries around the world, including a sharp acceleration in departures as Venezuelans flee the lack of security and economic opportunity. Ministers took note of the call by the United Nations High Commissioner for Refugees to assist countries in the region that are absorbing the Venezuelan outflow, to

which Vice President Pence announced a significant United States contribution.

Maduro and his regime have led Venezuela to ruin and are solely responsible for the immense human suffering occurring in Venezuela today. The Maduro regime has continued to undermine democracy, impoverish its citizens, and loot the country to line its pockets. Essential goods, such as food and medicine, have become increasingly scarce. During the meeting on Venezuela hosted by the Secretary, participants reviewed how the government's control over food distribution is a mechanism for social control and a vehicle for corruption. Participating countries agreed to strengthen international cooperation to curb Venezuelan corruption that is worsening the humanitarian situation.

Over the last year, Treasury has taken a number of actions to counter the Maduro's regime assault on democracy and its own people. Since 2015, OFAC has designated over 50 current and former Government of Venezuela officials, including Maduro himself, and denied them access to the U.S. financial system. This year, we have announced the designation of eight individuals, including four current or former senior military officers on January 5 and four additional current or former officials on March 19. These designations shine a spotlight on current and former officials who continue to benefit from a corrupt system, even as Venezuela's citizens, economy, and constitutionally enshrined democratic institutions languish.

On August 24, 2017, President Trump issued an Executive order which imposed a carefully calibrated set of prohibitions that deny the regime critical sources of financing, protect the U.S. financial system, and aim to shield Venezuelans from punishingly expensive debts. In addition, on March 19, the President issued an Executive order that prohibits all transactions related to and dealings in, by U.S. persons or within the United States, any digital currency, digital coin, or digital token, including the Venezuelan "Petro" and "Petro-gold." The Petro is a desperate effort by a corrupt government to circumvent existing U.S. sanctions. At face value, the Petro is a scam ripe for exploitation by corrupt regime insiders seeking to defraud investors and ordinary Venezuelans.

To aid financial institutions in identifying transactions that may be linked to Venezuelan corruption, FinCEN issued an advisory in September 2017 informing financial institutions of widespread public corruption in Venezuela and the methods senior Venezuelan political figures—as well as their associates and front persons—may use to move and hide corruption proceeds. Combined with our financial sanctions on debt and equity as well as our targeted designations, this advisory put financial institutions on watch for possible illicit fund flows.

Our sanctions related to Venezuela are narrowly tailored to deny the Maduro regime access to critical sources of financing, but they do not otherwise prohibit financial transactions with Venezuela, including the provision of humanitarian remittances.

To avoid any disruption to the provision of humanitarian goods to the Venezuelan people, OFAC issued a General License that authorizes all debt financing related to exports to Venezuela of agricultural commodities, food, medicine, and medical devices. OFAC

routinely engages with the private sector and others to prevent confusion from hindering lawful activity, including with respect to humanitarian aid and remittances.

Q.12. How will the Treasury Department work with the other banking regulators—OCC, FinCEN, FDIC, and the Federal Reserve—along with the IRS to help banks meet the banking needs of legitimate consumers and businesses that are at risk of losing access—or have already lost access?

- Has Treasury been able to stem the decline in correspondent banking relationships that have limited financial access to many?
- If so, how?
- If not, what policies could restore and expand correspondent banking relationships?

A.12. Protecting the integrity of the U.S. financial system and preventing its use for criminal purposes is of paramount importance. It is our responsibility at Treasury and within the law enforcement community to detect and prevent illicit use of the U.S. financial system. Financial institutions play a critical role in safeguarding the international system from abuse by illicit actors, which at times includes making risk-based decisions about with whom, where, and how they conduct business.

At the same time, we take concerns about de-risking seriously. We value the importance of preserving access to the U.S. financial system to support economic growth, financial inclusion, and financial transparency while continuing to enforce U.S. laws and regulations. Financial inclusion and financial transparency are complementary and mutually reinforcing objectives. Keeping legitimate transactions in the regulated financial systems improves financial transparency. Treasury has worked with the Federal regulators to issue guidance and clarify the importance to financial institutions of implementing risk-based approaches that assist in preventing overcorrections that might exclude legitimate banking customers.

In the last few years, Treasury has led the U.S. Government's efforts related to de-risking. These efforts have included Treasury-led engagements and dialogues with stakeholders from the public sector and industry, in addition to Treasury's ongoing open line of communication with U.S. financial institutions. Further, Treasury's work on this issue involves close coordination with global bodies and multilateral organizations, including the Financial Action Task Force, the Financial Stability Board, the World Bank, and the IMF.

Treasury recognizes that financial institutions' decisions on whether and how to maintain customer relationships are driven by multiple factors, including: profitability and business strategy motives; current global economic conditions; and real concerns about suspicions of illicit financial activity, including money laundering and the financing of terrorism.

An important way to ensure financial inclusion while increasing transparency is by making sure financial institutions are devoting the resources they have to high value activities. As discussed in my testimony, financial institutions have been improving their ability to identify customers and monitor transactions by experimenting with new technologies that rely on artificial intelligence and

machine learning. We laud and encourage these innovations, which advance the underlying purposes of the BSA. We are working closely with our counterparts at the Federal Banking Agencies to discuss ways to further incentivize financial institutions to be innovative in combating financial crime.

Q.13. Last year, the Countering Iran's Destabilizing Activities Act of 2017 (Public Law 115–44) was enacted. In Section 271, it required the Treasury Department to publish a study by May 1, 2018, on two issues: 1. Somali Remittances. The law required 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. 2. 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.

Q.13.a. What is the status of this study?

A.13.a. The Treasury Department submitted this report to Congress in fulfillment of its obligations under CAATSA on Friday, April 27, 2018.

Q.13.b. Are you contacting other organizations in your research?

A.13.b. Treasury contacted other governmental and multilateral bodies that have studied this problem, Federal banking agencies, and private sector financial institutions.

Q.13.c. Which ones—or types of groups—have you met with?

A.13.c. As noted above, these include other governmental and multilateral bodies that have studied this problem, Federal banking agencies, and private sector financial institutions with which we are engaging.

Q.13.d. Will the Treasury Department meet the deadline of May 1, 2018, to publish the report?

A.13.d. Yes. The Treasury Department submitted this report to Congress in fulfillment of its obligations under CAATSA on Friday, April 27, 2018.

Q.13.e. Anonymous incorporation is not difficult for criminals—virtually no States require corporate applications provide the identity of the corporation's ultimate owner. Law enforcement has said it needs to know the owners of firms in order to investigate financial crimes and terrorism.

How should Congress and/or Treasury tailor these proposed requirements so as not to be overly burdensome on either incorporating entities or the States themselves?

A.13.e. There is no question that vulnerabilities exist in corporate formation without the disclosure of beneficial ownership information. Illicit actors may more easily hide illicit funds and avoid detection through business entities because the true owner is masked. The collection of beneficial ownership information is

critical both at the time of account opening and when a company is being incorporated. FinCEN's Customer Due Diligence (CDD) rule, which is set to be implemented by covered financial institutions in May 2018, requires those institutions to identify and verify the identity of the beneficial owners of their legal entity customers. For purposes of the CDD Rule, covered financial institutions are federally regulated banks and federally insured credit unions, mutual funds, brokers or dealers in securities, futures commission merchants, and introducing brokers in commodities, as defined in 31 CFR 1010.605(e)(1). This change will assist financial institutions in managing risks and law enforcement in pursuing criminals who launder illicit proceeds through legal entities. This is an important step forward.

We are committed to further increasing the transparency and accountability in our financial system, and we look forward to working with Congress to support legislation that addresses this issue.

Q.13.f. Should Congress exempt any firm already regulated by Federal banking regulators and companies with over 20 employees?

A.13.f. We are aware of options in proposed legislation to allow for various business types and sizes to be exempt from reporting beneficial ownership information. We are reviewing the various legislative proposals and look forward to working with Congress on the issue of enhancing the transparency of beneficial owners.

Q.13.g. Some argue that those types of companies are very unlikely to open bank accounts to hide or move criminal funds or to hold illegal assets, do you agree?

A.13.g. We are aware of options in proposed legislation to allow for various business types and sizes to be exempt from reporting beneficial ownership information. Many business types and sizes can be used to hide or move illicit assets. We are reviewing the various legislative proposals and look forward to working with Congress on the issue of enhancing the transparency of legal entities by requiring the reporting of beneficial ownership information at the time of company formation.

Q.13.h. Does the Treasury Department need legislation to issue regulations requiring corporations and limited liability companies formed in any State that does not already require ownership disclosure to file information about their beneficial ownership with Treasury as well?

A.13.h. We are not aware of any Federal law that currently authorizes the Treasury Department to impose such a disclosure requirement on companies in general. Legislation granting Treasury the authority to impose such a disclosure requirement would be required.

Q.13.i. What type of disclosure should be required: name, current address, non-expired passport or State-issued driver's license, identification of any affiliated legal entity that will exercise control over the incorporated entity, *etc.*?

A.13.i. Access to unique identifiers of the beneficial owners of legal entities is crucial for law enforcement to investigate money laundering, terrorist financing, and other financial crimes. We look forward to working with Congress and law enforcement to propose

identifiers that should be disclosed about the beneficial owners of legal entities during the incorporation process.

Q.13.j. Should the rules require that beneficial owners be updated no later than 60 days after any change in ownership?

A.13.j. It is important that beneficial ownership information be accurate and up-to-date to assist law enforcement in identifying the true owners of companies whenever that information changes.

Q.13.k. Should the rules provide civil penalties for anyone who submits false or fraudulent beneficial ownership information, does not provide complete or updated information; and/or knowingly discloses subpoena, summons, or other requests for beneficial ownership information without authorization?

A.13.k. Any legislation that requires the disclosure of beneficial ownership information at the time of company formation should have appropriate penalties. We are supportive of civil penalties for anyone who submits false or fraudulent beneficial ownership information; does not provide complete or updated information; and/or knowingly discloses subpoena, summons, or other requests for beneficial ownership information without authorization. We believe the availability of civil penalties provides a significant deterrent to individuals and companies providing false information.

Q.14. Author and reporter David Cay Johnston reports in his book, The Making of Donald Trump, that public records show highly suspicious money from Russia is behind Trump's businesses. He alleges that "over the past three decades, at least 13 people with known or alleged links to Russian mobsters or oligarchs have owned, lived in, and even run criminal activities out of Trump Tower and other Trump properties. Many used his apartments and casinos to launder untold millions in dirty money. Some ran a worldwide high-stakes gambling ring out of Trump Tower—in a unit directly below one owned by Trump. Others provided Trump with lucrative branding deals that required no investment on his part. Taken together, the flow of money from Russia provided Trump with a crucial infusion of financing that helped rescue his empire from ruin, burnish his image, and launch his career in television and politics."

Q.14.a. Please provide a list of convicted criminals who had business dealings with the Trump Corporation?

A.14.a. It would not be appropriate for Treasury to comment on matters of potential investigative interest, or in a way that may confirm or deny the existence of such interest.

Q.14.b. Please list the condominiums and their owners that the Federal Government seized from Russian emigres who were convicted of crimes such as money laundering, violence, *etc.*?

A.14.b. The Department of the Treasury does not maintain this type of information.

Q.14.c. What is the size of Russian mob money laundering in the United States? What do you recommend we do to limit money laundering from international and domestic organized crime syndicates?

A.14.c. Although FinCEN supports law enforcement efforts to investigate Russian Organized Crime money laundering, and has

conducted analysis of BSA filings related to this topic, FinCEN does not have an estimate of the extent of this activity from that data. Treasury continues to support increasing transparency for all kinds of financial vehicles, including shell companies, to limit money laundering from organized crime syndicates. Shoring up this vulnerability, as FinCEN is doing with the soon-to-be-effective Customer Due Diligence rule, will prevent the ease with which these syndicates can profit off of their illicit activity.

Q.15. Like many corporate executives, President Donald Trump takes advantage of more corporate-friendly businesses laws. Analysis of his FEC filings finds he registered 659 businesses. Despite defining himself as a New Yorker, only 19 percent of his businesses are chartered in New York. Only 11 percent of his businesses were chartered in Florida where he has a second home. Instead, more than two-thirds of his corporations were chartered in Delaware (48 percent) or Nevada (23 percent). President-elect Donald Trump filed a Federal Election Committee (FEC) filing in July 2016 listing 515 corporations for which he serves on the Board of Directors. Of these, 263 of the corporations begin with "Trump." A number of the other corporations contain some combination of his initials "DT" or "DJT." 2 Quartz. "A List of Everything Donald Trump Runs That Has His Name On It." Looking only at corporations which included "Trump," which did not include another family member (*i.e.,* his father or his children), and which could be reasonably determined to be one of Donald Trump's companies (*i.e.,* excluding initialed companies and companies containing Trumpe, Trumpf, Trumpy, *etc.*), it seems: 315 companies are incorporated in Delaware. Of which, Trump self-reported as a board member of at least 182. The New York online corporate registry does not provide an immediately obvious status of the companies so we cannot analyze current versus dissolved corporations. One hundred forty-nine companies are incorporated in Nevada. Of which, only 15 are currently active. A few have been formally dissolved; however, the remainder are in a progressively permanent state of revocation for failure to keep up with filings and fees. Of the 15 active corporations, Trump self-reported as a board member of at least 9. One hundred twenty-nine companies are incorporated in New York. Of which, Trump self-reported as a board member of at least 60. The New York online corporate registry does not provide an immediately obvious status of the companies so we cannot analyze current versus dissolved corporations. Seventy companies are incorporated in Florida. Of which, 22 are currently listed as active. Of the active corporations, Trump self-reported as a board member of at least 3. Five companies are incorporated in Wyoming; only 1 is active.

Q.15.a. Can you confirm that these figures about President Trump's business locations are accurate?

A.15.a. Treasury does not generally maintain comprehensive corporate registry information and is not in a position to opine on the information presented in this question.

Q.15.c. Have any of President Trump's current or former businesses been indicted or convicted for money laundering or other financial crimes?

A.15.c. The Department of the Treasury does not maintain this type of information.

RESPONSE TO WRITTEN QUESTION OF CHAIRMAN CRAPO FROM M. KENDALL DAY

Q.1. There has been a lot of discussion around expanding information sharing authorities under Section 314 of the USA PATRIOT Act.

How would you expand 314(b) authorities in a way that is both useful to all financial institutions and able to protect sensitive law enforcement information?

A.1. Information sharing is crucial to law enforcement investigations and prosecutions. Financial institutions are often the first line of defense against money laundering, and the information they collect—on their own and as part of the 314(b) process—can ultimately help law enforcement by providing critical leads in existing investigations and spurring new ones. These leads help law enforcement detect and deter criminal activity and, in some cases, may help law enforcement stop crimes in progress before they cause greater harm.

Under the existing 314(b) authorities, financial institutions may share information with one another for purposes of identifying and reporting activities that may involve terrorist activity or money laundering. Statutory authority allowing information sharing on a broader range of activity would expand and enhance the information reported to law enforcement and give it greater insight into the financial activities of criminals. That, in turn, would strengthen our efforts to detect and deter criminal activity of all kinds.

Existing 314(b) authorities already contain a number of important safeguards designed to protect sensitive law enforcement information, and these safeguards could be extended to any broadening of the activities covered by 314(b). Financial institutions that wish to participate in 314(b) sharing must first file a notice with the Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN). Before sharing information, institutions must also take reasonable steps to verify that other financial institutions have filed a notice under 314(b). In addition, financial institutions must establish and maintain procedures to safeguard the security and confidentiality of the shared information, and they may only use the information for specific purposes. Critically, 314(b) does not authorize participating financial institutions to share a Suspicious Activity Report (SAR) itself or disclose the existence of a SAR.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM M. KENDALL DAY

Q.1. During the hearing, I asked you whether the independent monitor installed as part of HSBC's 2012 deferred prosecution agreement (DPA) with DOJ had certified that HSBC had complied with the letter and spirit of its obligations under DPA. You provided a partial answer, stating only that HSBC generally complied with its obligations under the DPA. You described HSBC's

satisfaction of all of the independent monitor's recommendations as "a different issue." However, the DPA provides that "HSBC Holdings shall adopt all recommendations in the [monitor's] report." (Unless the monitor signs off on an alternative proposed by HSBC, within 30 days, to meet the same purpose or objective). Thus, one of HSBC's obligations under the DPA is to implement the monitor's recommendations. HSBC cannot skirt this obligation without a "determination" by the monitor or DOJ that some "alternative proposal" is appropriate. Accordingly, I have three further questions about HSBC's implementation of the monitor's recommendations:

Q.1.a. Did the monitor certify that HSBC implemented and adhered to all his recommendations and other remedial measures specified in the DPA?

Q.1.b. Did DOJ overrule any of the monitor's recommendations, or make a determination with respect to any of his recommendations that an alternative proposal was appropriate? If so, how many? Please provide the number of overruled recommendations, or determinations that an alternative proposal was appropriate, both as a raw quantity and as a percentage of all the monitor's recommendations.

Q.1.c. For each overruled recommendation, or determination that an alternative proposal was appropriate, please explain (i) the nature and content of the recommendation, or alternative proposal; (ii) why DOJ overruled the recommendation, or determined that an alternative proposal was appropriate; and (iii) describe the alternative proposal(s) that DOJ allowed HSBC to implement instead, and whether each such alternative proposal has been fully and effectively implemented.

A.1.a.–c. The U.S. Government Accountability Office has noted that some $5 billion in fines, penalties, and forfeitures was collected from financial institutions for violations of the Bank Secrecy Act (BSA) between 2009 and 2015. Those numbers underscore that the Department of Justice (Department) and other agencies do not hesitate to hold financial institutions accountable when they do not comply with their BSA and sanctions obligations. HSBC was one of a number of examples of such efforts.

The Department has considered that, since the Department and HSBC entered into the 2012 Deferred Prosecution Agreement (DPA), HSBC worked to address the monitor's recommendations and, more broadly, strengthen its anti-money laundering (AML) program to avoid engaging in the types of willful criminal violations that led to the DPA. While the monitor's recommendations are a highly useful benchmark, the Department assesses the overall efforts of a company when exercising its discretion in deciding whether to extend a DPA or let it sunset as defined by its terms. Consistent with longstanding Department policy, we do not comment on the circumstances of individual cases. However, on April 5, 2018, we were pleased to provide a comprehensive briefing to your staff regarding DPAs. We hope this briefing was helpful in providing some background and context to address some of the issues raised by your questions above.

Q.2. In your testimony you described BSA information as critical to DOJ efforts to combat crime and terrorism.

Q.2.a. Can you describe in greater detail, from your experience in the Department of Justice's criminal division, the role that BSA-generated financial intelligence plays in counterterrorism and other law enforcement investigations—in developing investigative leads, sharpening focus on certain criminal players and their banks, or otherwise?

A.2.a. Effective AML programs—including accurate and timely SARs—play a critical role in the fight against criminal activity, and often serve as an important source of information for law enforcement investigations into money laundering, terrorist financing, and other crimes. Prosecutors and agents routinely use the information generated by BSA filings, including SARs and Currency Transaction Reports (CTRs), on both a proactive and reactive basis. Law enforcement, for example, often uses SARs, CTRs, and other BSA reporting to identify the leads necessary to launch an investigation. Law enforcement also uses BSA reporting to obtain information on known targets and their illicit transactions to advance investigations already underway. Additionally, law enforcement and regulators rely on BSA information to identify broader trends and risks.

Further, effective AML programs help financial institutions detect efforts to launder illicit proceeds, which can, in turn, prevent those funds from ever entering the U.S. financial system. Domestic collection of AML information also improves the United States' ability to respond to similar requests from foreign law enforcement for investigative assistance, thus increasing our ability to fight financial crime on the global stage.

Q.2.b. What financial intelligence tools are currently most useful to prosecutors, sanctions overseers and others who combat money laundering, and where do we need to strengthen DOJ's tool kit?

A.2.b. Because most criminals are motivated by financial gain, they must find ways to use the proceeds of their crimes. For the most sophisticated criminal actors and organizations—who are often generating substantial amounts in illicit proceeds—it is impractical, inefficient, and simply dangerous to move their money in hard currency. As a result, many criminals—and especially the most sophisticated among them—must bring their proceeds into the financial system in order to launder them. Successful introduction and laundering of illicit proceeds through the financial system allows criminals to purchase goods, reinvest in the criminal enterprise, or fund additional criminal conduct, all of which cause further harm to our communities—not just through the promotion of the underlying criminal conduct itself, but also through the distorting effects that criminal proceeds can have on our markets.

Financial intelligence is critical to law enforcement's efforts to thwart these illicit money flows because it allows law enforcement to see the full criminal network. By reviewing information from SARs, CTRs, and other BSA reporting, for example, law enforcement may be able to trace money flowing to different parts of the network—those that generate the illicit proceeds and those used to redistribute them. Because this data is so essential to law enforcement's work, the Department believes that any proposals to alter such reporting requirements should take into account the significant value of this information and the effects—particularly the

potential harms—such changes might have on law enforcement investigations and prosecutions.

Other tools are also important to law enforcement's money laundering investigations and prosecutions. As this Committee is aware, the pervasive use of front companies, shell companies, nominees, or other means to conceal the true beneficial owners of assets is one of the greatest loopholes in this country's AML regime. The lack of beneficial ownership information can significantly slow investigations because determining the true ownership of bank accounts and other assets often requires that law enforcement undertake a time-consuming and resource-intensive process. For example, investigators may need grand jury subpoenas, witness interviews, or foreign legal assistance to unveil the true ownership structure of shell or front companies associated with serious criminal conduct. This process can take years—information obtained on a particular entity, for example, may show that it is a shell company owned by yet another shell company, requiring additional subpoenas or other information-gathering efforts. In some cases, law enforcement may not be able to determine the owners of illicit proceeds at all.

Treasury's Customer Due Diligence Final Rule—and its requirement that financial institutions collect and verify the personal information of certain beneficial owners when the companies they own, control, or profit from open accounts—is a critical step that will make it more difficult for criminals to circumvent the law by using opaque corporate structures. But we must do more. Other steps are needed to ensure that criminals cannot hide behind nominees, shell corporations, and other legal structures to frustrate law enforcement. More effective legal frameworks would reduce the United States' vulnerability to criminals seeking access to our financial system, facilitate law enforcement investigations, and bring the United States into compliance with international AML and counter-terrorist-financing (CTF) standards. The Department looks forward to continued discussions with its interagency partners, Congress, and industry regarding stronger laws that target individuals who seek to mask the ownership of companies, accounts, and sources of funds, as well as proposals to require the collection and maintenance of beneficial ownership information.

Another important law enforcement tool is the information it obtains from its foreign partners. Because money often moves across multiple jurisdictions in the global economy, U.S. law enforcement depends on the cooperation of overseas counterparts to obtain evidence and to trace, freeze, and seize assets wherever they are located. However, existing authorities do not fully address the complexities of these international investigations. Specifically, under the existing authority in 31 U.S.C. § 5318(k), foreign banks are not required to produce records in a manner that would establish their authenticity and reliability for evidentiary purposes. The statute also does not contain any anti-tip-off language, meaning that foreign banks who receive subpoenas from U.S. law enforcement could disclose the subpoenas to account holders or others, thereby compromising an ongoing investigation. The only sanction provided under current law is the closure of the correspondent account, which, in most cases, will not result in the production of the

records, and may in fact impede law enforcement investigations. There is no procedure to seek to compel compliance with subpoenas to foreign banks, nor any explicit authority to impose sanctions for contempt. Finally, the current statute provides that no effort can be taken by the Attorney General or the Secretary of Treasury to close the correspondent account or a foreign bank when the foreign bank has brought proceedings to challenge enforcement of the subpoena. The Administration continues to discuss proposed amendments to address these problems, and looks forward to working with Congress on these issues.

Q.3. The Panama Papers and other similar document leaks revealed the widespread systematic use of shell corporations by wealthy bad actors seeking to not only evade lawful tax collection, but also to facilitate all kinds of financial crime.

Q.3.a. How would you characterize the urgency of the threat to the U.S. financial system posed by anonymous shell companies, and by the lack of a coherent national framework for identifying beneficial ownership at the point of company formation?

A.3.a. The pervasive use of front companies, shell companies, nominees, and other means to conceal the beneficial owners of assets is one of the greatest loopholes in this country's AML regime. We consistently see bad actors using these entities to disguise the ownership of the dirty money derived from criminal conduct.

Indeed, the Financial Action Task Force's (FATF) 2016 review of our AML/CTF system highlighted this issue as one of the most critical gaps in the United States. The FATF rated the United States "noncompliant" on the FATF standard covering transparency and beneficial ownership of legal persons, noting the United States' "generally unsatisfactory measures for ensuring that there is adequate, accurate, and updated information" on beneficial ownership, as defined by FATF, that "can be obtained or accessed by competent authorities in a timely manner." The result, FATF said, is that U.S. law enforcement authorities "must often resort to resource-intensive and time-consuming investigative and surveillance techniques."

More effective legal frameworks are accordingly needed to ensure that criminals cannot hide behind nominees, shell corporations, and other legal structures to frustrate law enforcement. When law enforcement is able to obtain information on the identities of the persons who ultimately own or control these legal entities, it can better see the full network of criminal proceeds as bad actors try to bring money into our financial system. With proper law enforcement access to beneficial ownership information, the Department could bring more cases, more quickly, with more impact.

Q.3.b. Can you provide the Committee with concrete examples you have seen of how bad actors use shell companies for money laundering, terror finance and other illicit purposes?

A.3.b. Below are several illustrative examples of the use of shell or front companies to facilitate illicit conduct:

- In 2017, Ebong Tilong, the owner of a Houston home health agency, was sentenced by a U.S. District Judge in the Southern District of Texas to 80 years in prison for his role in a $13

million Medicare fraud scheme and for filing false tax returns. In November 2016, after the first week of trial, Tilong pleaded guilty to one count of conspiracy to commit healthcare fraud, three counts of healthcare fraud, one count of conspiracy to pay and receive healthcare kickbacks, three counts of payment and receipt of healthcare kickbacks, and one count of conspiracy to launder monetary instruments. In June 2017, Tilong pleaded guilty to two counts of filing fraudulent tax returns. According to the evidence presented at trial and his admissions to the tax offenses, from February 2006 to June 2015, Tilong received more than $13 million from Medicare for home health services that were not medically necessary or not provided to Medicare beneficiaries. In connection with his guilty plea to the tax offenses, Tilong admitted that to maximize his gains from the Medicare fraud scheme, he created a shell company to limit the amount of tax that he paid to the IRS on the proceeds that he and his co-conspirators stole from Medicare.

- In April 2018, Nicholas A. Borgesano, Jr. was sentenced to 15 years in prison and ordered to pay $54 million in restitution in connection with a $100 million compounding pharmacy fraud scheme. In November 2017, Borgesano pleaded guilty in the Middle District of Florida to one count of conspiracy to commit healthcare fraud and one count of conspiracy to engage in monetary transactions involving criminally derived property. According to admissions made in his plea agreement, Borgesano owned and operated numerous pharmacies and shell companies that he and his co-conspirators used to execute a fraud scheme involving prescription compounded medications. The scheme generated over $100 million in fraud proceeds. Borgesano admitted that he disbursed proceeds of the fraud scheme through a variety of methods, including by check and wire transfer to co-conspirators' shell companies and through the purchase of assets. Seven other defendants previously pleaded guilty to conspiracy to commit health care fraud for their roles in the scheme. Real properties, vehicles, and a 50' Cigarette racing boat purchased with proceeds from the fraud scheme were forfeited as part of the sentencing of Borgesano and others. Those assets totaled over $7.6 million.
- In August 2017, the United States filed two civil complaints in the U.S. District Court for the District of Columbia seeking the imposition of a civil money laundering penalty and to civilly forfeit more than $11 million from companies that allegedly acted as financial facilitators for North Korea. One complaint seeks nearly $7 million associated with Velmur Management Pte. Ltd., a Singapore-based company, and the other seeks more than $4 million from Dandong Chengtai Trading Co. Ltd., a company in Dandong, China. The complaints allege that the companies have participated in schemes to launder U.S. dollars on behalf of sanctioned North Korea entities. According to the complaints, the companies participated in financial transactions in violation of the International Emergency Economic Powers Act, the North Korea Sanctions and Policy Enhancement Act of 2016, and Federal conspiracy and money laundering statutes. One of the complaints alleges that Velmur

and Transatlantic Partners Pte. Ltd. laundered U.S. dollars on behalf of sanctioned North Korean banks that were seeking to procure petroleum products from a designated entity. According to the complaint, designated North Korean banks use front companies, including Transatlantic, to make U.S. dollar payments to Velmur. The second complaint alleges that Dandong Chengtai and associated front companies controlled by Chi Yupeng, a Chinese national, comprise one of the largest financial facilitators for North Korea.

- In 2016, Thomas Davanzo and Robert Fedyna were sentenced to 121 months and 135 months in prison, respectively, for their participation in a multi-State scheme to defraud biofuel buyers and U.S. taxpayers by fraudulently selling biofuel credits and fraudulently claiming tax credits. Both defendants were also ordered to forfeit ill-gotten gains from the conspiracy of over $46 million and other items to the Government, including gold coins, jewelry and Rolex watches, thoroughbred horses, vehicles, and properties. Davanzo and Fedyna operated several shell companies that were used to facilitate the scheme. As part of the scheme, Davanzo and Fedyna operated entities that purported to purchase renewable fuel, on which credits had been claimed and which was ineligible for additional credits, produced by their co-conspirators at Gen-X Energy Group (Gen-X), headquartered in Pasco, Washington, and its subsidiary, Southern Resources and Commodities (SRC), located in Dublin, Georgia. They then used a series of false transactions to transform the fuel back into feedstock needed for the production of renewable fuel, and sold it back to Gen-X or SRC, allowing credits to be claimed again. This cycle was repeated multiple times.

Q.3.c. 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.c. Money can be laundered in a wide variety of ways outside the financial sector. For example, company formation agents, investment advisors, real estate agents, lawyers, and other professionals can be exploited by criminal actors seeking to conceal or otherwise move illicit proceeds. These professionals may—knowingly or unknowingly—help disguise the identity of the criminal actors behind the movement of illicit funds. They may do this by helping the bad actors hide the true owners of asset. That, in turn, can significantly slow an investigation and sometimes grind it to a halt altogether.

Lawyers and law firms, for example, routinely hold funds on behalf of clients to cover things like retainer payments. But when the funds are in limited amounts or held on a short-term basis, a dedicated client bank account can be cumbersome. Interest on lawyer accounts (IOLAs) allow lawyers to pool these funds on behalf of multiple clients. But IOLA accounts can present heightened money laundering risks because financial institutions do not have information on a law firm's many clients.

The Department's ongoing civil asset forfeiture action to recover more than a billion dollars allegedly stolen from the Malaysian sovereign wealth fund, lMDB, demonstrates the ways in which bad actors may use other entities and persons, including lawyers, to facilitate money laundering. Our publicly filed complaint in that matter alleges that nearly $370 million in stolen funds was diverted by the defendants over a 7-month period in 2010 from a 1MDB joint venture into an IOLA account held by a law firm in the United States. The money was then allegedly used by one of the defendants to fund his opulent lifestyle, including the purchase of luxury real estate, a Beverly Hills hotel, and a private jet, as well as the production of the movie "The Wolf of Wall Street." In other words, $370 million passed through financial institutions where, unless the bank asked additional questions, the financial system saw these transfers as on behalf of the law firm—not on behalf of the underlying individual allegedly involved in the 1MDB scheme.

In addition to highlighting the role of lawyers, the lMDB case also underscores how criminals use the real estate sector to launder and hide their ill-gotten gains. FinCEN has issued and expanded Geographic Targeting Orders (GTOs) in recent years focusing on the real estate sector to learn more about individuals who may be attempting to hide their assets and identity by purchasing residential properties with cash and/or through limited liability companies and other opaque structures. The Department looks forward to more discussions on additional steps that may be warranted to address the money laundering risks emanating from this sector.

Q.3.d. Who should we be looking at that we are not currently regulating—real estate firms, escrow agents, company formation lawyers, others?

A.3.d. Please see above.

Q.4. As banks have racked up huge fines in recent years for skirting sanctions and violating money laundering regulations, the sector as a whole has begun to wake up to AML obligations in place for many years, and many have made big investments to strengthen compliance.

Q.4.a. Do you believe that AML laws and regulations on the books now offer a sufficient deterrent to such behavior?

A.4.a. In recent years, the Department has resolved numerous AML and sanctions-based violations with major financial institutions. These resolutions have involved Commerzbank, Citigroup, BNP Paribas, Standard Chartered, HSBC, UBS, RBS, and Barclays, to name just a few. While the Department believes these resolutions have a deterrent effect on willful violations, they also demonstrate that institutions still face challenges in creating and encouraging a culture of compliance—meaning, in some cases, financial institutions still struggle to see managing compliance risk as equally important as managing credit risk or liquidity risk.

Q.4.b. Are there specific steps you would urge Congress to consider to strengthen the current regime?

A.4.b. The Department supports continued discussion of methods to better target financial institution reporting, as that will increase

efficiencies for both law enforcement and industry. However, financial institutions play a critical role in the fight against money laundering and terrorist financing; therefore, from a law enforcement perspective, any regulatory reform to existing reporting requirements for financial institutions must be done with caution, following careful analysis of the existing regime.

For example, law enforcement relies extensively on SARs and CTRs in civil and criminal investigations and prosecutions, including those involving money laundering and terrorist financing. The Department uses the information contained in these filings—on both a proactive and reactive basis—to carry out investigations of specific individuals and entities and to identify leads, connect the dots, and otherwise advance investigations in their early stages. Law enforcement and regulators also use aggregated information from this reporting to identify trends and risks.

Proposed increases in the monetary thresholds for SARs and CTRs would decrease filing, and correspondingly, reduce law enforcement's access to information. Such changes could also eliminate an array of data that provides critical leads and information for law enforcement when pursuing investigations and prosecutions. The Department believes that any proposals to alter such reporting requirements should accordingly take into account the significant value of this information and the effects—particularly the potential harms—such changes could have on law enforcement investigations and prosecutions.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR SASSE FROM M. KENDALL DAY

Q.1. Mr. Day, your testimony estimated that money laundering reaches around $2 trillion annually, $300 billion of which is in the United States and $64 billion of which is generated by drug trafficking sales. I'd like to get a further breakdown of this number.

Q.1.a. Can you provide a geographic breakdown of where the money laundering takes place within the United States?

A.1.a. Because money laundering is a necessary consequence of nearly all profit-generating crime, it can occur anywhere in the world. Moreover, criminals always work to exploit gaps and vulnerabilities in existing laws and regulations to find new ways to conduct illicit transactions. It is therefore difficult to say precisely how much money laundering takes place within the United States, and whether money laundering activity is concentrated in any particular geographic area.

Q.1.b. Can you provide a more precise breakdown of where the money laundering generally takes place by criminal industry, beyond drug trafficking to also include fraud, tax evasion, human smuggling, organized crime or terrorist organizations such as Hezbollah, and public corruption?

A.1.b. Treasury's National Money Laundering Risk Assessment (2015) (NMLRA) analyzed more than 5,000 law enforcement cases, financial reporting by U.S. financial institutions, and reports from across the Government and private sector to define key money

laundering and terrorist financing risks to the United States. According to the NMLRA:

- Approximately 20 percent of the estimated $300 billion generated in illicit activity annually in the United States—$64 billion—is associated with drug trafficking.
- Fraud accounts for most financial crime in the United States. This includes healthcare fraud, identity theft, tax fraud, mortgage fraud, retail and consumer fraud, and security fraud, with healthcare fraud accounting for the largest dollar volume of fraud losses to the Federal Government—approximately $80 billion annually.
- Direct and indirect losses from identity theft totaled $24.7 billion in 2012.
- The Internal Revenue Service found $6.5 billion in attempted fraudulent tax refunds in 2010, and the Treasury Inspector General for Tax Administration found potentially $5.2 billion more.

Q.2. You testified that a "large amount that isn't included in the $300 [b]illion would touch the U.S. financial system . . . through U.S. dollar clearing or other services that our financial system provides . . . to the global economy."

Can you provide a more precise figure for how much money laundering annually at least touches the U.S. financial system?

A.2. Little empirical evidence exists to determine precisely how much dirty money flows through the U.S. financial system. According to the U.N. Office of Drugs and Crime, however, best estimates show that criminal proceeds totaled $2.1 trillion in 2009, and of that, close to $1.6 trillion was laundered. Given the size, sophistication, and stability of the U.S. financial system, and the number of products and services offered by U.S. financial institutions, bad actors continuously seek to launder their illicit proceeds through our financial system.

Q.3. I'd like to understand better the law enforcement context for the United State's efforts to fight money laundering.

Q.3.a. Does the U.S. financial system substantially—even if inadvertently—facilitate human trafficking?

Q.3.b. If so, how?

Q.3.c. What about terrorism, such as organizations like Hezbollah?

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

Q.3.e. How can law enforcement officials use anti-money laundering tools to target specific groups such as MS–13 or Hezbollah?

Q.3.f. Are there particular criteria of suspiciousness associated with transactions conducted for the benefit of groups such as MS–13 or Hezbollah?

Q.3.g. Can you walk me through a typical case where law enforcement officials used financial intelligence, such as suspicious activity reports, to fight terrorism or transnational criminal organizations such as MS–13?

A.3.a.–g. Criminals will always work to exploit gaps and vulnerabilities in existing laws and regulations to find new

methods to conduct their illicit transactions, whether those transactions are related to human trafficking, drug trafficking, terrorism, gang activity, and other crimes. New methods are always being devised, as the criminal underworld seeks to take advantage of emerging technologies and to outpace the development of new detection and investigation tools by law enforcement. Moreover, the United States has the deepest, most liquid, and most stable markets in the world. These features of the U.S. financial system bring many benefits, but they also attract criminals and their illicit funds. Criminals will continue to use every available money laundering method available to them, exploiting opportunities wherever they find them.

To combat these criminals and criminal organizations, as well as their efforts to launder money through our financial system, law enforcement routinely relies on AML tools.

Prosecutors and investigators use the information generated by BSA fillings, including SARs and CTRs, to identify the leads necessary to launch an investigation. They also use BSA reporting to advance investigations already underway. Moreover, law enforcement and regulators rely on BSA information to identify broader trends and risks. For criminal groups, this financial intelligence is particularly important because it allows law enforcement to see the full criminal network. By reviewing information from SARs, CTRs, and other BSA reporting, for example, law enforcement may be able to trace money flowing to different parts of the network—those that generate the illicit proceeds and those used to redistribute them.

The Department, in coordination with our colleagues from other agencies and international law enforcement partners, has had numerous recent successes in thwarting criminals who sought to move, hide, or otherwise shelter their criminal proceeds using the U.S. financial system. Financial intelligence has played—and will continue to play—a critical role in many such prosecutions. Some examples of investigations and prosecutions that have relied on BSA data from financial institutions include the cases chosen by FinCEN for its annual "Law Enforcement Awards." Summaries of the cases that won the award in 2017 can be found at *https://www.fincen.gov/sites/default/files/2018-01/LE%20Awards%202017%20FINAL%20May9%20cases.pdf.*

Q.4.a. 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 healthcare 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 identity money laundering and how much more progress can be made in this front?

A.4.a. Technological innovations, including artificial intelligence, can be useful tools for financial institutions and other organizations in identifying patterns and detecting anomalies. These innovations have the potential to not only improve the detection of suspicious

transactions and activities, but to allow for such detection with greater efficiency. It is important to note, however, that these sophisticated technological tools do not eliminate the need for human interaction and detection. Human instincts and analysis are vital in law enforcement's fight against all types of crime, including money laundering.

The Department supports technological innovations that will enable financial institutions to better identify, prevent, and report on money laundering, terrorist financing, and other crimes. To better understand these innovations, and their potential implications for investigations and prosecutions of illicit finance, the Department routinely participates in discussions with Treasury, Federal banking regulators, financial institutions, and international partners on these topics.

Q.4.b. Outside of AI and machine learning, how can recent FinTech innovations such as blockchain fight money laundering?

A.4.b. As noted above, the Department routinely participates in discussions with regulators, the private sector, and foreign counterparts to better understand the potential implications of these fast-emerging technological innovations for the investigation and prosecution of money laundering and other crimes.

Q.4.c. How much does bitcoin, blockchain, and other cryptocurrencies facilitate money laundering?

A.4.c. Criminals use cryptocurrencies to conduct illicit transactions because they offer potential anonymity, since cryptocurrency transactions are not necessarily tied to a real-world identity and enable criminals to quickly move criminal proceeds among countries. Virtual currencies thus offer an alternative to cash. The Department continues to see the use of bitcoin by criminals but has also noted an increase in the use of alternative cryptocurrencies. As with any criminal behavior, the Department can and does draw on its full complement of law enforcement tools to investigate and prosecute this activity, when supported by the evidence.

As just one example, in 2013, the Government shut down Liberty Reserve, which allowed users around the world to send and receive payments using cryptocurrencies—and which was used by online criminals to launder the proceeds of Ponzi schemes, credit card trafficking, stolen identity information, and computer hacking schemes. Liberty Reserve's founder built and operated Liberty Reserve expressly to facilitate large-scale money laundering for criminals by providing them near-anonymity and untraceable financial transactions. In 2016, Liberty Reserve's founder pleaded guilty to money laundering charges and was sentenced to 20 years in prison.

The Department announced in July 2017 that it had seized the largest criminal marketplace on the internet, AlphaBay. AlphaBay operated for over 2 years on the dark web and was used to sell deadly illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals throughout the world. AlphaBay operated as a hidden service on the "Tor" network, and utilized cryptocurrencies including Bitcoin, Monero, and Ethereum to hide the locations of its underlying servers and the identities of its administrators, moderators, and users. Based on law enforce-

ment's investigation of AlphaBay, authorities believe the site was also used to launder hundreds of millions of dollars deriving from illegal transactions on the website.

As illustrated by these examples, the laundering of illicit proceeds through cryptocurrencies knows no borders. And some countries, unlike the United States, do not currently regulate virtual currencies—and therefore have limited oversight and few AML controls. The assistance of our interagency and international partners is an important element of the Department's success in its AML efforts. Because money often moves across multiple countries in the global economy, U.S. law enforcement depends on the cooperation of foreign counterparts to aggressively investigate money laundering cases touching the United States. Domestic and international law enforcement partners must work together to obtain evidence and to trace, freeze, and seize assets wherever they are located.

Q.4.d. How can law enforcement officials best stop this newer form of money laundering?

A.4.d. Please see answer above.

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.

Q.5.a. What percentage of SARs are actually read by someone in law enforcement?

A.5.a. Law enforcement relies extensively on SARs in civil and criminal investigations and prosecutions, including those involving money laundering and terrorist financing. The Department uses the information contained in these filings—on both a proactive and reactive basis—to carry out investigations of specific individuals and entities and to identify leads, connect the dots, and otherwise advance investigations in their early stages. Law enforcement and regulators also use aggregated information from this reporting to identify trends and risks. A key component of these efforts are SAR Review Teams, which cover all 94 Federal judicial districts. Through their review and analysis of SARs, these teams aim to prevent future terrorist attacks, disrupt and dismantle criminal enterprises, combat money laundering, strengthen the U.S. financial system through the enforcement of the BSA, facilitate interagency cooperation and information sharing, gather intelligence, and improve communications among law enforcement agencies and the financial community.

Q.5.b. How often do financial institutions receive feedback from law enforcement officials as to the utility of their SAR filing?

A.5.b. The Department cannot comment on open investigations, and therefore often cannot comment on the usefulness of any particular information shared by financial institutions with law enforcement. Moreover, a Federal statute prohibits the disclosure of certain information regarding grand jury subpoenas for financial institution records. However, the Department actively participates in Treasury's Bank Secrecy Act Advisory Group (BSAAG), which consists of representatives of Federal regulatory and law enforcement agencies, financial institutions and trade groups with members subject to the BSA's requirements. Through this group, Treasury obtains advice on the operation of the BSA, including the SAR process. The Department also supports further study of SARs, CTRs, and other reporting requirements, and believes that gathering data about these reports will enable Congress and the Administration to better assess whether to amend the existing regime.

Further, Treasury's recently launched FinCEN Exchange program brings together law enforcement, financial institutions, and FinCEN in regular briefings—which the Department has attended—to facilitate information sharing on cases, typologies, and threats. This initiative will not only help financial institutions build their systems and algorithms to better identify risks and prioritize targets, but it will also help achieve our broader shared goal of a strong and effective AML regime. The FinCEN Exchange program is an addition to other efforts designed to foster cooperation between the public and private sectors, including the BSAAG.

Q.5.c. 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 we resolve this conflict?

A.5.c. Proposed increases in the monetary thresholds for SARs and CTRs would decrease filing, and correspondingly, reduce law enforcement's access to information. Such changes could also eliminate an array of data that provides critical leads and information for law enforcement when pursuing investigations and prosecutions.

There are many crimes that do not involve the movement of significant amounts of money. One potential disadvantage of raising the CTR and SAR reporting thresholds without careful consideration and study of the existing data is that law enforcement may lose visibility into those crimes. The lone wolf terrorist is an apt example—those cases typically do not involve large transfers of money. Therefore, these transactions may not hit upon one of the CTR or SAR thresholds, were Congress to increase those thresholds. Figures from FinCEN, for example, show that 79 percent of CTR filings in 2017 were for amounts below $30,000—one of the thresholds that has been proposed. Increasing the $10,000 threshold for CTRs—also the current threshold for CMIRs at the borders—could thus reduce CTR filing significantly, hurting law enforcement's access to information regarding the use of cash. Increasing SAR reporting thresholds would similarly decrease SAR

filings, leaving law enforcement with less information on suspicious activity generally.

The Department supports continued discussion of methods to better target financial institution reporting, as that will increase efficiencies for both law enforcement and industry. At the same time, the Department believes that any proposals to alter such reporting requirements should take into account the significant value of this information and the effects—particularly the potential harms—such changes could have on law enforcement investigations and prosecutions.

Q.5.d. 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.5.d. As noted above, Treasury's recently launched FinCEN Exchange program brings together law enforcement, financial institutions, and FinCEN in regular briefings—which the Department has attended—to facilitate information sharing on cases, typologies, and threats.

This initiative will not only help financial institutions build their systems and algorithms to better identify risks and prioritize targets, but it will also help achieve our broader shared goal of a strong and effective AML regime.

Q.5.e. 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.5.e. The Department supports continued discussion of methods to enhance information sharing and better target financial institution reporting, and looks forward to continued discussions with its interagency partners, Congress, and industry on these topics.

Q.6.a. Often, financial institutions will de-risk 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 de-risking is actually unhelpful for law enforcement purposes, because it drives these criminals underground and makes it more difficult to track them?

A.6.a. Yes, in some circumstances, de-risking by closing some customers' financial accounts in order to reduce the risk exposure of financial institutions to certain categories of high-risk customers and jurisdictions may hinder ongoing law enforcement investigations.

Q.6.b. At the moment, do the regulators that evaluate and enforce financial institutions compliance with our Federal money laundering take this into account?

A.6.b. The Department defers to its colleagues at the Federal banking regulators to respond to this question.

Q.6.c. 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 de-risk?

A.6.c. As noted above, the Department actively participates in Treasury's BSAAG, through which Treasury obtains advice from Federal regulatory and law enforcement agencies, financial institutions, and trade groups on the operation of the BSA. Treasury's recently launched FinCEN Exchange program also brings together law enforcement, financial institutions, and FinCEN in regular briefings—which the Department has attended—on cases, typologies, and threats.

Q.6.d. 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.6.d. The Department supports continued discussion of methods to enhance information sharing and better target financial institution reporting, and looks forward to continued discussions with its interagency partners, Congress, and industry on these topics.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR TILLIS FROM M. KENDALL DAY

Q.1. Mr. Day—in your testimony and at the hearing, you site figures that the U.N. Office on Drug and Crime estimates that annual illicit proceeds total more than $2 trillion globally. Additionally, you site that number to be around $300 billion in 2010.

Q.1.a. In terms of how DOJ (Department) allocates its resources, does the Department allocate resources based on the predicate offense and/or the most prevalent source of illicit activity?

A.1.a. The Department has a dedicated section in the Criminal Division, the Money Laundering and Asset Recovery Section (MLARS), leading its asset forfeiture and AML efforts. MLARS handles significant cases in these areas and also works closely with other components of the Criminal Division and U.S. Attorneys' Offices across the country on such matters. MLARS' Bank Integrity Unit investigates and prosecutes complex, multi-district, and international criminal cases involving financial institutions and individuals who violate various Federal statutes, including the Money Laundering Control Act, the BSA, and economic and trade sanctions programs authorized by the International Emergency Economic Powers Act. The Unit's prosecutions generally focus on banks and other financial institutions, including their officers, managers, and employees, whose actions threaten the integrity of the individual institution, the wider financial system, or both.

MLARS' Money Laundering and Forfeiture Unit investigates and prosecutes professional money launderers and gatekeepers who provide their services to serious criminal organizations, such as Mexican drug cartels, as well as individuals and entities using the latest and most sophisticated money laundering tools and techniques. The Money Laundering and Forfeiture Unit also litigates civil forfeiture cases for the Criminal Division and, in appropriate cases, in partnership with United States Attorneys' Offices. It also

provides support to the Division in cases involving significant or complex criminal forfeiture allegations. The Unit also serves as the Division's experts on domestic forfeiture and, in this role, provides advice to other Division attorneys and United States Attorneys' Offices.

In addition, MLARS recently added a lawyer in the role of Digital Currency Counsel in MLARS's Special Financial Investigations Unit. That attorney focuses on providing support and guidance to investigators, prosecutors, and Government agencies on cryptocurrency prosecutions and forfeitures; expanding and implementing cryptocurrency-related training to encourage and enable more investigators, prosecutors, and Department agencies to pursue such cases; developing and disseminating policy guidance on various aspects of cryptocurrency; advising Assistant U.S. Attorneys (AUSAs) and Federal agents on complex questions of law related to cryptocurrencies; and identifying additional actors—including professional money launderers, money transmitters, gatekeepers, and financial institutions—who use cryptocurrencies to facilitate illicit finance.

Also instrumental in the Department's AML efforts are the Criminal Division's Fraud Section, Computer Crimes and Intellectual Property Section, Narcotic and Dangerous Drug 24 Section, Organized Crime and Gang Section; the Tax Division; the Civil Rights Division's Human Trafficking Prosecution Unit; the Organized Crime Drug Enforcement Task Forces; and the Department's investigative agencies, including the Federal Bureau of Investigation and the Drug Enforcement Agency. These prosecutors and investigators lend critical expertise in the predicate offenses involved in money laundering.

Q.1.b. What does this filter system look like?

A.1.b. In addition to the knowledge and resources available through MLARS, described above, the Department also deploys prosecutors as warranted in those jurisdictions facing particular criminal threats. For example, in August 2017, the Department announced the formation of the Opioid Fraud and Abuse Detection Unit, a pilot program specifically focused on opioid-related healthcare fraud. As part of that initiative, the Department funded 12 experienced AUSAs for a three-year term to focus solely on investigating and prosecuting healthcare fraud related to prescription opioids, including pill mill schemes and pharmacies that unlawfully divert or dispense prescription opioids for illegitimate purposes.

Q.1.c. Can you overview this system for me in terms of how the Department looks at illicit activity, filters this activity, and then concurrently using this information decides how or how not to bring criminal charges for BSA violations?

A.1.c. The Department follows the specific facts and evidence where they lead for each individual case. Where these facts and evidence support doing so, the various components of the Department mentioned above may take action for BSA violations, as demonstrated by a number of recent cases.

Q.2. Mr. Day—in follow up to a question I asked you at the hearing, I referenced a "working group" that Secretary Mnuchin is

forming at FSOC to study and evaluate issues related to digital currencies. I appreciate that fact that DOJ and others are also continually working on issues regarding digital currencies, but my question relates to the nature of FSOC.

Q.2.a. Specifically, since DOJ is not a member of FSOC, and as such, I want to know if you or others have been in communication with FSOC or Secretary Mnuchin to discuss the value that might be present in having someone from DOJ participate in the aforementioned "working group"?

A.2.a. Yes. John Cronan, the former Acting Assistant Attorney General for the Department's Criminal Division, attended a March 2018 meeting of Treasury's Financial Stability Oversight Council (FSOC). At that meeting, he discussed the role of cryptocurrency in illicit finance and the Department's efforts—in coordination with other Government agencies—to attack the challenges posed by cryptocurrencies.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM M. KENDALL DAY

Q.1. Is there a way to maintain a top-shelf effective anti-money laundering/combating the financing of terrorism (AML/CFT) policy while maintaining a commitment to increase access to financial products for the underbanked and immigrants who rely on remittance services?

A.1. The Department defers to its colleagues at the Federal banking regulators to respond to this question.

Q.2. Cryptocurrency exchanges are money services businesses supervised by State regulators and subject to Federal AML/CFT laws.

Q.2.a. What additional tools could we give regulators and law enforcement to enhance AML/CFT supervision?

A.2.a. The Department defers to its colleagues at Treasury to respond to this question.

Q.3. How prevalent is money laundering in cryptocurrency markets?

A.3. Criminals use cryptocurrencies to conduct illicit transactions because they offer potential anonymity, since cryptocurrency transactions are not necessarily tied to a real-world identity and enable criminals to quickly move criminal proceeds among countries. Virtual currencies thus offer an alternative to cash. The Department continues to see the use of bitcoin by criminals but has also noted an increase in the use of alternative cryptocurrencies. As with any criminal behavior, the Department can and does draw on its full complement of law enforcement tools to investigate and prosecute this activity, when supported by the evidence.

As just one example, in July 2017, the Department announced that it had seized the largest criminal marketplace on the internet, AlphaBay. AlphaBay operated for over 2 years on the dark web and was used to sell deadly illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals throughout the world. AlphaBay operated as a hidden service on

the "Tor" network, and utilized cryptocurrencies including Bitcoin, Morrero, and Ethereum to hide the locations of its underlying servers and the identities of its administrators, moderators, and users. Based on law enforcement's investigation of AlphaBay, authorities believe the site was also used to launder hundreds of millions of dollars deriving from illegal transactions on the website.

In 2013, meanwhile, the Government shut down Liberty Reserve, which allowed users around the world to send and receive payments using cryptocurrencies—and which was used by online criminals to launder the proceeds of Ponzi schemes, credit card trafficking, stolen identity information, and computer hacking schemes. Liberty Reserve's founder built and operated Liberty Reserve expressly to facilitate large-scale money laundering for criminals by providing them near-anonymity and untraceable financial transactions. In 2016, Liberty Reserve's founder pleaded guilty to money laundering charges and was sentenced to 20 years in prison.

As illustrated by these examples, the laundering of illicit proceeds through cryptocurrencies knows no borders. And some countries, unlike the United States, do not currently regulate virtual currencies—and therefore have limited oversight and few AML controls. The assistance of our interagency and international partners is an important element of the Department's success in its AML efforts. Because money often moves across multiple countries in the global economy, U.S. law enforcement depends on the cooperation of foreign counterparts to aggressively investigate money laundering cases touching the United States. Domestic and international law enforcement partners must work together to obtain evidence and to trace, freeze, and seize assets wherever they are located.

Q.4. Are there instances in which a failure to maintain an adequate AML program should result in legal consequences for individuals instead of corporations? If so, what are those circumstances?

A.4. Yes, where the facts and evidence support doing so, the Department does not hesitate to take action against individuals in connection with inadequate AML compliance programs. In December 2017, for example, a former vice president of Rabobank National Association (Rabobank) entered into a DPA the United States for his role in aiding and abetting Rabobank's failure to maintain an AML program that met BSA requirements. In February 2018, Rabobank, the California subsidiary of Netherlands-based Cooperative Rabobank U.A., pleaded guilty to a felony conspiracy charge for impairing, impeding, and obstructing its primary regulator by concealing deficiencies in its AML program and for obstructing the regulator's examination of Rabobank. Rabobank agreed to forfeit more than $368 million as a result of allowing illicit funds to be processed through the bank without adequate BSA or AML review. Additionally, in 2013, the head manager and the designated AML compliance officer of a Los Angeles check cashing store were sentenced to 5 years and 8 months in prison, respectively, for failing to follow Federal reporting and AML requirements in relation to more than $8 million in transactions.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM M. KENDALL DAY

Q.1. Gaming and tourism are some of Nevada's top sectors. In my State, 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 my State have suggested that gaming operators would welcome a review of BSA requirements. 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 depository and nondepository regulated entities. I wanted to follow up on my question in the Committee about the pros and cons of eliminating the requirement that a detailed factual narrative is required when filing a Suspicious Activity Report (SAR) form for structuring situations. In your responses, you mentioned that useful information is found in the detailed factual narrative more generally which I understand but wonder how useful this information is for structuring situations.

What are the pros and cons of eliminating the factual narrative for just structuring situations?

A.1. Like all BSA-generated financial intelligence, information in SAR filings—both in the reporting fields and in the factual narrative—is of great value to law enforcement investigations and prosecutions of money laundering, terrorist financing, and other crimes. The Department uses the information contained in SAR filings to carry out investigations of specific individuals and entities and to identify leads, connect the dots, and otherwise advance investigations in their early stages, among other things. Eliminating any portion of SAR data—even for a subset of the SAR filings—would decrease the amount of information available to law enforcement. Thus, while the Department welcomes discussions on how BSA reporting can be improved, it believes that such discussions should take into account the significant value of this information and the effects such changes could have on law enforcement investigations and prosecutions.

Q.2. I wanted to follow up on my question about raising the Currency Transaction and Suspicious Activity Reporting thresholds. In the hearing, you mentioned concerns that small dollar amounts can be used for criminal activities so there are risks to raising the thresholds. Some recommend raising them to either inflation or a lesser amount—from $5,000/$10,000 for suspicious activity reports and $20,000 or $25,000 for currency transaction reports.

Please expand on what we should consider if the threshold amounts for CTRs and SARs were increased.

A.2. Proposed increases in the monetary thresholds for SARs and CTRs would decrease filing, and correspondingly, reduce law enforcement's access to information. Such changes could also eliminate an array of data that provides critical leads and information for law enforcement when pursuing investigations and prosecutions. The Department believes that any proposals to alter such reporting requirements should accordingly take into account the

significant value of this information and the effects—particularly the potential harms—such changes could have on law enforcement investigations and prosecutions.

Moreover, there are many crimes that do not involve the movement of significant amounts of money. One potential disadvantage of raising the SAR and CTR reporting thresholds without careful consideration and study of the existing data is that law enforcement may lose visibility into those crimes. The lone wolf terrorist is an apt example—those cases typically do not involve large transfers of money. Therefore, these transactions may not hit upon one of the CTR or SAR thresholds, were Congress to increase those thresholds. Figures from FinCEN, for example, show that 79 percent of CTR filings in 2017 were for amounts below $30,000—one of the thresholds that has been proposed. Increasing the $10,000 threshold for CTRs—also the current threshold for Currency and Monetary Instrument Reports (CMIRs) at the borders—could thus reduce CTR filing significantly, hurting law enforcement's access to information regarding the use of cash. Increasing SAR reporting thresholds would similarly decrease SAR filings, leaving law enforcement with less information on suspicious activity generally.

Accordingly, the Department believes that any discussion of amending these reporting thresholds should be analyzed against existing reporting data, and balanced against law enforcement's need to maintain visibility into these types of criminal activity.

Q.3. 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.

Do you think institutions are taking advantage of those red flags, in order to better assess whether their banks are being used to finance human trafficking?

A.3. Law enforcement relies extensively on SARs and CTRs in civil and criminal investigations and prosecutions to identify and trace illicit proceeds for a range of crimes. With respect to financial institutions' use of the red flags laid out in the FinCEN advisory, the Department defers to its colleagues at Treasury to respond to this question.

Q.4. I served as Attorney General of Nevada for 8 years. I know that investigations of organized crime, terrorist financing and money laundering rely on collaboration with leaders and governments of other nations.

As the Under Secretary for Terrorism and Financial Crimes, how does your office collaborate with African nations to curb terrorist financing and money laundering?

A.4. The Department defers to its colleagues at Treasury to respond to this question.

Q.5. Secretary Mandelker, Treasury's Office of Technical Assistance has been a critical resource to collaborate and strengthen other nations. I would like to better understand how the Office of Technical Assistance works.

Q.5.a. Which nations did the Office of Technical Assistance serve in 2016 and 2017? How many nations requested assistance but have been denied?

Q.5.b. Please detail why the assistance was denied: lack of U.S. funding, diplomatic considerations, another nation was better suited to provide the information, *etc.*?

Q.5.c. Please provide annual OTA funding levels from 2010 until today?

A.5.a.–c. The Department defers to its colleagues at Treasury to respond to these questions.

Q.6. For years, Treasury relied on supplemental fund transfers from the State Department, USAID and other Government agencies.

Q.6.a. How much did OTA receive from State and USAID in 2014, 2015, 2016, and 2017?

Q.6.b. How is the OTA working with the International Monetary Fund and the World Bank to prevent terrorist financing and money laundering?

A.6.a.–b. The Department defers to its colleagues at Treasury to respond to these questions.

Q.7. Kenya's M–Pesa is an electronic system that captures every transaction. All M–Pesa customers must identify themselves with their original identification document. There is three-factor authentication: SIM card, ID and the PIN. The Central Bank of Kenya receives regular reports on transactions.

What can we learn from Kenya and other nations about how to use mobile banking to provide access to financial services and also avoid terrorist and other forms of illicit financing?

A.7. The Department defers to its colleagues at Treasury to respond to this question.

Q.8. 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 de-risking has become epidemic in some communities, such as communities along the Southwest border, remittances providers serving fragile nations like Somalia and humanitarian groups. In your testimony, you mention Treasury's efforts to ensure humanitarian remittances reach Venezuela as you work to stem financial corruption in that nation.

Please explain what steps the Treasury Department is taking in Venezuela to stabilize humanitarian remittances?

A.8. The Department defers to its colleagues at Treasury to respond to this question.

Q.9. How will the Treasury Department work with the other banking regulators—OCC, FinCEN, FDIC and the Federal Reserve—along with the IRS to help banks meet the banking needs of legitimate consumers and businesses that are at risk of losing access—or have already lost access?

Q.9.a. Has Treasury been able to stem the decline in correspondent banking relationships that have limited financial access to many?

Q.9.b. If so, how?

Q.9.c. If not, what policies could restore and expand correspondent banking relationships?

A.9.a.–c. The Department defers to its colleagues at Treasury to respond to these questions.

Q.10. Last year, the Countering Iran's Destabilizing Activities Act of 2017 (Public Law 115–44) was enacted. In Section 271, it required the Treasury Department to publish a study by May 1, 2018, on two issues: 1. Somali Remittances. The law required 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.

Q.10.a. What is the status of this study?

Q.10.b. Are you contacting other organizations in your research?

Q.10.c. Which ones—or types of groups—have you met with?

Q.10.d. Will the Treasury Department meet the deadline of May 1, 2018 to publish the report?

A.10.a.–d. The Department defers to its colleagues at Treasury to respond to these questions.

Q.10.e. Anonymous incorporation is not difficult for criminals—virtually no States require corporate applications provide the identity of the corporation's ultimate owner. Law enforcement has said it needs to know the owners of firms in order to investigate financial crimes and terrorism.

Q.10.f. How should Congress and/or Treasury tailor these proposed requirements so as not to be overly burdensome on either incorporating entities or the States themselves?

Q.10.g. Should Congress exempt any firm already regulated by Federal banking regulators and companies with over 20 employees?

Q.10.h. Some argue that those types of companies are very unlikely to open bank accounts to hide or move criminal funds or to hold illegal assets, do you agree?

Q.10.i. Does the Treasury Department need legislation to issue regulations requiring corporations and limited liability companies formed in any State that does not already require ownership disclosure to file information about their beneficial ownership with Treasury as well?

Q.10.j. What type of disclosure should be required: name, current address, nonexpired passport or State-issued driver's license, identification of any affiliated legal entity that will exercise control over the incorporated entity; *etc.*?

Q.10.k. Should the rules require that beneficial owners be updated no later than 60 days after any change in ownership?

Q.10.l. Should the rules provide civil penalties for anyone who submits false or fraudulent beneficial ownership information, does not provide complete or updated information; and/or knowingly discloses subpoena, summons, or other request for beneficial ownership information without authorization?

A.10.e.–l. The Department defers to its colleagues at Treasury to respond to the questions directed to Treasury. As discussed above, the pervasive use of front companies, shell companies, nominees, and other means to conceal the beneficial owners of assets is one of the greatest loopholes in this country's AML regime. We consistently see bad actors using these entities to disguise the ownership of the dirty money derived from criminal conduct. Indeed, FATF's 2016 review of our AML/CTF system highlighted this issue as one of the most critical gaps in the United States. The FATF rated the United States "noncompliant" on the FATF standard covering transparency and beneficial ownership of legal persons, noting the United States' "generally unsatisfactory measures for ensuring that there is adequate, accurate, and updated information" on beneficial ownership, as defined by FATF, that "can be obtained or accessed by competent authorities in a timely manner." The result, FATF said, is that U.S. law enforcement authorities "must often resort to resource-intensive and time-consuming investigative and surveillance techniques."

More effective legal frameworks are accordingly needed to ensure that criminals cannot hide behind nominees, shell corporations, and other legal structures to frustrate law enforcement. When law enforcement is able to obtain information on the identities of the persons who ultimately own or control these legal entities, it can better see the full network of criminal proceeds as bad actors try to bring money into our financial system. With proper law enforcement access to accurate, up-to-date, and detailed beneficial ownership information, the Department could bring more cases, more quickly, with more impact.

The Department looks forward to continued discussions with its interagency partners, Congress, and industry regarding stronger laws that target individuals who seek to mask the ownership of companies, accounts, and sources of funds, as well as proposals to require the collection and maintenance of beneficial ownership information.

Q.11. Author and reporter David Cay Johnston reports in his book, The Making of Donald Trump, that public records show highly suspicious money from Russia is behind Trump's businesses. He alleges that "over the past three decades, at least 13 people with known or alleged links to Russian mobsters or oligarchs have owned, lived in, and even run criminal activities out of Trump Tower and other Trump properties. Many used his apartments and casinos to launder untold millions in dirty money. Some ran a worldwide high-stakes gambling ring out of Trump Tower—in a unit directly below one owned by Trump. Others provided Trump with lucrative branding deals that required no investment on his part. Taken together, the flow of money from Russia provided Trump with a crucial infusion of financing that helped rescue his

empire from ruin, burnish his image, and launch his career in television and politics."

Q.11.a. Please provide a list of convicted criminals who had business dealings with the Trump Corporation?

A.11.a. The Department does not track the information you have requested in the format you have requested.

Q.11.b. Please list the condominiums and their owners that the Federal Government seized from Russian emigres who were convicted of crimes such as money laundering, violence, *etc.*?

A.11.b. The Department does not track the information you have requested in the format you have requested.

Q.11.c. What is the size of Russian mob money laundering in the United States? What do you recommend we do to limit money laundering from international and domestic organized crime syndicates?

A.11.c. As to the first question, the Department does not track the information you have requested in the format you have requested.

As to the second question, the Department will continue to draw on its full complement of law enforcement tools to investigate and prosecute money laundering by all types of actors, including international and domestic crime syndicates. One tool that is vital to this effort is BSA reporting, including SARs and CTRs. Information from BSA reporting not only helps to generate leads and advance investigations already underway, but it also plays a particularly important role in the investigation and prosecution of criminal groups, as this reporting can help law enforcement see the full criminal network. By reviewing information from SARs, CTRs, and other BSA reporting, for example, law enforcement may be able to trace money flowing to different parts of the network—those that generate the illicit proceeds and those used to redistribute them. The Department also welcomes further dialogue with Congress about the tools most helpful to its enforcement efforts.

Q.12. Like many corporate executives, President Donald Trump takes advantage of more corporate-friendly businesses laws. Analysis of his FEC filings finds he registered 659 businesses. Despite defining himself as a New Yorker, only 19 percent of his businesses are chartered in New York. Only 11 percent of his businesses were chartered in Florida where he has a second home. Instead, more than two-thirds of his corporations were chartered in Delaware (48 percent) or Nevada (23 percent). President-elect Donald Trump filed a Federal Election Committee (FEC) filing in July 2016 listing 515 corporations for which he serves on the Board of Directors. Of these, 263 of the corporations begin with "Trump." A number of the other corporations contain some combination of his initials "DT" or "DJT." 2 Quartz. "A List of Everything Donald Trump Runs That Has His Name On It." Looking only at corporations which included "Trump," which did not include another family member (*i.e.,* his father or his children), and which could be reasonably determined to be one of Donald Trump's companies (*i.e.,* excluding initialed companies and companies containing Trumpe, Trumpf, Trumpy, *etc.*), it seems: 315 companies are incorporated in Delaware. Of which, Trump self-reported as a board member of at least 182. The New York online corporate registry does not provide an immediately

obvious status of the companies so we cannot analyze current versus dissolved corporations. One hundred forty-nine companies are incorporated in Nevada. Of which, only 15 are currently active. A few have been formally dissolved; however, the remainder are in a progressively permanent state of revocation for failure to keep up with filings and fees. Of the 15 active corporations, Trump self-reported as a board member of at least 9. One hundred twenty-four companies are incorporated in New York. Of which, Trump self-reported as a board member of at least 60. The New York online corporate registry does not provide an immediately obvious status of the companies so we cannot analyze current versus dissolved corporations. Seventy companies are incorporated in Florida. Of which, 22 are currently listed as active. Of the active corporations, Trump self-reported as a board member of at least 3. Five companies are incorporated in Wyoming; only 1 is active.

Q.12.a. Can you confirm that these figures about President Trump's business locations are accurate?

A.12.a. We are unable to confirm this information.

Q.12.b. Have any of President Trump's current or former businesses been indicted or convicted for money laundering or other financial crimes?

A.12.b. The Department does not track the information you have requested in the format you have requested.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Trends in Bank Secrecy Act/Anti-Money Laundering Enforcement

Jay B. Sykes
Legislative Attorney

January 12, 2018

Congressional Research Service
7-5700
www.crs.gov
<Product Code>

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

This report provides an overview of recent trends in the enforcement of the Bank Secrecy Act (BSA), the principal U.S. anti-money laundering law regulating financial institutions.

The report begins by providing general background information on BSA penalties and enforcement. The report concludes by discussing three recent trends that commentators have observed in BSA enforcement: (1) an increase in the frequency with which BSA enforcement actions involve an assessment of money penalties, and an increase in the size of those penalties, (2) an increased emphasis by regulators on the acceptance of responsibility by institutions entering into settlement agreements for BSA violations, and (3) an increased risk of individual liability for BSA violations.

Contents

Contacts

Background

The BSA is "the primary U.S. anti-money laundering (AML) law" regulating financial institutions.[1] Among other things, the Act and related regulations impose certain reporting and recordkeeping requirements[2] and require certain institutions to establish AML programs that meet specified minimum standards.[3] The BSA and related regulations provide for civil and criminal penalties for violations of their provisions, as well as the forfeiture of assets involved in a violation.[4] The level of BSA penalties varies based on the type of entity charged with a violation, the type of violation, and the defendant's level of intent.[5]

The Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury primarily charged with administering the BSA, has enforcement authority to bring administrative actions for failure to meet BSA requirements.[6] The Office of the Comptroller of the Currency (OCC),[7] the Federal Deposit Insurance Corporation,[8] the Federal Reserve,[9] the Securities and Exchange Commission,[10] the Financial Industry Regulatory Authority,[11] and the National Credit Union Administration[12] also have authority to enforce the BSA's requirements against the institutions they regulate. Moreover, the Department of Justice (DOJ) regularly brings criminal charges for BSA violations.[13]

BSA Enforcement Trends

Increases in Penalty Frequency and Size

Commentators have noted an increase in the frequency with which BSA enforcement actions have involved an assessment by federal regulators of monetary penalties, and an increase in the

[1] *BSA and Related Regulations*, OFFICE OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.treas.gov/topics/compliance-bsa/bsa/bsa-regulations/index-bsa-regulations.html.

[2] *See* 31 U.S.C. §§ 5313-5316; 31 C.F.R. §§ 1010.300-1010.370, 1010.400-1010.440.

[3] *See* 31 U.S.C. § 5318(h); 31 C.F.R. §§ 1010.200-1010.230.

[4] 31 U.S.C. §§ 5321-5322; 31 C.F.R. §§ 1010.820-1010.840 (listing penalties).

[5] *See supra* note 4.

[6] *See* 31 U.S.C. § 310; 31 C.F.R. § 1010.810(a).

[7] *See* 12 U.S.C. § 1818(i)(2); 12 C.F.R. §§ 21.11, 21.21, 163.180.

[8] *See* 12 U.S.C. § 1818(i)(2); 12 C.F.R. § 326.8.

[9] *See* 12 U.S.C. § 1818(i)(2); 12 C.F.R. § 208.63.

[10] *See* 15 U.S.C. § 78u; 17 C.F.R. § 240.17a-8.

[11] *See* 31 C.F.R. § 1023.220.

[12] *See* 12 U.S.C. § 1786; 12 C.F.R. § 748.2.

[13] *See, e.g.*, *Banamex USA Agrees to Forfeit $97 Million in Connection with Bank Secrecy Act Violations*, U.S. DEP'T OF JUSTICE (May 22, 2017), https://www.justice.gov/opa/pr/banamex-usa-agrees-forfeit-97-million-connection-bank-secrecy-act-violations; *Western Union Admits Anti-Money Laundering and Consumer Fraud Violations, Forfeits $586 Million in Settlement with Department of Justice and Federal Trade Commission*, U.S. DEP'T OF JUSTICE (Jan. 19, 2017), https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million; *Commerzbank AG Admits to Sanctions and Bank Secrecy Act Violations, Agrees to Forfeit $563 Million and Pay $79 Million Fine*, U.S. DEP'T OF JUSTICE (Mar. 12, 2015), https://www.justice.gov/opa/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations-agrees-forfeit-563-million-and. *See also* 5 U.S.C. §§ 510, 515-519; 28 C.F.R. § 0.55.

size of those penalties.[14] According to a June 2016 study conducted by National Economic Research Associates, Inc. (NERA), nearly 90% of BSA/AML enforcement actions from 2012 through 2015 involved an assessment of money penalties, compared to less than half of such enforcement actions from 2002 through 2011.[15] NERA also observed that BSA/AML penalties "have grown substantially in both absolute terms and as a proportion of firm capital."[16] Specifically, NERA found that more than 80% of the total money penalties imposed for BSA/AML violations since 2002 have been levied after 2012.[17] Moreover, according to that same report, since October 2009, nearly one-third of BSA/AML penalties have exceeded 10% of a defendant institution's capital.[18] By contrast, no penalty imposed before 2007 exceeded 9% of a defendant institution's capital.[19]

Two recent BSA/AML enforcement actions stand out for their size. In 2012, HSBC Holdings plc and HSBC Bank USA N.A. (together, HSBC) were assessed a $665 million civil money penalty, forfeited roughly $1.2 billion, and entered into a deferred prosecution agreement (DPA) based on, among other things, their failure to maintain an effective AML program and conduct appropriate due diligence on foreign correspondent account holders.[20] The HSBC enforcement action was pursued concurrently by the DOJ, the OCC, the Federal Reserve, and the Department of the Treasury.[21] Pursuant to the DPA, HSBC admitted responsibility for violating the BSA and associated regulations from 2006 to 2010.[22] Specifically, HSBC admitted that during the relevant time period, it "ignored the money laundering risks associated with doing business with certain Mexican customers and failed to implement a BSA/AML program that was adequate to monitor suspicious transactions from Mexico."[23] According to the DPA, as a result of HSBC's failures, at

---

[14] Sharon Brown-Hruska, *Developments in Bank Secrecy Act and Anti-Money Laundering Enforcement and Litigation*, NERA Economic Consulting (June 2016) at 12, http://www.nera.com/content/dam/nera/publications/2016/PUB_Developments_BSA_AML_Lit-06.16.pdf. *See also 2015 Year-End Review of BSA/AML and Sanctions Developments and Their Importance to Financial Institutions*, Sullivan & Cromwell LLP at 2 (Mar. 3, 2016), https://www.sullcrom.com/siteFiles/Publications/SC_Publication_2015_Year_End_Review_of_BSA_AML_3_3_16.pdf (noting that "[i]n 2015, we continued to see record-setting fines . . . against financial institutions for violations of BSA/AML . . . laws.").

[15] Brown-Hruska, *supra* note 14 at 12.

[16] *Id.*

[17] *Id.*

[18] *Id.* at 7.

[19] *Id.*

[20] United States v. HSBC Bank USA, N.A., No. 1:12-cr-00763, 2013 WL 3306161 (E.D.N.Y. July 1, 2013); Statement of Facts, United States v. HSBC Bank USA, N.A., No. 1:12-cr-00763 (E.D.N.Y., filed on Dec. 11, 2012) [hereinafter "Statement of Facts"], https://www.justice.gov/sites/default/files/opa/legacy/2012/12/11/dpa-attachment-a.pdf; *HSBC Holdings Plc. and HSBC Bank N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement*, U.S. Dep't of Justice (Dec. 11, 2012), https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations. A "correspondent account" is an account established by a foreign bank or financial institution "to receive deposits from, or to make payments or other disbursements on behalf of" the foreign bank or financial institution, "or to handle other financial transactions related to" the foreign bank or financial institution. 31 C.F.R. § 1010.605(c)(1). BSA regulations require certain institutions to establish due diligence programs for foreign correspondent accounts that meet specified minimum standards. *Id.* § 1010.610.

[21] *See HSBC Holdings Plc. and HSBC Bank N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement*, *supra* note 20.

[22] Statement of Facts at 3.

[23] *Id.*

least $881 million in drug trafficking proceeds were laundered through HSBC Bank USA without being detected.[24]

In a series of other BSA enforcement actions, a number of federal regulators assessed large penalties against JPMorgan Chase Bank, N.A. (JPMorgan) in January 2014 for its role in the Bernard L. Madoff Ponzi scheme. JPMorgan entered into a DPA with the United States Attorney's Office for the Southern District of New York concerning Madoff-related BSA violations.[25] Pursuant to the DPA, JPMorgan admitted that it violated the BSA by failing to maintain an effective AML compliance program and failing to file suspicious activity reports (SARs) concerning transactions related to the Madoff scheme.[26] JPMorgan further agreed to forfeit $1.7 billion to compensate victims of the Madoff fraud—the largest-ever penalty for a BSA violation.[27] Separately, the OCC and FinCEN assessed civil money penalties of $350 million and $461 million, respectively, against JPMorgan for its Madoff-related BSA violations.[28]

Emphasis on Acceptance of Responsibility

A second recent trend in BSA/AML enforcement is an increased emphasis by regulators on the acceptance of responsibility by institutions charged with BSA violations.[29] In 2013, FinCEN Director Jennifer Shasky Calvery indicated that FinCEN had changed its approach of generally allowing financial institutions charged with BSA violations to enter into settlements "without admitting or denying" the facts alleged in a penalty assessment.[30] Shasky Calvery noted that in FinCEN's most recent enforcement actions, defendant institutions had been required to stipulate to a statement of facts, reflecting the agency's new position that "[a]cceptance of responsibility and acknowledgment of the facts is a critical component of corporate responsibility."[31] Two years

[24] *Id.* As part of the DPA, HSBC also agreed to oversight by a corporate monitor to ensure the effectiveness of its AML reforms. HSBC announced last month that the DOJ agreed to release HSBC from the monitorship after finding that it had made sufficient improvements. *HSBC Holdings plc Expiration of 2012 Deferred Prosecution Agreement*, HSBC (Dec. 11, 2017), http://www.hsbc.com/news-and-insight/media-resources/media-releases/2017/hsbc-holdings-plc-expiration-of-2012-deferred-prosecution-agreement.

[25] *Manhattan U.S. Attorney and FBI Assistant Director-in-Charge Announce Filing of Criminal Charges Against and Deferred Prosecution Agreement With JPMorgan Chase Bank, N.A., In Connection With Bernard L. Madoff's Multi-Billion Dollar Ponzi Scheme*, U.S. DEP'T OF JUSTICE (Jan. 7, 2014), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-filing-criminal.

[26] *Id.*

[27] *Id.*

[28] Consent Order for the Assessment of a Civil Money Penalty, In the Matter of JPMorgan Chase Bank, N.A., JPMorgan Bank and Trust Company, N.A., Chase Bank USA, N.A., AA-EC-13-109, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Jan. 7, 2014), https://www.occ.treas.gov/topics/laws-regulations/enforcement-actions/bank-enforcement-actions/ea-2014-001.pdf; *JPMorgan Admits Violation of the Bank Secrecy Act for Failed Madoff Oversight; Fined $461 Million by FinCEN*, FINANCIAL CRIMES ENFORCEMENT NETWORK (Jan. 7, 2014), https://www.fincen.gov/news/news-releases/jpmorgan-admits-violation-bank-secrecy-act-failed-madoff-oversight-fined-461. Note that FinCEN deemed its penalty satisfied by JPMorgan's payment to the U.S. Attorney's Office for the Southern District of New York. *Id.*

[29] *See* Brown-Hruska, *supra* note 14 at 2-3; *Remarks of Stephanie Brooker, Associate Director of Enforcement, Financial Crimes Enforcement Network (FinCEN)*, 2015 Bank Secrecy Act Conference (June 18, 2015), https://www.fincen.gov/news/speeches/remarks-stephanie-brooker-associate-director-enforcement-financial-crimes-0 [hereinafter "Remarks of Stephanie Brooker"]; *Remarks of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network*, American Bankers Association/American Bar Association Money Laundering Enforcement Conference (Nov. 19, 2013) [hereinafter "Remarks of Jennifer Shasky Calvery"], https://www.fincen.gov/sites/default/files/shared/20131119_ABA_ABA.pdf.

[30] Remarks of Jennifer Shasky Calvery at 4.

[31] *Id.*

later, FinCEN's Director of Enforcement confirmed the agency's changed approach when she indicated that FinCEN operates under a "presumption" that "a settlement of an enforcement action will include an admission to the facts, as well as the violation of law."[32] Along these lines, NERA's 2016 study found that four of the six largest BSA/AML violations charged between 2010 and 2015 "required the [defendant] financial institution to admit the accuracy of government claims and accept responsibility for the actions of its officers, agents, and employees who violated BSA/AML regulations."[33]

Increased Risk of Individual Liability

Finally, commentators have noted an increased risk of individual liability for BSA violations.[34] In December 2014, FinCEN assessed a $1 million civil money penalty against Thomas Haider, the former Chief Compliance Officer of MoneyGram International for willful violations of the BSA's program requirements and failure to timely file SARs concerning fraudulent telemarketing operations and other schemes.[35] FinCEN's enforcement action led to litigation over the application of the BSA to individuals. In January 2016, a federal district court held in *U.S. Department of Treasury v. Haider* that individuals can be liable for violations of the BSA's AML program requirements.[36] In that case, Haider argued that individuals cannot be liable for violations of the BSA's program requirements because the relevant BSA provision provides that "financial institution[s] shall establish anti-money laundering programs,"[37] in contrast to the BSA's provision requiring the filing of SARs, which provides that "any financial institution, *and any director, officer, employee, or agent of any financial institution*, [may be required] to report suspicious transactions relevant to a possible violation of law or regulation."[38] The court rejected this argument, reasoning that because the BSA's general civil penalty provision authorizes the imposition of money penalties against, among other individuals, "officer[s]" of financial institutions,[39] Haider could be held liable for violations of the BSA's AML program requirements.[40] Regulators have recently pursued a number of other BSA enforcement actions against individual compliance officers.[41]

---

[32] Remarks of Stephanie Brooker.

[33] Brown-Hruska, *supra* note 14 at 4.

[34] *Id.* at 3; *2015 Year-End Review of BSA/AML and Sanctions Developments and Their Importance to Financial Institutions*, *supra* note 14 at 7-10.

[35] *FinCEN Assesses $1 Million Penalty and Seeks to Bar Former MoneyGram Executive from Financial Industry*, Financial Crimes Enforcement Network (Dec. 8. 2014), https://www.fincen.gov/news/news-releases/fincen-assesses-1-million-penalty-and-seeks-bar-former-moneygram-executive.

[36] *See* U.S. Dep't of Treasury v. Haider, No. 15-1518, 2016 WL 107940 at *3 (D. Minn. Jan. 8, 2016).

[37] 31 U.S.C. § 5318(h).

[38] *Haider*, 2016 WL 107940 at *2; 31 U.S.C. § 5318(g) (emphasis added).

[39] 31 U.S.C. § 5321(a)(1).

[40] *Haider*, 2016 WL 107940 at *2-3.

[41] *See* Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order, In the Matter of Lia Yaffar-Pena, Release No. 79124, Securities and Exchange Commission (Oct. 19, 2016), https://www.sec.gov/litigation/admin/2016/34-79124.pdf; *FINRA Fines Raymond James $17 Million for Systemic Anti-Money Laundering Compliance Failures, Former AML Compliance Officer Fined and Suspended*, Financial Industry Regulatory Authority (May 18, 2016), http://www.finra.org/newsroom/2016/finra-fines-raymond-james-17-million-systemic-anti-money-laundering-compliance; Consent Order, In the Matter of Charles Sanders, AA-EC-2015-92, Office of the Comptroller of the Currency (Mar. 15, 2016), https://www.occ.gov/static/enforcement-actions/ea2016-038.pdf. While these enforcement actions were not based on violations of the statutory provision at (continued...)

This increased emphasis on individual prosecutions is broadly consistent with the approach outlined by the DOJ in the September 2015 "Yates Memo," which emphasized the importance of individual accountability for corporate wrongdoing.[42] Current Deputy Attorney General Rod Rosenstein has indicated that while he "generally agree[s] with the critique that motivated" the Yates Memo, the memo is currently under review.[43] Accordingly, it remains to be seen whether the DOJ under President Trump will maintain the previous Administration's emphasis on individual responsibility in white-collar enforcement actions and prosecutions.

Author Contact Information

Jay B. Sykes
Legislative Attorney
jsykes@crs.loc.gov, 7-1064

(...continued)

issue in *Haider*, they are consistent with a broader trend of increased risk of individual liability for BSA violations.

[42] Memorandum from Sally Quillian Yates, Deputy Att'y Gen., U.S. Dep't of Justice to All U.S. Att'ys et al., Individual Accountability for Corporate Wrongdoing (Sept. 9, 2015), https://www.justice.gov/archives/dag/file/769036/download.

[43] *Deputy Attorney General Rod Rosenstein Keynote Address on Corporate Enforcement Policy*, NYU Program on Corporate Compliance & Enforcement (Oct. 6, 2017), https://wp.nyu.edu/compliance_enforcement/2017/10/06/nyu-program-on-corporate-compliance-enforcement-keynote-address-october-6-2017/.