S. HRG. 115–405

COMBATING MONEY LAUNDERING AND OTHER FORMS OF ILLICIT FINANCE: HOW CRIMINAL ORGANIZATIONS LAUNDER MONEY AND INNOVATIVE TECHNIQUES FOR FIGHTING THEM

HEARING

BEFORE THE

SUBCOMMITTEE ON
NATIONAL SECURITY AND INTERNATIONAL TRADE
AND FINANCE

OF THE

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

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

ON

MODERNIZING THE UNITED STATES' ANTI-MONEY-LAUNDERING REGIME, EXPLORING HOW CRIMINAL ORGANIZATIONS LAUNDER MONEY AND THE INNOVATIVE TECHNIQUES THAT ARE AVAILABLE TO FIGHT THEM

JUNE 20, 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

33–424 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*

SIERRA ROBINSON, *Professional Staff Member*

COLIN MCGINNIS, *Democratic Policy Director*

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

SUBCOMMITTEE ON NATIONAL SECURITY AND INTERNATIONAL TRADE AND FINANCE

BEN SASSE, Nebraska, *Chairman*
JOE DONNELLY, Indiana, *Ranking Democratic Member*

BOB CORKER, Tennessee	MARK R. WARNER, Virginia
TOM COTTON, Arizona	HEIDI HEITKAMP, North Dakota
MIKE ROUNDS, South Dakota	BRIAN SCHATZ, Hawaii
DAVID PERDUE, Georgia	

AMMON SIMON, *Subcommittee Staff Director*
NICK CATINO, *Democratic Subcommittee Staff Director*

C O N T E N T S

WEDNESDAY, JUNE 20, 2018

WITNESSES

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

COMBATING MONEY LAUNDERING AND OTHER FORMS OF ILLICIT FINANCE: HOW CRIMINAL ORGANIZATIONS LAUNDER MONEY AND INNOVATIVE TECHNIQUES FOR FIGHTING THEM

WEDNESDAY, JUNE 20, 2018

U.S. SENATE, SUBCOMMITTEE ON NATIONAL SECURITY AND INTERNATIONAL TRADE AND FINANCE, COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Subcommittee met at 2:35 p.m., in room SD–538, Dirksen Senate Office Building, Hon. Ben Sasse, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF CHAIRMAN BEN SASSE

Senator SASSE. This hearing will come to order.

This is the third Banking Committee hearing on modernizing our Nation's outdated anti-money-laundering regime. Today we will explore how criminal organizations launder money and the innovative techniques that are available to fight them.

I am pleased that Chairman Crapo is committed to examining this topic because modernizing our anti-money-laundering regime, AMLs, for the purposes of this hearing, is vital to financial institutions in Nebraska and Indiana and across the country. These vital institutions must spend millions of dollars on sometimes unnecessary AML compliance efforts, dollars that should be directed toward either more effective anti-money-laundering activities or toward lending to local businesses and farmers in States like Nebraska.

I have heard stories of financial institutions at home who must file SARs or CTRs on fireworks sales, county fairs, rodeos, softball leagues, and even churches running their capital campaigns. Another financial institution must perform enhanced due diligence on their local Rotary Club. We can and must do better than this. We all want to stop money laundering, but we should do it in the most effective and efficient way as possible.

This discussion today will cover how to improve cooperation and coordination with law enforcement officials and how to incentivize and enable financial institutions to adopt innovative AML techniques. This includes leveraging artificial intelligence and machine learning while still preserving strict AML rules targeting criminal activity.

We will be hearing from Dennis Lormel, president and CEO of DML Associates and the former Chief of the FBI Financial Crimes Program. Thank you for being here. Dennis will talk about how criminal organizations launder money and avoid detection by financial institutions and how financial institutions are fighting back and how they should more effectively fight back.

We will also be hearing from Tracy Woodrow, senior vice president, BSA officer, and anti-money-laundering director for M&T Bank. Tracy will discuss the successes of financial institutions in targeting criminal organizations and the barriers that financial institutions face when trying to fight these criminal organizations.

Finally, we will hear from Chip Poncy, the president and cofounder of the Financial Integrity Network. Chip is stuck in traffic in a protest in DC right now but should be here in the next 15 to 20 minutes. He will be discussing how criminal organizations launder money and avoid detection by financial institutions and other major areas of crime that involve money laundering.

Criminal organizations are constantly devising new ways to launder money because they have monetary incentives to do so. If financial institutions have any chance of stopping them, the AML regimes must also be constantly innovating. We do not have enough of that innovation right now. These innovations do exist, and we will be hearing about some of the most cutting-edge approaches to doing that today, including how financial institutions can identify potential human traffickers by looking at patterns in their financial transactions. But financial institutions cannot and will not effectively adopt these new innovations without more incentives to do so.

I believe our current AML system falls short in many regards. Encouraging AML innovation includes evaluating our fragmented system of regulatory compliance and its possible negative impact on innovation. We should also be considering how to better evaluate financial institutions by focusing more on tangible outcomes rather than merely process measures.

As it happens, regulators can begin to move away from simply measuring compliance with process-heavy risk management requirements such as filling out the SARs. What is measured ultimately improves. So if we measure mostly compliance by SAR filings, financial institutions will just file more SARs. But if we move toward measuring results, that is, actually identifying and discovering the hidden resources funding human traffickers and drug cartels, financial institutions may be able to help identify more potential criminals. Suspicious activity reports will always be a vital part of our financial system, but producing them is not our main goal. Stopping crime is.

Improving the system requires creating better feedback loops between law enforcement and bank regulators. They may also involve encouraging the use of no-action letters. At the least, we should be giving financial institutions more incentives and more flexibility to design their own AML systems without fearing regulatory liability that could spring from adopting more innovative and more effective AML techniques.

Finally, more information sharing, both with FinCEN and other financial institutions, could be very useful for law enforcement

purposes. But this must be done with the utmost attention to privacy concerns, particularly in light of the recent cyber breaches we have seen at the SEC, at Equifax, and at retailers.

Thank you again to the three of you for appearing in front of this Committee, and I thank Senator Donnelly for agreeing to work on this hearing with me. And I would like to hear what Senator Donnelly has to say.

STATEMENT OF SENATOR JOE DONNELLY

Senator DONNELLY. Thank you, Mr. Chairman, for holding today's hearing, and thank you to our distinguished witnesses for appearing before the Subcommittee.

Today's hearing will explore how criminal organizations launder money and avoid detection by financial institutions. We will also discuss how to improve cooperation and coordination between law enforcement and financial institutions and, most importantly, ensure that our policies help us better identify illicit finance and catch as many bad guys as possible.

The Bank Secrecy Act was enacted nearly 50 years ago to enlist the financial services industry to help detect and prevent money laundering and fraud. Since that time, the BSA has become the cornerstone of U.S. anti-money-laundering policy and has expanded numerous times.

The goal of money laundering is often to disguise the illegal origins of criminal proceeds. The types of criminal activities furthered by money laundering include human trafficking, drug trafficking, arms trafficking, and financial fraud.

Without an effective AML regime, criminal organizations have an easier time moving and accessing financing, which furthers their criminal activities. For example, money laundering by drug traffickers like the Sinaloa cartel in Mexico has a direct connection to the opioid crisis in my home State of Indiana, where nearly 800 people died of opioid-related overdose deaths in 2016.

The United States is undoubtedly committed to combating illicit finance with robust AML laws and policies, but notable gaps and vulnerabilities remain. Several reports have concluded that the United States is among the easiest countries to create an anonymous shell company which could allow persons to legally open bank accounts and buy property. As a result, criminal networks, corrupt dictators, and even terrorists can move money through the United States as a legal business entity.

Recent rules from Treasury to ensure banks know their customers will help, but criminals have an incentive to lie and can hide behind a corporate veil. Additionally, even though financial institutions are on the front line of identifying and preventing money laundering, they receive very little feedback from law enforcement on the millions of suspicious activity reports filed each year. If financial institutions have a better idea of what they should be looking for, we can improve the efficiency and effectiveness of our BSA/AML system to more accurately identify suspicious activity.

It is imperative we bolster cooperation and coordination between financial institutions and law enforcement in order to increase the hit rate of BSA reporting. That is how we can catch more bad guys.

There are many tough questions for us to consider today. I look forward to hearing from this panel.

Thank you, Mr. Chairman.

Senator SASSE. Thank you, Senator Donnelly.

First, we will hear from Dennis Lormel, the former Chief of the FBI Financial Crimes Program and the current CEO of DML Associates. Mr. Lormel, thank you.

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

Mr. LORMEL. Thank you, Mr. Chairman and Mr. Donnelly. Thank you guys for holding this hearing. I think it is really important, and I agree with the statements that you made coming into this that there is a lot we can discuss.

I would like to clarify one thing, if I may. When you first introduced us, you talked about that I was going to talk about money laundering and how criminals launder money. I would just like you to know, sir, that I do not represent criminals when we launder money. I work with the financial institutions and certainly with the Government to a great degree.

Senator SASSE. Thank you for clarifying that. We had Bureau agents waiting outside the door.

[Laughter.]

Senator DONNELLY. The Chairman and I were having a long discussion about that.

Mr. LORMEL. No, it is funny, sir, because sometimes when we get into it, when I speak at conferences and things, that comes up. People ask me, "So do you actually launder money?" And I say, "No. I work with the financial institutions."

The lightness aside, this is a serious topic, so I certainly appreciate the fact that you are holding this hearing. I think there is a lot of discussion and a lot of healthy discussion that needs to come.

I have been involved in this for 45 years. I spent 31 in the Government, 28 with the FBI, and for the last 14 I have worked in the financial services industry as a consultant with a number of institutions on a lot of these issues. And I think I have developed a very unique perspective in that I understand the law enforcement side and I understand the benefits and burdens side that banks have to deal with on an ongoing basis in terms of regulatory compliance. So I look forward to touching on that.

You said it. Make no mistake about it. This is very serious. The BSA and BSA information is really vital to law enforcement, and they do a good job with it.

Terrorist organizations, criminals, criminal organizations, and bad actors rely on the financial system to access money, and the one commonality they have, even though a lot of the activity we are going to talk about and the different criminal activity you talked about—the drug dealers, the human smugglers, the human traffickers, trade-based money laundering, the real estate issues—Senator, you mentioned the opioids. There are so many different ways that that money can move, and so it is important to put into context who we are dealing with. We are dealing with individuals, we are dealing with groups of individuals. We are dealing with

organizations, domestic and international, transnational criminal organizations. You are dealing with homegrown violent extremists, and you are dealing with terrorist organizations. So that landscape is so robust.

In my written statement that I submitted for the record, on page 3, I have a diagram, and that is from a PowerPoint presentation that I have done, and I certainly welcome to share that PowerPoint with you. But, in any event, if you look at the money-laundering cycle, when you look at all of these different organizations, the one thing they have in common is they have to launder money. And I believe that in most of these predicate offenses, what you are going to find is that there is a good deal of fraud and money laundering. So if you listed all of the predicate offenses, everything we talked about, and put fraud on the top and put money laundering on the bottom, I think that represents kind of a sandwich, and the fraud and the money laundering represent the bread, the gourmet bread that would be on that sandwich. And for any successful organization, they have got to be able to use fraud; they have got to launder the money; and they do it through a lot of means.

So when you look at that diagram that I have, every organization, regardless of what they are doing, they are going to raise, move, store, and spend. And in some instances, they are going to move and store and continue that cycle more and more, and that makes it more challenging for law enforcement because it seemingly legitimizes the money.

So if you look at money laundering, money laundering is a three-step process: placement, layering, and integration. So between the raise and move is the placement. The integration comes in between the next two steps, the move and spend. And then the integration—I am sorry. Layering was the next step. And then the integration is that last step. And so all organizations, regardless of how dissimilar they are, are going to have that type of pattern of activity in how they are going to launder money.

One thing I want to highlight here, because I know we have limited time in the statements and we will get into more discussion, but the problem of human trafficking. I think the industry, banks have done a fabulous job in identifying typologies. I want to point out that the Polaris Foundation published a book last year, published a study last year with 25 specific typologies on human trafficking. I think that is a terrific study.

One of the things I want to highlight, when we talk about the—if I may, I have run a little long, if you do not mind, sir.

Senator SASSE. Continue.

Mr. LORMEL. One of the things that I think is important, because you both cited it in your testimony, is making SARs more efficient. And one of the ways we do that is through what I call "targeted monitoring." And if you look at human trafficking, there have been tremendous initiatives in targeted monitoring.

Back in 2010, JPMorgan Chase with Homeland Security Investigations, they had a targeted monitoring project where analysts from the banks met with analysts from Homeland Security. They developed typologies and what Homeland Security was seeing in terms of patterns of activity, and based on that, over the baseline transaction monitoring that the banks have, these teams of banks,

they basically put together special typologies, and from those typologies they had a terrific hit rate in terms of suspicious activity reporting.

Just now, in January during the Super Bowl or in the run-up to the Super Bowl, they replicated that, this time with a U.S. bank, and that was a terrific case study. And just like that, I think the FBI, the Financial Crimes Section and the Terrorist Financing Operations Section each have ongoing working groups. Unfortunately, the capacity to bring in more banks is not there, but with the groups that they are working with, the FBI is providing good feedback and good information for them to develop the reportable SARs that are so valuable.

So on that note, thank you, sir, for letting me run a little long, and, Chip, I have been dancing until you got here, buddy.

[Laughter.]

Senator Sasse. We are going to go to Ms. Woodrow now, but, Mr. Poncy, thank you for being here and glad you made it through the protests.

Mr. PONCY. Thank you, Chairman.

Senator SASSE. Next up, Tracy Woodrow is senior vice president and BSA officer and the anti-money-laundering director at M&T Bank. Thank you for being here.

STATEMENT OF TRACY S. WOODROW, SENIOR VICE PRESIDENT AND BANK SECRECY ACT/ANTI-MONEY-LAUNDERING DIRECTOR, M&T BANK CORPORATION

Ms. WOODROW. Good afternoon, and thank you for having me. Chairman Sasse, Ranking Member Donnelly, and Members of the Subcommittee, thank you for holding today's hearing to discuss the AML regime.

Since 2013, I have overseen M&T Bank's AML/counterterrorist financing and sanctions compliance efforts. I also chair a working group at The Clearing House Association that is analyzing the resources that banks devote to these efforts.

At M&T I lead a team of over 300 professionals who are dedicated to the detection and deterrence of money laundering and terrorist financing, while ensuring that our customers can conduct transactions in a safe, secure, and private manner. We use a variety of tools in this effort and are beginning to adapt new technologies to assist us with it.

For example, we are using flexible data analytics to understand emerging risks and suspicious activity patterns. We are also working directly with law enforcement to identify red flags that may indicate suspicious activity and have accomplished a great deal with this collaboration.

Finally, we are exploring the use of automation, artificial intelligence, and shared utilities across financial institutions to assist us in better assessing the huge amounts of data and identifying unusual financial transactions.

Criminal organizations move money through the financial system in many ways, including the use of cash, ACH, wires, investments, and trade finance, as well as through emerging technologies such as virtual currency and person-to-person applications. They use shell companies to hide their identities or to create the false

impression of legitimate business activity. And they use front companies and money mules to hide the real people behind their transactions. With so many varied and ever-changing techniques to move illicit funds, it is critical that we never become complacent or satisfied with yesterday's methods for identifying suspicious activity.

With this in mind, I will highlight four particular areas for potential reform.

First, the Treasury Department should establish priorities for the AML regime, which could in turn form the basis for financial institution supervision and examination. In turn, BSA reporting requirements should be rationalized to allow institutions to focus their resources on that which is most useful to law enforcement, as required by the BSA.

Priorities should be based upon a data-driven review of the SAR and CTR submissions to determine what information is truly useful and whether that information could be provided to law enforcement in a more modern and streamlined fashion.

It is difficult for financial institutions to know if their SAR and CTR filings are useful to law enforcement. Based upon a recent survey by The Clearing House members, a median of 4 percent of SARs and less than one-half percent of CTRs result in any law enforcement contact after the filings. These numbers indicate that there may be a disconnect between how financial institutions are deploying their resources and law enforcement's priorities.

Second, greater information sharing between law enforcement and financial institutions should be encouraged. Law enforcement has access to intelligence from many sources which can help financial institutions to provide better leads. For example, financial institutions can use such information as IP or Internet addresses, geographic locations and addresses, and information about suspected shell companies to develop targeted leads to identify potential suspicious activity.

I have personally witnessed the improved speed, efficiency, and investigative results that can be achieved when banks work cooperatively with law enforcement. I think this should be the norm, not an anecdotal success story.

Third, institutions should have the flexibility to explore innovative technological solutions to AML compliance, either individually or in concert with their peers. Illicit finance often moves between multiple financial institutions as criminal actors work to complicate and conceal their money trail. Therefore, financial institutions should be allowed to safely and securely share additional data with each other for the purpose of detecting suspicious activity.

Finally, shell companies and front companies are often used to conceal the real actors behind illicit transactions. I support efforts to establish a nationwide framework for the collection of beneficial ownership information by a trusted Government body and to make that data available to law enforcement and qualified financial institutions.

In conclusion, financial institutions are on the front lines of the battle to keep money launderers and terrorist financers from using the U.S. financial system to inflict harm in our communities, and we are committed to this mission. I applaud the Subcommittee's

interest in modernizing the regulatory regime to improve the effectiveness of the work we do as AML professionals.

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

Senator SASSE. Thank you, Ms. Woodrow.

Chip Poncy is the president and co-founder of the Financial Integrity Network. Thank you for being here. You have 5 minutes.

STATEMENT OF CHIP PONCY, PRESIDENT AND CO-FOUNDER, FINANCIAL INTEGRITY NETWORK, AND SENIOR ADVISOR, CENTER ON SANCTIONS AND ILLICIT FINANCE

Mr. PONCY. Chairman Sasse, thanks so much, and I apologize to everyone for being late.

Chairman Sasse, Ranking Member Donnelly, thank you for having me here and inviting me to testify. This hearing comes at an important time. The United States has one of the most effective AML/CFT regimes in the world. However, criminal organizations and others continue to exploit vulnerabilities in our financial system and in our anti-money-laundering regime.

Such illicit financial activity increasingly threatens our national security, the integrity of the financial system, and confidence in vulnerable global markets. Our efforts to combat these threats have struggled to keep pace with three interrelated developments.

The first of these is a significant expansion of money-laundering predicates and corresponding AML responsibilities. Our AML efforts now encompass practically all forms of serious crime, including various types of fraud, drug trafficking, corruption, terrorist financing, sanctions evasion, and the proliferation of weapons of mass destruction.

This expansion of money laundering has naturally led to the corresponding expansion of our broader AML efforts. We now have a comprehensive AML/CFT regime that includes and relies upon a complex web of key stakeholders, including Federal, State, and local authorities, the private sector, and international counterparts.

Across governments, here and abroad, this includes law enforcement, regulatory authorities, national security, intelligence, and policymaking communities.

Across the private sector, this includes not only banks but an increasing range of nonbanking financial institutions, financial service providers, and certain other gatekeepers to an increasingly complex financial system. This complexity requires clear AML/CFT governance that Congress can help direct.

The second key development challenging our AML/CFT regime is the constantly evolving nature of the financial system. Particularly over the past generation, our system has become increasingly complex, sophisticated, and intermediated. Such heightened complexity and globalization have enabled greater access to our financial system for illicit actors.

The third development challenging our AML efforts is the increasing reliance on our AML/CFT regime to advance an expanding set of national security interests. The financial transparency that we achieve through sound AML implementation is increasingly important. We rely on this transparency to apply sanctions and targeted financial measures, financial pressure campaigns against

rogue actors. This is true with respect to criminal organizations, but also terrorist groups, corrupt elites, and hostile states.

These developments present opportunities and challenges. The challenges are clear. As my written testimony explains, criminals and other illicit actors exploit the complexities and efficiencies of the globalized financial system in a variety of ways. Money launderers place, layer, and integrate criminal proceeds through cash-intensive businesses, formal and informal payments systems, capital markets, real estate, digital currencies, and virtually all forms of financial products and services.

Terrorist groups continue to exploit our financial system to raise, move, and use funds in support of various terrorist-related activity. Corrupt elites launder stolen assets through sovereign wealth funds, private banking accounts, and other services. Weapons proliferators mask illicit trade and payments through transshipment and front companies.

Understanding the details of any particular scheme requires substantial subject matter expertise, expertise across various types of financial crime, as well as across different illicit groups and networks and the regions in which they operate. This is a substantial investment.

However, virtually all forms of illicit finance seek anonymity, obfuscation, and appearances of legitimacy to escape detection. Anonymous companies and unregulated or undersupervised parts of the financial system continue to undermine our best efforts. These developments and well-established vulnerabilities should guide efforts to strengthen our AML/CFT regime. AML reform should close critical gaps and strengthen our AML/CFT regime, including through the following actions:

First, end the creation of anonymous companies in the United States.

Second, strengthen oversight and supervision of vulnerable and unregulated financial sectors.

Third, enhance the targeting of illicit financing networks.

Fourth, clarify expanded information sharing between and among private sector financial institutions and Government authorities.

And, fifth, encourage innovative approaches and the application of new technologies to buildupon our current foundation.

My written testimony lays out more detailed recommendations that Congress should consider to enact these types of reforms. I would be happy to discuss these or any questions you may have.

Thank you again for your time and consideration. Apologies again for being late.

Senator SASSE. Thank you. Thank you to each of you for your testimony and for being here.

Mr. Lormel, let us begin with you. Could you give some specific examples of the way an organization like, say, MS–13 specifically tries to avoid detection in the financial system?

Mr. LORMEL. Thank you, Senator. Groups like MS–13, so you look at the group itself, and they operate—I would look at them as a transnational group because they are certainly down in South America, and there is a presence here in the United States that is pretty big. So, traditionally, the gangs like MS–13 are not as

organized as some of the more traditional transnational criminal groups. But, nonetheless, as I pointed out, they are going to have to use the system in certain ways.

So one of the things that they do is they control a corridor or a channel, and a lot of illicit goods, drugs, human trafficking is going to come through that corridor up through Mexico into the United States. And so that is one of the things they will do. And what they will look to do then is they will set up either front companies or they have to get into the financial system. A group like that I would assume is also going to be heavily involved in the informal system and use hawalas or illegal money remittance. I think the illegal money remittance operation is one of the biggest problems we have in the United States in terms of not identifying who the illegal money remitters are. So I think there is going to be a lot of cash smuggling, bulk cash smuggling through those chains. But as these groups like MS–13 are maturing, they are going to have to have business fronts, and they are going to have to have access through the banks, and they are going to set up some type of front or operation so that they can avoid detection. That is the key.

Again, following my flow chart, they are going to follow the pattern like that to get money in. And so as they get more sophisticated, they are going to have a CFO, and that CFO is going to be the one who is going to have that type of knowledge and ability. And make no mistake about it. As dangerous as they are on the street, they are going to have the capability and they are going to build an infrastructure that is going to make them that much more challenging to deal with.

Senator SASSE. So your CFO point is almost exactly where I was going to go. I was going to sort of ask you if this is a fair hypothesis about how to typologize this. There are individual bad actors that meet the threshold of being cross-border money launderers. There are large organizations that have a centralized structure. And there are large organizations that have a decentralized structure, I would assume?

Mr. LORMEL. Yes.

Senator SASSE. And you are saying that the accounting inside an organization like MS–13 is pretty decentralized, but for your three steps, I guess after placement, from layering to integration, you just presume that an organization like that as it becomes more complicated, it has integration that will have sophisticated accounting. I am curious about how far-thinking the planning is about how you do that integration.

Mr. LORMEL. I am not sure I follow. How far——

Senator SASSE. You said they are going to have a CFO.

Mr. LORMEL. Right.

Senator SASSE. Talk us through what the step is right before that and who the planner deciders are that you would want sophisticated accounting versus decentralized money that flows through the middle.

Mr. LORMEL. So what you are going to have—and I think a good example of this, there was a drug gang in San Juan, the Menores gang or something to that effect, and virtually they had job descriptions, and MS–13 is going to have the same thing. So your street people are going to have their job descriptions, you know, whether

they are drug runners, whether they are dealing with traditional organized crime, whatever that is going to be, and they will be compartmentalized from people in the more hierarchical sense of the organization.

Now, one of the challenges you are going to have with a group like MS–13 is how independent and decentralized the different cells are going to be around the country and then when you go internationally. But at some point there is going to be more of a structured business. They will have a business model.

I wrote a paper a few years back on the business model for a terrorist organization, and so I would look at that same thing, that same type of manual, and basically what is it they aspire to be and what kind of financing is it going to take to get to that aspirational level, and then how are they going to infiltrate the system to do that? And so that is important. That is, again, what they are going to have and what they are going to be doing, and so at some point that CFO or the C-suite, so to speak, are going to be—they are going to have a more global macro picture; whereas, the different groups may have kind of a more limited micro picture.

Senator SASSE. Thank you. Do the other two of you want to add anything on specific techniques that you see?

Ms. WOODROW. Thanks. I think whatever the organization is that is trying to move the money, they are all moving it in similar ways, using similar techniques. The idea is to hide what you are doing, make it look as legitimate as possible.

There was a recent indictment in the Southern District of Florida, and I thought it was an interesting case study in this where you had probably multiple illicit actors outside the United States based in Nigeria. They were committing frauds and schemes against American persons, and when those American persons would pay them, they needed to move their money back.

So they used a complicated web of money mules and front companies in order to conduct transactions that looked, absent any other information, like legitimate transactions. So you might have a cash-intensive business that is receiving—that is depositing cash. If your business normally accepts cash, that could look routine and usual. They also had individuals that they had hired, probably through a work-at-home scheme, where they would solicit persons with clean records to use those persons to access their accounts, then move the money through that network to outside of the United States banks, generally in more friendly countries that have a high level of ordinary trade with the United States, and then finally to the illicit actors behind the whole scheme.

And you see that pattern of obfuscation, so use of people who do not have records, who do not have negative news associated with them, in order to bring the money into the system and then move it around between what looks like legitimate business activity, but it is actually a front.

Senator SASSE. Thank you.

Mr. Poncy?

Mr. PONCY. Thank you, Chairman. I completely agree with what Dennis and Tracy have said, and I am honored to be here next to them. They are real experts in the field.

I would just add that the technique really depends on the type of predicate offense we are talking about. The cash-based predicates, like drug trafficking, the key challenge is how do you get that cash into the system. So you are going to have placement opportunities to disrupt, placement needs that invite opportunities to disrupt, and we have controls for that that we may not be fully exploiting. When you look at structuring activities, that continues to, to my understanding, light up the BSA database, and I am not sure that we have got enough resources to hit all that. So there are techniques that are tried and true and that will always be there around cash-based predicates.

When you get to other forms of money laundering, particularly with fraud, the money is already in the system, so you are looking at wires, and you can say, well, it is third-party wires or it is trade-based money laundering. The problem is the wire rooms in our banks are—the straight-through processing of the volumes of this are such that it is very difficult without advance intelligence to say this is the wire I am interested in.

And so one of the ideas that we have been kicking around internally is to think through, much as we have expanded in trade finance the need for banks and financial institutions to look at trade finance documentation so that there is a better understanding of the related parties and the markets and the jurisdictions and actors that may be involved. We do not do that when we talk about wire rooms and straight-through processing because it would completely shut down the system.

Are there messaging formats that would be friendlier in allowing us to run screens and continue to have straight-through processing? Those sorts of techniques are innovative, and trying to adapt to the reality that as our money-laundering predicates have expanded past cash, we have to figure out a better way to preserve straight-through processing, at the same time get intelligence out of those systems that allow us to direct our resources.

The final thing I would say is that no matter what the organization is, the prevalence and sophisticated money laundering and illicit finance of anonymous companies, gatekeepers, front or straw persons, correspondence, and then ultimately back to working into a target market like the United States is prevalent. And so you have U.S. financial institutions that are increasingly removed from the source of the risk. If it is placed in a foreign market through a nonbank financial institution, then it is corresponding into a local bank that then corresponds with a dollar clearer in New York. The New York institution has a very difficult time trying to understand that pathway. And in trying to understand that, without targeted intelligence, they are going to shut down the system to try to look at all this. That intermediation is a killer.

Senator SASSE. Senator Donnelly.

Mr. LORMEL. Senator, if I may just one second, sir, going back, if I was investigating and were looking at MS–13, one of the things I would be looking at from an enterprise-wide standpoint, having an enterprise-wide investigation, would be to see if they were using funnel accounts. Basically if they are operating in different regions, do they have some type of funnel account operation where money is funneled through one account to a central account? And that is

what I would be looking for, and that is what I would be looking for in suspicious activity reports and, to a degree—well, CTRs would not have that, but certainly I would be looking for patterns on all of those things. But the funnel accounts would be my starting point.

Senator SASSE. Thank you.

Senator Donnelly.

Senator DONNELLY. Thank you, Mr. Chairman.

Although the United States has a strong anti-money-laundering framework, authorities have one hand tied behind their back due to lax business ownership transparency. Many reports have concluded that the United States is among the easiest countries to create an anonymous shell company. As a result, criminal networks, corrupt dictators, and even terrorists have been able to move money through the United States as a legal business entity. Law enforcement officials often have great difficulty identifying the beneficial owner. This is deeply alarming, especially since illicit proceeds from crime total as much as $300 billion or more in this country, or 2 percent of the economy, according to the DEA and other estimates. If we cannot identify the bad guys, that means more drug trafficking, human trafficking, arms trafficking, and fraud.

Mr. Lormel and Mr. Poncy, could you please describe how criminals exploit these shell companies and the lax corporate transparency rules to evade AML detection?

Mr. LORMEL. Thank you, Senator, and I am glad you brought that point up, because when I finished, I am remiss because I did not state that I wanted to mention there were four areas that we needed to look at, and beneficial ownership is one of them.

The other thing is I am concerned about, as an aside, raising the thresholds on SARs and CTRs. I think that would be problematic. I think we need to have better feedback mechanisms, and I think we need to look at the regulatory requirements versus regulatory expectations.

But in my written statement, sir, I did give a case study or a case example of the Alavi Foundation. Our sanctions have done a really good job against Iran, and so Iran has to get into the financial services industry. They have to get into that, and they use shell companies. And they have been very good at that, and a classic case is they owned a building in New York on Fifth Avenue through a bunch of front companies, and it took the Government quite a long time to work around that.

I know when I was in law enforcement, when you came into that shell company environment and trying to work through who is really pulling the strings behind that shell, and I would think—to Senator Sasse's question about MS–13, I would be looking for shell companies there. But that Alavi Foundation with Iran is a classic example of the use of shell companies by a foreign power, and certainly, you know, they are doing that quite a bit. And just, again, it demonstrates the success of our sanctions.

Senator DONNELLY. Mr. Poncy?

Mr. PONCY. Thank you, Senator Donnelly. I could not agree more. I think it is becoming increasingly clear that the biggest threat to our anti-money-laundering and counter-illicit financing

efforts is the threat posed by anonymous companies. Several of those are created here, and there is plenty of testimony and evidence to support that illicit actors continually use U.S. anonymous companies or companies created in the United States in particular because of the perception of legitimacy.

I can recall when I was at Treasury and certainly in my private sector experience, where we see money-laundering-related accounts pretty far away from the United States, held in the names of U.S. companies, that provides a veneer of legitimacy and behind which there is no accountable person to hold responsible for the activities of the company.

The comments that I would have—and these are elaborated on in my testimony—are first that anonymous companies are used across every possible form of fraud in financial crime. That is clear. Whether you are talking sanctions that are jurisdictional against Iran, that are targeted against drug-trafficking organizations, or you are talking about various predicate offenses to money laundering, anonymous companies are used throughout. That is the first point.

The second point is that what we see in our cases, and whether in the Government or what we see in the private sector, is a fraction of what we do not see, and this is what is so frustrating. I think the notion that, you know, that we see, to your point, a fraction of the 2 percent or 5 percent or whatever the estimate is of illicit finance that people can peg, what we are looking at may not even be statistically relevant, which raises the question of where are all of these bad actors and these illicit assets? And if we know out of the evidence that we have that we cannot track and trace anything through an anonymous company, it is pretty clear that getting transparency over that technique or mechanism is essential to turning the lights on, and particularly when we have gone out to financial institutions appropriately and said, "You need to look through the legal entity accounts that you open and make sure that you understand the beneficial owners."

It is very hard for them to do that when the very authorities that are telling them to do that are creating the anonymous vehicles that present the problem.

Senator DONNELLY. Let me ask one more question this round, and it would go to something that Mr. Lormel mentioned. The Iran-owned Manhattan high-rise is not the only example of high-priced real estate being used for money laundering. According to recent reports in the media and geographic targeting orders from Treasury, it appears foreign money is frequently used in all-cash purchases of expensive properties.

What are the AML risks of huge cash transactions in real estate? And how can we better identify those transactions? Ms. Woodrow, if you would go first, and then around the horn, so to speak.

Ms. WOODROW. Certainly. Thank you. Well, real estate, particularly in very high value markets, such as, for example, Miami and New York, is an advantageous area to invest in, both from an ordinary investor standpoint as well as from a money launderer's standpoint. You have the ability as a money launderer to invest a large sum of money in a single asset. That asset can grow in value and also can be transferred.

Particularly in areas where there is a high velocity of turnover, you can also kind of get wrapped up in the rest of the legitimate activity and be less conspicuous.

Real estate is often also purchased in the names of LLCs or trusts for very ordinary purposes, and money launderers are able to use those same tools, those LLCs and those trusts, to purchase the real estate and hide who they really are behind it. This is where the gatekeepers come in.

So, ordinarily, money launderers are not going to try to go to a bank and get a mortgage to pay for a $1 million high-rise apartment because we are going to do due diligence, KYC, as well as credit underwriting. They are going to try to buy the property in cash or through a check or a wire. Those proceeds tend to go to gatekeepers, such as real estate agents, attorneys, title companies to hold the money while the sale is pending.

That is the place where a bank may see the transaction. The difficulty is those gatekeepers have escrow accounts where they are holding all kinds of money for all kinds of different real estate transactions. But that is where we might be able to detect something is happening. Otherwise, the transaction is going on without the use of a financial institution.

Senator DONNELLY. Maybe we can get back to this later. Thank you, Mr. Chairman.

Senator SASSE. Senator Heitkamp.

Senator HEITKAMP. Thank you, Mr. Chairman.

One of the concerns that I have, obviously, is economies of scale. If you are a large financial institution, you can have a fairly robust plan to protect our financial system from nefarious financial transactions. But if you are a small bank, if you are a regional or a small bank, it just gets tougher and tougher, and these regulations are among their top concerns.

And so I guess I want to maybe get some advice from all of you on how we can better resource our regional banks and our community banks and our credit unions to accomplish the purposes that we know are essential. And so we will start with you, Mr. Lormel.

Mr. LORMEL. Well, that is certainly a challenge. One of the things that I am a big advocate for are working groups and information sharing and partnerships. So to the extent we can improve the information sharing, especially down at that level, so what you have, Senator, are going to be kind of working groups. There are national working groups, and certainly the smaller banks are less inclined to be involved in those. So it is at the grassroots level. It is at whatever jurisdiction they are in and in their cities and things, is to work with—to get involved with the working groups for law enforcement, because you have to leverage—as you pointed out, they have limited resources. So how do you leverage those resources? And for me that is partnering and getting into a better sense of sharing information to the extent that you can.

But I am also a big proponent—and I have written about this in a couple of articles—of kind of like a SWAT approach, in a sense. Even in a small institution where you have limited resources, it is taking the extra step, and if you make the analogy of a law enforcement SWAT team, for instance, they have primary responsibilities and SWAT is their secondary or collateral responsibility. So

when you go back into the institution here, you take one person or a team of people to the extent that you can build it and have them specially trained.

One of the things that I am really impressed with with bankers is the commitment, and you talk to Tracy and their staff, as to how dedicated they are to what they are doing. So it is to be really familiar with a lot of these issues, and issues particularly that would hit their bank and to be able to, again, leverage your resources and capabilities and responding and prioritizing to things.

Senator HEITKAMP. I think that would not exactly give them any comfort.

Ms. Woodrow?

Ms. WOODROW. Thank you for asking that question. As a representative of a regional bank, I certainly feel that pressure. And there is so much of a difference between the very large money center banks and the community banks, credit unions. We are all subject to the same law. We all have to follow the same regulations. But the ability, the sophistication, and the resources are very different.

I think that is one of the reasons why I feel it is important that we allow banks of all sizes to experiment and to collaborate with each other. So, for example, small banks, community banks, and regional banks could get together and collaborate on activities, collaborate on resources and technology, rather than going it alone. And to do this, it is important to make sure that we have that flexibility both from a regulatory perspective and an examiner perspective, that they are willing to allow us to do that, and from an information-sharing perspective so that we could pool our resources and I think be much more effective.

Senator HEITKAMP. Mr. Poncy?

Mr. PONCY. Thank you, Senator. It is a great question and one that we debated a lot when I was in Government and continue to see in the private sector.

The first answer, which you probably heard and deserves some more color, is this is the risk-based approach. So if you are a small thrift or a community bank, you do not have the same risks as a dollar-clearing money center bank. But you still have the responsibility to understand the risks associated with your customers, which if they are local you are going to know them better, the products and services that you offer, which, again, they would be fairly straightforward banking products and less esoteric financial instruments, and the markets in which you are transacting. You probably do not have correspondent relationships with Kerplakistan.

So that should inform a targeted approach to risk management that is very different for a local community bank than it is for a global bank. That philosophical understanding breaks down often in practice because it is challenging. And so the first point I would make is that in implementing a risk-based approach, there has to be more training—more training about what a risk-based approach means, what the determinants of risk are across customers' products, services, and markets, and how those risks are evident in certain local communities in ways that are vastly different than other places. That is the first point.

The second is that with respect to managing those risks, there should be greater attention and prioritization over what we call "utilities" or "consortium." So take training as an example. Why isn't training provided in a regional platform or a community bank platform in a more accelerated fashion? This is an area where community banks can pool their resources to get an education on this, and, again, something that we are working on.

Another way to think about utilities is operational. Dennis mentioned, and I fully agree, we have talked for years around taking the Bank Secrecy Act Advisory Group, which sits at Treasury, as basically a central policymaking group exempt from FACA, and localizing those around prosecutor offices and saying, Why don't we have local SAR review teams meeting on a regular basis with the filers in that community that help those community banks understand this is what your local investigators are seeing, this is what your prosecutors are interested in? It creates much more of a public-private sector partnership. So the utilities are a second idea.

The last one just looks at shared risk management as a principle. This gets to Senator Donnelly's point about real estate. It is very difficult for community banks to absorb all the responsibility of risk management when a lot of those risks are coming through financial service sectors that distance the bank from the underlying risk. Almost every bank I can think of has escrow accounts, to Tracy's point, whether it is for real estate or for law firms or for other purposes. And we see money laundering through those accounts.

There is a case in my testimony that is literally incredible about over $300 billion that were laundered through a top law firm in the United States, an escrow account, to buy real estate on behalf of the alleged, under DOJ's civil complaint, the former Prime Minister of Malaysia. That is an astounding case. That is an astounding case. How does that happen at a top bank and a top law firm? Because we do not have controls on those sorts of intermediary accounts. Community banks do not have that exposure, but they have those types of accounts that can introduce it.

So that is a shared risk management responsibility that requires banks to—or, sorry, requires authorities to give banks some relief by sharing that risk management responsibility with others that introduce that risk.

Senator HEITKAMP. I think just speaking from a position as a former law enforcement officer, I think you would have a hard time convincing law enforcement officers and prosecutors to share intel more broadly to nonlaw enforcement folks, and that creates a real challenge because you want to avoid the subpoena that is going to tell you you did something wrong, but law enforcement is not going to want to broadly broadcast, you know, what they are currently looking at and where they go.

If I can just get a few more minutes, I want to talk about artificial intelligence. There has been a lot of talk about whether artificial intelligence is going to be the great equalizer. It was interesting. During a Banking hearing recently, I made the claim that perhaps on compliance burdens it will, again, skew to the larger banks. And, actually, a regional bank officer who was testifying said, no, she thought that it might actually bring costs down and

allow you to balance, depending upon what product is out there that is going to provide that kind of compliance check.

So if we looked at—you know, this is a function we are asking banks to take on for the betterment and the security of our country. It is not something that, you know, is part of their business model, but it is a critical component of making sure that we are safe and secure. And so when we look at artificial intelligence, does it make sense to look at products which can be deployed and look at shared costs for that kind of technology that will lower costs for smaller financial institutions but achieve a better result consequently? Mr. Poncy?

Mr. PONCY. Senator, you are hitting on, I think, one of the most exciting ideas in AML in a long time, and I agree with everything you said. I would just point to the relationship between the potential of these new technologies to include artificial intelligence and the need for data. The data that you need to drive AI systems so that you have real fidelity in the results and understand that this is a bad apple and this one looks like a bad apple but it is actually legitimate requires pooling of information at the moment, is constrained by information-sharing restrictions or ambiguities. There is a section in my testimony—and I know we have talked about it in other places—about the need to clarify and strengthen information-sharing allowances, if not requirements, so that financial institutions can do exactly what you are saying, that they can take their transactional information, their customer information, their counterparty information, throw it onto a platform with the right kinds of controls around it, where these types of artificial intelligence systems can exploit that data to learn what good looks like and what bad looks like. Once those models are established, those can be migrated to other platforms.

We do not know enough, frankly, at least in my view, to know what is the best way to do this, but clearly the next step is to encourage pilots around these sorts of enterprises, and that can be done with stronger information sharing allowances or requirements and incentives to banks and others to play.

Just two more points because they are related. One is if you think about this from a bank perspective, if you are the general counsel of a bank and you hear this conversation, you can think this is really exciting, we should do it. But what happens if I put my information into that platform because I want to do the right thing, and then there is an investigation stemming from my voluntary or at least my proactive approach to compliance and risk management that all of a sudden exposes my bank to an enforcement action? I cannot do that as a general counsel in good faith as a fiduciary to my institution, create that exposure. So what kind of downside protection are you going to give me? We cannot give safe harbor. We have all been there before. But we can be creative in thinking about protections that incentivize institutions by giving them downside risk management.

On the upside, if I am going to be putting my information into this platform and dedicating analysts to that, do I get any credit for that? Because that is not necessarily in my exam manual. It is not necessarily part of my exam process. And these are resources that have an opportunity cost.

So if I am playing in that space, what sort of credit do I get for that? I know that sounds petty, but it is not, because if you are sitting there running these programs, you have to make these choices, and this is where congressional direction can really help.

Senator HEITKAMP. I do not think it is petty. I think that we are asking banks and financial institutions to perform a function that does not add any value to them but adds value to the country and the security of the financial system as a whole but also the security of our country against human traffickers, against money launderers, you know, the whole nine yards.

So a tough topic, but I am really concerned about what is going to happen to our small community banks as we have put more and more regulatory burden on them, more regulatory burden and a high-risk regulatory burden.

Thank you, Mr. Chairman.

Senator SASSE. Thank you, Senator.

Let us go back to this question from the beginning of Senator Heitkamp's questioning about the feedback loops. And, Ms. Woodrow, you talked about this in your opening statement, your stat that only 4 percent of the time do SARs ever result in the bank hearing anything back. Can you unpack that a little bit? A, how do we know that? And then, B, let us move toward best- and worst-case scenarios about what, say, regional banks understand about what is happening on the other side of their regulatory filings?

Ms. WOODROW. Certainly, Senator. Thank you. Anecdotally, we have always heard from our peers that very few SARs result in law enforcement getting back to the bank in any way, whether it be through a subpoena or a request for SAR backup documentation. So through The Clearing House, we decided to get some data, and we took a poll of our membership, and I also contributed to that. And that is where we got the 4 percent number, and that was consistent with what I was seeing as well.

What we find are that it is very seldom that we do get feedback. Now, sometimes we do get direct feedback if law enforcement is able to use our investigation to successfully pursue a criminal conviction. I have to say law enforcement is incredibly grateful to that effort, and we have had great responses from the FBI, from local law enforcement, from the U.S. Attorney's Offices, and we relish that feedback and are able to use that to go back and talk to our staff about, OK, this was what we saw and we thought it might be suspicious, and here is what law enforcement had to say about it. So that is hugely important to us.

And, also, those communications with law enforcement as to what they are seeing, there is a communication that the district attorney of New York provides. They had a meeting and provided us with some IP addresses where potentially terrorist financing activity was occurring. We were able to take those IP addresses and run them against our bank's systems to see if any of our customers had accessed their accounts in those locations. That triangulation of information is so incredibly pertinent to what we do and allows us to really shift through the millions and millions of transactions that we are dealing with on a yearly basis. And, you know, the bigger the bank, the more that becomes a challenge.

Senator SASSE. It seems to me that those feedback loops matter for three reasons. You are leading 300 people, is that what you said, in your organization?

Ms. WOODROW. Yes, over 300.

Senator SASSE. If they are just sitting on the other side of a black box doing a regulatory job as opposed to feeling any connection to a larger mission with law enforcement and for the social good, if they do not have any sense of whether or not their work matters, they are inevitably going to be less innovative in trying to figure out ways that this next generation of more data, enhanced data-saturated world is going to have some of you all giving new ideas about how this should happen, but also aiding law enforcement in the case of those current investigations, which are complicated, but where you may know IP or specific computer locations of these institutions.

Mr. Lormel, on the FBI side, so when you were at the Bureau running this section, can you give us a perspective on is there more information that the 300 folks reporting to Ms. Woodrow could be supplying to you if those feedback loops were tighter?

Mr. LORMEL. Absolutely, yes. And one of the things, when I ran the Financial Crimes Program at the FBI, I met frequently—and, beyond that—I started the terrorist financing operations at the FBI, and particularly after 9/11, I met on a very frequent basis with Jim Sloan, who was then the Director of FinCEN, and Jim and I would sit for hours and have this discussion about what can we do to put a feedback mechanism in place that is consistent.

In my written testimony, I give you some examples of some of the working groups, and on those working group levels, there is tremendous feedback. But this is a significant issue, and it is a significant problem. And if we could put a consistent feedback mechanism where there is an automatic feedback loop back to the financial institution, I think there is tangible and intangible value there. Certainly the tangible value is what benefit they are going to get, but also the intangible. I think if I were able to contact FinCEN and say, hey, your SAR did this, this, and this, those folks who do that, their morale is going to be a lot better because they are going to have a better sense of accomplishment. And I made the comment before and I really means this. One of the things that—I really enjoy working in this space with people like Tracy because they are very dedicated, just like we were in law enforcement, and they really want to do the right thing. And the more we give them that ammunition and if we can put that feedback mechanism in place, I think that would be one of the biggest benefits to anything we can do to enhance the BSA.

Senator SASSE. Thank you.

Mr. Poncy, I am going to ask you about this as well, but I am going to defer to Senator Donnelly first, but in my next round I will come back to you.

Senator DONNELLY. Thank you, Mr. Chairman.

I wanted to ask you about virtual currencies, which are an alternative to cash that criminals may use for illicit transactions. Bitcoin, Ripple, and Etherium provide anonymity, are lightly regulated, with limited AML controls. This is to everybody. To what extent do you believe criminal networks, terrorist groups, and rogue

nations utilize cryptocurrencies as a means for moving money anonymously?

Mr. LORMEL. I will start out on that. I think the more these systems mature, the more they are going to be used. I think on the front end—I have listened recently to some law enforcement presentations, and law enforcement feels pretty comfortable, especially with Bitcoin and the blockchain, that they can identify transactions, and so there is a deterrent there by virtue of that, and I think there are some good cases out in California on that. But the more comfortable they get in that space and the more that they can get around and create anonymity or a sense of anonymity, you are going to see more and more of that activity happen. And if you liken Bitcoin and virtual currency to regular currency, to cash, the more comfortable the bad guys get with that and the more cash-like they think and act, the more they will use this as a case.

There was a case in New York, and I apologize, I do not recall the girl's name. She was recently arrested in New York as a sympathizer and providing material support to the Islamic State. She was a healthcare worker, and she went to Syria, and she wound up teaming up with the Islamic State in some camps over there using the facade of aid. But my point is when she came back to the United States, she committed all types of credit card frauds and things, and she purchased Bitcoin, and she used the Bitcoin to—she used the Bitcoin, and she converted the Bitcoin back to cash, and she sent that money over to Syria. And the FBI has made a good case, and I speak about it because I know that she has been indicted, so there are charging documents there.

Ms. WOODROW. Thank you. Bitcoin is something—and other virtual currencies—that we have been looking at a lot over the last year. We did notice amongst our customer base that the transactions between customers and Bitcoin brokers had increased quite substantially, particularly in the later half of last year. So trying to sort out which of those are just ordinary transactions done by ordinary people, either because they are interested or because they think it is a good investment or whatever their purpose, from those that are listed is particularly tough because we lose a little bit of the trail once it goes into the distributed ledger, because we are not seeing it. We can see very clearly sometimes when there is money movement between financial institutions, a little bit different on the virtual currency side.

Virtual currency brokers in the United States are deemed to be money services businesses by FinCEN, so they should also have an AML program as well as Know Your Customer. The difficulty is those that are operating outside the United States. And, remember, this is a virtual environment, so maintaining jurisdiction over the actors is a real challenge. They could be literally anywhere on the planet. But it is something that we are seeing more of. I certainly am familiar with dark web websites where you buy literally any type of illicit good or service you can think of. Those are almost always transacted in virtual currencies.

Senator DONNELLY. OK. Let me ask you a different question, Mr. Poncy. If CTR/SAR thresholds were increased above current levels, how do you think that would impact law enforcement and their investigations?

Mr. PONCY. Thanks, and Dennis is the best person I know to opine on this, but——

Senator DONNELLY. He was going to be next.

Mr. PONCY. OK, good. I am going to take a little bit different direction, but it is consistent, I think, with where Dennis is thinking. To me, raising thresholds is sort of a derivative question to the primary issue of how do you get law enforcement access to more data and how do you do that in a way that is less costly to financial institutions, because that is what is really going on here. Reports are expensive, and you have industry that continuously is saying, look, you know, inflation rates have gone up, and our SARs are going through the roof, and this is all expensive, and how are you using this, and can we get some relief here. That is the conversation, and law enforcement is saying the more data the better because financial information is becoming increasingly important to everything we do. And so we do not want to do anything that is going to turn off the pipe because we do not know which data you have that may be relevant to what we are looking at now or what we are looking at down the road, so do not turn anything off. And both sides are right, but there is a solution for both, which is given the current technologies that are coming online, we can collect and manage and analyze bulk data better than ever before.

So if you imagine a scenario where we have straight-through processing of bulk data coming in to FinCEN or the BSA which Congress required us to study in 2004, 14 years ago, on cross-border wires, all cross-border wires going into this database, law enforcement would love that, to see anybody who is sending money into the United States or getting money from the United States. That is a huge data set. And building that sort of straight-through processing certainly is expensive, but once you have that done, imagine that the business as usual expense of that is significantly less than processing individual transactions and making determinations of whether to file this or not, just get it in.

The second way to think about accelerating data access for law enforcement and reducing costs for financial institutions is to do what other financial centers have done, which, in addition to doing cross-border wire reporting in bulk form, is to think about reporting all accounts. If you have a customer account, send an account-opening form to FinCEN and have that form—if you have got that information as law enforcement, a lot of the need for additional data is addressed, and then these conversations get——

Senator DONNELLY. I apologize. I have limited time. I have to pass it to Dennis and then back to the Chairman.

Mr. LORMEL. Thank you, Senator. What Chip is saying—and I like those ideas—I think that is a long-term look. In the immediate term, I am a firm believer that we cannot raise the SAR threshold or the CTR threshold. I think the information at that level right now is invaluable to law enforcement.

Senator Sasse gave me the example of let us talk about MS–13. I would think if we were able to go back and do a study on that, you are going to see a lot of CTRs. You are going to see suspicious activity reports. And I can go back to when I was in the Bureau, Zacarias Moussaoui, when I ran the Terrorist Finance Operations Section, he came into the United States, he had $35,000 in cash on

him when he came in. And Jeff Breinholt is sitting here, who I worked with at the Department of Justice at the time, and we were shocked that he actually filed a CMIR, or he filed the appropriate papers with Customs coming into the country. But then he went and withdrew money from—cash out of a bank account, $14,000. That is intelligence that we would lose if we raised that threshold to $30,000.

You know, I realize that we are talking about a smaller percentage, but people like that are so dangerous. And so I think—and I think you really need to task law enforcement to give you some statistics on this. I talked to the Bureau when I was coming up here to testify. I was able to talk to my former counterparts who took my positions, and they are firm believers that we need the threshold at that level. And I will certainly defer to them in terms of their ability to give you the proof.

Senator DONNELLY. OK. Thank you, Mr. Chairman.

Senator SASSE. Thank you, Senator.

Let us stay here a little bit, and I think there is probably a debate that is worth teasing out. Maybe a few distinctions for some rookies.

So there is cross-border stuff. There is intra-U.S. stuff. There are small organizations and large organizations. And then there are cases where we have some reason to be suspicious versus mere quantification. Maybe there is no distinction that is worth drawing here, too, which is a lot of this we are thinking about because of the regulatory compliance burden of data that may not ultimately be used, and then there is a separate conversation which is about personally identifiable information and the fact that building a big database in a world where, let us face it, we, public sector and private sector, are pretty terrible at cyber defense right now. And so the bigger database you create, the more that is going to be a target for future hacking, and we have seen that with Equifax and others, and you have seen obviously the reports today that many people in the intelligence community have known about for some time, but the Chinese hack of OPM 3 years ago, now we see specific records of that showing up in financial fraud today that abused personal information.

So there are a whole bunch of distinctions there, but it seems like one question that is worth teasing out is of the $10,000 threshold—and I think this was set in 1970. Is that right? So the inflation-adjusted view of that would be $65,000, $70,000 today. If we did not have that—and obviously we have lots of small financial institutions who do not want to be doing these reports right now. I think one of the critical questions we should be asking is how much of the information that is between that $10,000 and $65,000 threshold that comes in from small institutions is actually used. What do we know?

Mr. PONCY. I think you have got a great handle, Senator, on these issues that are——

Senator SASSE. You are not technically under oath, but lying is still ill advised.

[Laughter.]

Mr. PONCY. You have teased out exactly all the difficult debates around what appears to be a fairly straightforward question. There

is just one additional one I would add. In terms of that delta of between $10,000 and $65,000, what is relevant? I completely agree with Dennis that there needs to be a study of—because that is discoverable, right? That is a discoverable question as to the value of that information, which I know Treasury has, with law enforcement, I think, released some sort of an RFP or study to try to get their arms around this. But we need that data.

The additional issue that I think is important to recognize is that while the inflation threshold would jump dramatically to the mid-60s, there is also a very different role of cash in today's economy, particularly in the United States. So it is a bit of an offset in the sense that who is placing $10,000 in cash these days and why? Right? I mean, take your traditional laundromats—no pun intended—restaurants, gas stations, *et cetera.* I remember as a kid—and this is obviously a small sample size, but you paid cash wherever you went on this sort of stuff, or maybe a checkbook. Everyone has a credit card, right? And you are doing Apple Pay and other things. Who is depositing $10,000 of cash and why? That is a more important question now than it was in 1970 by a long shot.

So it offsets that immediate instinct to look at the inflation threshold and go there because cash is more rare now and is a bigger marker than it used to be, in my view.

Senator SASSE. Please.

Ms. WOODROW. I would love to address the cash question. So I think one would assume, based upon, you know, how we transact, we are using our credit cards all the time, that cash would not be as prevalent, and it is something that every year I have to do a risk assessment for my institution and figure out where are the products and services and areas where I want to focus my effort. And so I looked at the use of cash over time, and what I saw was something interesting. Cash deposits and withdrawals had only gone down by 4 percent over a 4-year period, which was much less than I had thought. Businesses are still using cash, whether it be small businesses that are operating on close margins, they just do not have the time to wait for a check to clear, or they do not have the technology to accept things like PayPal and others, or, you know, bars, restaurants, *et cetera,* still a very cash—at least in my institutions, still a lot of cash.

What we also saw was that ACH transactions have gone through the roof, so particularly with the person-to-person payment applications, the Venmos, PayPals, and other types of work.

So I still think cash is an issue. In my own institution, we file over 120,000 CTRs a year. Now, most of them are straight-through processed, so I would not consider it my biggest concern from a resources standpoint, but not all of them are. There is some manual intervention.

The SAR threshold, it is $5,000, if you know who your suspect is. It costs, for each investigation that results in a SAR, anywhere from a few hundred dollars to a few thousand dollars. And that is whether you are filing a SAR on a $5,000 transaction, a $100,000 transaction, or a $1 million transaction. So I think it is important that that analysis be done of what are the SARs and CTRs that are being used, and for those which are not being used very much, can we think about a more efficient way of providing information

to law enforcement that is not this heavily manual process that is meticulously examined, has to be meticulously documented every time?

Senator SASSE. I have follow-up questions, but I want to let Mr. Lormel get in.

Mr. LORMEL. Just one comment, Senator. I think, as I mentioned a little earlier, to me one of the biggest problems we have in the financial services industry are the illegal money remitters that are operating as the ice cream shop or some grocery store or whatever, and they are actually involved in illegal money remittance. That is where you are going to see a lot of cash transactions. And I think in those, if I were still running the Financial Crimes Program, I would be looking to do a special where you had kind of a nationwide takedown of these—to promote awareness to the nature of this problem, I think, you know, from what I had seen. And we went back—and this goes back to when I was in the Bureau. This is a consistent problem, and it was interesting when Tracy said that she has only seen a decline of 4 percent in cash. That tells me that those illegal money remitters are still up and running and flourishing.

Senator SASSE. I want to let Senator Donnelly have the floor back, but just one quick one that I am sure is not easy. You are good? OK. Then how big—what is the shape of the curve in our assumptions about who the money launderers in America? If we had a 35,000-foot view at FinCEN or at the Bureau and we could rank-order the biggest money launderer in America to some mom-and-pop, you know, illegal lemonade stand, do we think that there is an 80/20 curve that the big guys are a really big share of this? Or is most of it small and medium size? That would drive the way we would actually do our analysis in our fusion centers.

Mr. LORMEL. That is a terrific question, and the FBI in the last couple of years, they stood up a money-laundering unit again. When the financial crisis came, they disbanded that unit, but they have got that up and running. And one of the things that they are targeting, Senator, are the facilitators, the money-laundering facilitators. We started the hearing, and I joked about not being a money launderer. But, quite frankly, there are a lot of people like me out there who do this, and they facilitate. And Tracy talked about the gatekeepers.

And so what the FBI is doing is they are targeting that level, so that is a high level of people, and one of the challenges we have societally is that you are going to see those money launderers at all those levels. But, clearly, there are a level of more advanced and more sophisticated money launderers.

Senator SASSE. Thank you.

Mr. PONCY. Thank you, Senator. Again, great question. My last few years at the Treasury Department, we had a team that was focused on what we called "3PML," third-party money launderers, to get to exactly your question. Is there what I would chronically call a "Keyser Soze of money laundering" that we do not see? Or is this happening where every criminal enterprise just self-launders because it is easy and they do not want to pay a premium for it? You know, how does this work? And at least in my experience and what I recall is that there really was not good data on this.

So we pushed really hard with the interagency through a number of law enforcement and intelligence agencies to stand up efforts to try to understand 3PML. What we found—and it is frustrating—is that sophisticated investigations that are inevitable with any third-party money laundering, a guy who is good at this and is worth chasing, he is not going to stay here very long. So those investigations tend to be the ones that are thwarted, and so that is why our data is not that great.

If you start to really examine the incentives for investigators, for prosecutors, for analysts to pursue those investigations, those incentives go downhill real fast, because the minute that you see you have got an investigation that is going to take years, take you to three jurisdictions that do not do what we do, if they do they will not give you the information, if you get there they will already be gone. You realize it is an expensive investigation, chewing up resources, opportunity costs and predicates, there is violent crime in your district right now, those are cases that just are difficult to make.

And if you then look at metrics that law enforcement is considering, arrests, indictments, confiscations, prosecutions, sentencing, *et cetera,* these metrics, right? They do not stack up to incentivize those sorts of investigations.

So I will defer to Dennis all day on this, but it was very clear to me that we did not have the type of dedicated funding for sophisticated financial investigations that we would need to answer that question with confidence, and one of the recommendations I have in my testimony is to create protected resources for the law enforcement community to stand up, dedicated units to go after third-party money laundering, with prosecutors, with investigators, with travel budgets, that allow them to start to answer that question in a systematic way.

Senator SASSE. We have a series of votes coming up, so we are going to have to wind up in about 10 minutes. But before we ask the sort of King for a Day questions for you all to go back through your top three recommendations about what you would like to see happen, could we unpack just once more our theory about how much of this money is cross-border? Of everything we care about, if we were much better at seeing money that moved in and out of the United States, does that solve most of our problem? Or do we think lots of the problem is intra-U.S. domestic money laundering?

Mr. LORMEL. I think it is more the transnational problem, certainly, and that does not diminish the problem in-country. But I would say it is more the cross-border issues.

Ms. WOODROW. I think it really depends on the underlying crime. Cross-border is certainly a substantial part, whether it comes to international drug trade, terrorist financing, international frauds.

From a regional or a community bank perspective, we are going to see a lot of that happening domestically, but eventually it is going to reach itself outside the borders.

Mr. PONCY. I fully agree, and in my testimony I have a number of pages dedicated to explaining how during my time in Government transnational organized crime literally became a national security threat. I think it was 2011 when we officially recognized that, and that action was years in coming, where, again, I go back

to anybody worth chasing is not here that long. They may have a market that they have to hit here, whether it is a drug market or it is a financial service or dollarization, but they are going to get in and get out because we are a deterrent in the sense that our AML/CFT regime is good. But just as every business these days is considering international connectivity from customers to suppliers to vendors, *et cetera,* the same is true for transnational organized crime. These are opportunistic groups that take advantage of globalization the same way that legitimate businesses do. And so as the whole world has gone global in terms of, again, their connectivity in a sophisticated, specialized global economy, TCOs, transnational criminal organizations, have done the same thing. To me it just puts more and more pressure on something that, notwithstanding the sort of Tomorrowland idea of cross-border reporting being too far off, that was supposed to be done years ago. In fact, there is a proposed rule that is already 2 or 3 years dated where systems studies have already been done. That can be turned on if it is resourced, if it is prioritized, and then we can test this, right? And we can actually get that data and start to see, to Dennis' point, where are funnel accounts. It is hard to see that at any individual institution because, again, anybody worth catching is not going to structure all this in one place. They are going to go to different institutions, they are going to go to different geographies. And until you start to see cross-border, oh, look at this, all of this is going to that counterparty, that jurisdiction, that financial institution, now I can see that, that is a funnel account offshore, which, if I were back, that is what I would be doing all day. We cannot see that, and it is within our grasp, and it is within our grasp in a way that is cost-effective.

Senator SASSE. Mr. Lormel, it seems like you had a point on funneling as well?

Mr. LORMEL. I was in agreement with Chip on that. That was well said, Chip.

Senator SASSE. Great. If we could just maybe limit yourselves to 2 or 3 minutes each, but we will go in the order that we began and do your sort of top three, or whatever the right number is, your King for a Day high-priority recommendations list, please?

Mr. LORMEL. Yes, sir. Thank you.

First, one thing we did not talk about was regulatory requirements versus regulatory expectations, so that would be something I would look at. I think one of the things that hamstrings the banks is the burden of the expectation versus what is required, the feedback mechanism. I really think if we can have a consistent feedback mechanism, that would be important.

The reporting thresholds, you know, I will defer to law enforcement to defend that, but I am an ardent believer that we need to keep the thresholds where they are. And beneficial ownership, we really need to do something about beneficial ownership.

So thank you. Thank you for holding this hearing. I think this was very thoughtful.

Senator SASSE. Thank you.

Ms. Woodrow?

Ms. WOODROW. Thank you, and I do appreciate the time and attention to this really important topic. I think if I was to look at my

priorities, improving consistency across the different banking regulators through a national strategy, whether that is led by FinCEN or another agency, improving that data sharing between law enforcement and financial institutions, help us get the information that we need to target our monitoring to what law enforcement really wants to see.

Third, allowing the sharing between banks so that we can collaborate and combine our resources and expertise.

And then I am in agreement with my co-panelists here on the importance of the transparency with regard to legal entities.

Senator SASSE. Thank you.

Ms. WOODROW. Thank you.

Senator SASSE. Mr. Poncy?

Mr. PONCY. I was trying to jam as many as I could into three points, so I was furiously scribbling to try to get ten inside of three. I was not really successful.

The first, anonymous companies. Absolutely we should be ending anonymous companies created in the United States. It is way overdue. There is plenty on the record for that. How you do that is an interesting question, but the how cannot prevent us from ever getting there. We are just going to have to prioritize and get it done. Reasonable people can disagree on what good looks like, but we should not let great prevent good from happening, which is really where we are.

Two is pilots. We do not know a lot about the questions that you have asked, and I think we need to create a market to get data. That is about information sharing. That is about new technologies. That is about systematic reporting, including cross-border reporting. We need pilots to get up and running so that we can see what good looks like.

Third, we really do need to invest in protected financial investigative teams that can go after sophisticated money launderers without having to worry about metrics that chronically put pressure on those budgets. And there is a part in my testimony that leans on the fact that—this is a potential wormhole, but our best financial investigative expertise has always been in IRS, and it has never been a popular agency for reasons you probably understand better than I. Does it need to stay that way? CPAs that also carry guns and badges, can they be more liberalized to work on sophisticated financial investigations to support the Bureau, to support DHS, to support others? They cannot do that without resources. They may never get there in IRS. But they can get there in Treasury. So there are ways to restructure this in ways that allow us to finance our best financial investigators, to support our best law enforcement agencies without that hang-up of the IRS, and that is an interesting conversation.

So those would be the three that I would pursue.

Senator SASSE. Very helpful on that last point. What we see across the IC, places where we are getting better in a world with more and more cyber crime and cyber risk generally, is a move away from an assumption about bureaucratic centrality and priority over other bureaucracies and fusion centers that are starting with what data do we have and what data do we need, and then

you build your human capital around something that begins with strategy and data access.

Thank you to all three of you for being here. We appreciate it. We are going to leave the record open—I think what I am officially supposed to say—for Senators who wish to submit questions for the record. Those questions are due on Wednesday, June 27th, and I encourage our witnesses, if you receive questions, to respond promptly.

I thank you for your cooperation and assistance, and this hearing is concluded.

[Whereupon, at 4:03 p.m., the hearing was adjourned.]

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

PREPARED STATEMENT OF DENNIS M. LORMEL

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

JUNE 20, 2018

Good afternoon Chairman Sasse, Ranking Member Donnelly and distinguished Members of the Subcommittee. My name is Dennis M. Lormel. I have been engaged in the fight against money laundering and illicit finance for 45 years. Between my law enforcement experience and my private sector consulting experience, as a subject matter expert, I have developed a unique perspective regarding the benefits and burdens of the Bank Secrecy Act (BSA). Having served for 31 years in the Government, 28 years as a Special Agent in the Federal Bureau of Investigation (FBI), I was the direct beneficiary of BSA reporting. Now, having been in the private sector, working as a consultant and subject matter expert, primarily with the financial services industry, I have become sensitive to the burdens and challenges of BSA reporting encountered by financial institutions. Those burdens and challenges are driven in part by regulatory requirements and expectations, as well as by the lack of consistent feedback mechanisms from law enforcement regarding the value of BSA reporting. Make no mistake, BSA reporting is essential to law enforcement's ability to defend our national security and the economy from the threats posed by terrorism, counterintelligence and criminal adversaries. Therefore, having a thoughtful discussion about how to meaningfully enhance and not diminish the effectiveness and efficiency of BSA reporting is critically important to all stakeholders.

Money laundering and other forms of illicit finance are an extremely important topic, especially when placed in context with BSA reporting requirements and expectations. I had the privilege of testifying before the Senate Banking Committee on January 9, 2018. As Subcommittee Members may recall, that hearing addressed "Combating Money Laundering and Other Illicit Finance: Opportunities to Reform and Strengthen BSA Enforcement." I applaud the Subcommittee for holding this hearing to delve deeper into this important topic. The reality is that terrorists, terrorist organizations, spies, criminals and criminal organizations invariably rely on the financial system to move and access funding. The one commonality that terrorists, spies and criminals share is the need for funding. Without adequate funding, bad actors are much less likely to succeed with their nefarious activities. Therefore, the more effective and efficient we can make BSA reporting, the more challenging and disruptive it will be for bad actors to move and access needed funding.

I would like to refer to my written statement from the January 9, 2018, hearing as a framework to build on with my testimony today. As I stated in that session: "In using the financial system, criminals and terrorists are confronted with distinct contrasts. On one hand, the financial system serves as a facilitation tool enabling bad actors to have continuous access to funding. On the other hand, the financial system serves as a detection mechanism. Illicit funds can be identified and interdicted through monitoring and investigation. Financing is the lifeblood of criminal and terrorist organizations. At the same time, financing is one of their major vulnerabilities."

By understanding how criminals and terrorists launder money and avoid detection; how financial institutions succeed in targeting them; how law enforcement can leverage financial intelligence derived from financial institution; and how the funding flows involving various criminal activities can differ or be similar; financial institutions position themselves to better detect and not facilitate money laundering. Once suspicious activity has been identified and reported, law enforcement is better positioned to interdict and disrupt said criminal activity. The more productively financial institutions and law enforcement can collaborate with each other and share information, the more effective and efficient BSA reporting will be.

You asked me to provide my perspective today on how criminal organizations launder money and avoid detection by financial institutions to include the following topics:

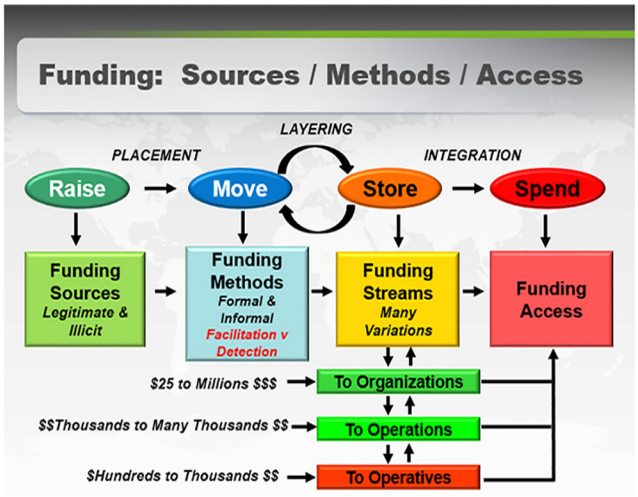
- Money laundering issues relating to narcotics trafficking, trade-based money laundering, human trafficking, and real estate money laundering;
- The development and implementation of money laundering typologies to fight crimes such as, but not limited to, human trafficking;
- Effective means of cooperation and coordination with law enforcement officials;
- How to improve information sharing between individual financial institutions and with law enforcement.

Background

Before addressing the four bullet points above, it is important to establish who we are dealing with; in what context we are dealing with them; discuss the nexus between money laundering and fraud, and how that relates to predicate offenses or specified unlawful activities; and visualize the flow of funds as to how bad actors use the financial system.

Who are we dealing with regarding the myriad of criminal offenses? We are dealing with individuals, groups of individuals, domestic criminal organizations, transnational criminal organizations, homegrown violent extremists and terrorist operatives, and terrorist organizations. Bad actors usually have the advantage of being more proactive. BSA reporting is inherently reactive. This gives the bad actors an advantage, which is a challenge for financial institutions and law enforcement. Another challenge is that the different categories of bad actors set forth above will interact with each other if it is in their mutual best interest. This is particularly true with transnational criminal organizations and terrorist organizations. This is referred to as the convergence between criminals and terrorists. There is a nexus between fraud and money laundering. Fraud and money laundering are interconnected. The proceeds of fraud and other predicate offenses or specified unlawful activities need to be laundered. Taking this a step further, if you list most predicate offenses, which would include drug trafficking, trade-based money laundering, human trafficking, and real estate fraud; they will most likely contain elements of fraud and require money laundering. If you list predicate offenses and placed fraud on the top of the list and money laundering at the bottom of the list and envision the list to be a sandwich, the predicate offenses would represent the meat. Fraud and money laundering would be the gourmet bread. A great sandwich requires great bread. Successful criminal activity requires fraud and money laundering.

It is important to visualize the flow of funds. Regardless of the nature of the predicate offense, and how similar or different they are, and how similar or different they flow through the financial system, the process is the same. Criminals and terrorists raise, move, store and spend funds. This is the basic funding flow. When criminals raise money the source of funds will be illicit. When terrorists raise money the source of funds will be legitimate or illegitimate. Funds are then moved either through the formal or informal financial systems. Funding will be stored and will either continue to be stored or continue to be moved and stored and then spent. This is where funding flows for different criminal activity may differ more significantly. Following the moving and storage flow the funds are spent. Money laundering is a three step process: placement, layering and integration. When money is raised and moved, this is the placement stage of money laundering. When money is moved and stored, it is the layering stage of money laundering. The more the money is moved and stored the more seemingly legitimized the funds become. When the money flows from being stored to spent, it represents the integration stage of money laundering. This is where funding is accessed as being seemingly legitimate in furtherance of nefarious purposes. As funds flow through the moving and storing phases, this is where financial institutions are facilitation tools or detection mechanisms. Below is a flow chart visualizing the funding flow described above. The funding flow below the funding streams box relate more directly to terrorist financing, although it could relate to transnational criminal organizations as well. The rest of the funding flow is consistent for criminals and terrorists alike.



The main distinction between terrorist financing and criminal money laundering is that terrorist financing tends to be linear and criminal money laundering tends to be circular. In that regard, in terrorism, the spend or funding access flows linearly to support a terrorist activity. In criminal money laundering, the spend or funding access flows back to the criminal or criminal enterprise in a circular manner.

Money laundering issues relating to narcotics trafficking, trade-based money laundering, human trafficking, and real estate money laundering

The Financial Action Task Force (FATF) is an international governmental body that serves as the standard bearer for combating money laundering. The FATF 40 Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing. Recommendation 3, of the FATF 40 Recommendations, states that "countries should apply the crime of money laundering to all serious offenses with a view to include the widest range of predicate offenses." Regardless of differences in the myriad of predicate offenses, law enforcement should include charges of money laundering when pursuing criminal prosecution in activities to include narcotics trafficking, trade-based money laundering, human trafficking and real estate money laundering. This reinforces why BSA reporting is so important.

When assessing money laundering issues regarding narcotics trafficking, trade-based money laundering, human trafficking and real estate money laundering, the starting point is the scope of the crime problem. Drug trafficking has long been and continues to be the most prolific global crime problem. Human trafficking has evolved to become the second most significant global crime problem. It is difficult to quantify trade-based money laundering. However, trade-based money laundering is, in a sense, a growth industry. Trade based money laundering is a global problem but centered more regionally where there are free trade zones. There are many real estate related frauds. For purposes of this discussion, much attention has been placed on the purchase of highly expensive real estate in select geographic regions around the world. Much of this real estate is purchased through shell companies or nominees and is paid for in cash.

The next consideration to assess is who we are dealing with, how are they likely to touch the financial system and where are the touch points geographically. Drug trafficking is more inclined to include domestic and transnationalcriminal organizations. Terrorist organizations will also engage in the sale of narcotics as a source of income. Human trafficking will more likely involve groups of individuals and both domestic and transnational criminal organizations. Trade-based money laundering will more likely involve individuals, groups of individuals and transnational

criminal organizations. For the most part, real estate money laundering involves individuals or groups of individuals. The key from an anti-money laundering (AML) perspective is to understand and identify the touch points individual criminals and groups have with financial institutions.

Narcotics trafficking and human trafficking groups can overlap by using the same supply chain or channels and involve the same groups. To the extent narcotics and human trafficking operations overlap, they will more likely have similar distribution flows. In any event, narcotics trafficking and human trafficking are more likely to have greater similarities. Trade based money laundering is more unique to other criminal activity in that it relies more on false invoicing and a wider variety of commodities. Real estate money laundering is more unique to itself because it relies more on individuals and not organizations and involves cash to purchase expensive fixed real estate. Thus there is no supply chain or channel in these real estate money laundering schemes. It should be noted that there could be exceptions to these norms.

When you understand the crime problems in terms of scope and geography, and in combination with who you are dealing with, you can begin to visualize the funding flow in terms of how the bad actors raise, move, store and spend their ill-gotten gains. An important key is to simplify the funding flow as much as possible. From an AML perspective, drug trafficking is not only the most prolific crime problem, it also represents the broadest exposure to financial institutions ranging from smurfs or mules structuring transactions under the $10,000 currency transaction report (CTR) threshold to the multi-million dollar movement of drug funds. To further complicate this challenge, drug traffickers exploit a variety of facilitation tools, such as shell companies, to avoid AML detection. Transnational drug trafficking organizations frequently engage in trade-based money laundering to move and convert large sums of money, cross border between countries, from one currency to another. One such common scheme is referred to as the Black Market Peso Exchange (BPME). This is where money brokers are used by drug traffickers to convert U.S. dollars or Euros to pesos through the sale of commodities, such as clothing or electronic equipment. As will be discussed later, patterns of funding activity or typologies involving human trafficking have been more predictable for financial institutions and law enforcement. Trade based money laundering presents a significant AML challenge for financial institutions to identify. Under and over invoicing is extremely difficult for financial institutions to identify. Trade and shipping documents tend to be less automated and more paper centric making analysis more difficult. As mentioned above, drug trafficking organizations rely on BPME, a form of trade-based money laundering, to convert the proceeds of drugs sold in the United States or Europe from dollars and Euros into pesos in Mexico and Colombia through the trade of commodities by money brokers. By their nature, BPME schemes are difficult for financial institutions to identify through traditional AML monitoring.

An example of a significant BPME case was Operation Fashion Police. In a major takedown in Los Angeles on September 10, 2014, nearly 1,000 Federal, State and local law enforcement officers seized approximately $100 million in cash, arrested nine subjects and searched dozens of businesses in the city's downtown fashion district alleged to have laundered money for Mexican drug cartels. Three fashion businesses were indicted. One was indicted for accepting bulk cash and funneling money through 17 businesses. The other two companies were indicted for structuring deposits of bulk cash to avoid reporting requirements. From reviewing the statements of facts in Federal charging documents, it appears that considerable evidence was developed from CTRs and suspicious activity reports (SARs). As a result of this case, FinCEN issued a Geographic Targeting Order (GTO) covering the Los Angeles fashion district.

With respect to real estate money laundering, FinCEN issued and subsequently renewed GTOs in six major metropolitan areas in the United States regarding the all cash purchase of luxury real estate. The GTOs required U.S. title insurance companies to identify natural persons behind shell companies used to make the all cash purchases. This crime problem demonstrates the significance of the money laundering risk presented by the issue of beneficial ownership.

The development and implementation of money laundering typologies to fight crimes such as, but not limited to, human trafficking.

Human trafficking is a heinous crime problem. I believe that AML professionals are dedicated and motivated to protect their financial institutions from the threat of money laundering and the risks associated with being exploited as a facilitation tool by bad actors. Two areas where this is particularly true are human trafficking and terrorist financing. As mentioned above, patterns of activity or typologies

involving human trafficking have been more predictable for financial institutions and law enforcement.

Before focusing more specifically on human trafficking, we should look more broadly at developing typologies to identify suspicious activity for criminal offenses. The BSA requires financial institutions to establish AML programs reasonably designed to identify and report suspicious activity. This starts with identifying red flags associated with each criminal activity. Red flags are generic warning signs. They are indicators that there might be suspicious activity. There are many lists of red flags regarding criminal activities available to financial institutions. From the list of generic red flags, I encourage financial institutions I work with to take generic red flags more specific to their institutional risk and to customize them to their institutional risk environment.

One mechanism to develop money laundering typologies is to review Federal court charging documents such as an indictment, plea agreement, criminal information and search warrant. In the affidavit supporting the charging document there will be a statement of facts. The statement of facts frequently sets forth the alleged typology used to commit the criminal offense. This is one mechanism where financial institutions can enhance the scenarios they use for transaction monitoring.

With respect to human trafficking, there are multiple sources of red flags available to financial institutions. Other red flag guidance is available from FATF, Homeland Security Investigations (HSI), the FBI and other viable sources. It should be noted that the Polaris Project has written a great reference guide about human slavery (trafficking), entitled "Typologies of Modern Slavery." In addition, human trafficking is widely discussed at industry AML training conferences. Training is one of the core pillars of an AML program. Human smuggling typologies and warning signs are frequent topics.

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

Effective means of cooperation and coordination with law enforcement officials

The most effective means of cooperation and coordination between financial institutions and law enforcement is through sustainable public and private partnerships. In addition to cooperation and coordination, these partnerships must include communication. Establishing viable partnerships begins with perspective. You must understand the perspective of your partner and overcome any impediments caused by differences in perspective. For example, the primary perspective of financial institutions is to protect the integrity of the institution, whereas the primary perspective of law enforcement is to develop evidence to obtain criminal prosecutions and to disrupt terrorist activity. At times, these perspectives can clash. In understanding perspectives and working through potential impediments, you must develop win-win situations for each partner. It's important to understand that a win-win situation may not be a best-case scenario but rather a good-case scenario. Once that has been established you can leverage the capabilities and capacity of partners to attain that good-case scenario in order to establish the win-win situation. When that foundation is established, partners can develop sustainable, innovative and impactful proactive measures to support law enforcement investigative initiatives.

The targeted monitoring projects described above involving JPMorgan Chase, and subsequently U.S. Bank, with HSI, are outstanding examples of public and private sector partnerships. Financial institutions conduct baseline transaction monitoring, which is inherently reactive. The rate of SARs used to predicate or enhance law enforcement investigations from baseline transaction monitoring is low. This is where

we must improve the effectiveness and efficiency of SAR reporting. Targeted monitoring projects result in a more proactive approach and a higher SAR utilization rate. Other outstanding examples of meaningful public and private sector partnerships is where both the FBI's Financial Crimes Section and Terrorist Financing Operations Section (TFOS) have ongoing national bank working groups in which they provide targeted information and feedback to participating financial institutions. The information sharing and feedback result in better quality BSA reporting.

As I stated in the January 9, 2018, hearing: "One of the most productive examples of public and private sector partnership, and information sharing, is the Joint Money Laundering Intelligence Task Force (JMLIT) in the United Kingdom (U.K.). JMLIT was formed by the government National Crimes Agency (NCA) in partnership with the financial sector to combat high end money laundering. JMLIT was established as a business-as-usual function in May 2016. It has been developed with partners in government, the British Bankers Association, law enforcement and more than 40 major U.K. and international banks. I'm hopeful that the United States can assess and work through information sharing and privacy concerns in order to replicate the U.K. JMLIT model."

How to improve information sharing between individual financial institutions and with law enforcement

As I stated in the January 9, 2018, hearing: "As an extension of public and private partnerships, we should consider how to improve information sharing. The PATRIOT Act provided us with information sharing vehicles such as Section 314(a) where financial institutions can share financial information with law enforcement and Section 314(b) where financial institutions can share information with each other. Efforts should be made to enhance Section 314 information sharing in the current environment. In addition, any proposed enhancements to the BSA should consider additional information sharing mechanisms. The more we can do to enhance information sharing, the more meaningful information will be for law enforcement and the more detrimental to criminals and terrorists. During their plenary session in June 2017, the Financial Action Task Force (FATF) stressed the importance of information sharing to effectively address terrorist financing. I have always been a huge proponent of information sharing to the extent legally allowable."

Law enforcement outreach is extremely important. At the grassroots or jurisdiction and/or field office level, there are informal working groups. Each of the 94 U.S. Attorney's Offices in the United States has law enforcement SAR review teams. An Assistant U.S. Attorney in each Judicial District leads the SAR review team. SAR review teams involve personnel from Federal law enforcement. In most SAR review team locations, Internal Revenue Service (IRS) Criminal Investigations plays a lead role. Depending on the jurisdiction, SAR review teams will also include State and local law enforcement agencies. Financial institutions, at the grassroots level, should participate with law enforcement at the jurisdiction level. Federal law enforcement agencies also have outreach programs at the national level and/or initiative specific level. This is exemplified by the working groups the FBI Financial Crimes Section and TFOS host at FBI Headquarters.

Feedback to financial institutions from law enforcement regarding the value of BSA reporting, particularly the value of SARs, is inconsistent. There are a number of inherent impediments to establishing a feedback mechanism. Such include the nature of criminal investigations. From the point a SAR is filed to the point a case is concluded, it could be a period of one or more years. If a case is a Grand Jury investigation, information cannot be disclosed by law enforcement. In addition, law enforcement lacks the resources to consistently provide feedback. There are always new cases to move forward with and investigators don't have time to provide feedback. Impediments aside, there are no excuses for not providing feedback. As noted in discussing targeted monitoring initiatives, in those situations, consistent feedback from law enforcement is provided and the quality of financial institution BSA reporting is outstanding.

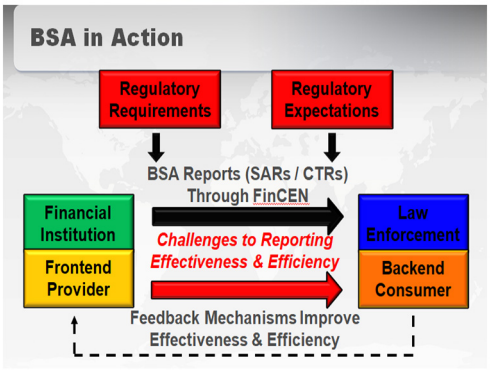
Countering the Threat by Enhancing BSA reporting from a law enforcement perspective

From my perspective, which includes my law enforcement experience and my private sector consulting experience, there are four issues that must be addressed in proposed legislation to improve or enhance BSA reporting effectiveness and efficiency. The first is less tangible or measurable and more challenging. The other three are more tangible. However one of those three is less measurable. The first is regulatory requirements versus regulatory expectations. The other three, which are more tangible are, the CTR and SAR reporting thresholds, feedback mechanisms and beneficial ownership. I believe the reporting threshold and beneficial ownership

are more measurable, whereas feedback mechanisms are not currently very measurable.

Basically, the flow of BSA reporting from financial institutions to law enforcement is extremely beneficial. However, when the filters of regulatory requirements and regulatory expectations are applied, especially the uncertainty of regulatory expectations, there is a drag or reduction in the flow and possibly the quality of BSA reporting. In keeping with the theme of the flow of information, we must consider the inconsistent feedback from law enforcement to financial institutions. Below is a flow chart which demonstrates the process of the dissemination of information.

If the space between the black and red arrows could be reduced, the real or perceived regulatory impediments would diminish and improve the flow of BSA reporting to law enforcement. An example of regulatory expectations is where financial institutions make a decision not to file a SAR. A frequent complaint I hear from AML compliance professionals is that they have to provide their regulators with more documentation for no-SAR decisions versus SAR filings. Consequently, financial institutions file SARs they otherwise would not, because of real or perceived regulatory expectations. These filings are not warranted. The time taken by financial institutions to document the no-SAR decision or to file SARs to merely satisfy regulators, coupled with the time required by law enforcement to review these SARs is time wasted and is counterproductive.



If a consistent feedback mechanism could be developed from law enforcement and financial institutions, the broken line on the above flow chart would become more connected and would improve feedback and more importantly, the quality of BSA reporting. I believe a feedback mechanism should be developed and implemented through FinCEN which is initiated by law enforcement. I further believe that SAR feedback would improve the quality of SAR submissions. I also believe that a SAR feedback mechanism would improve the morale of AML professionals who are involved in the SAR process. They would have a greater sense of accomplishment and satisfaction that their work contributes to law enforcement successes. Make no mistake; SARs play a significant role in law enforcement investigations. I believe that the FBI is assessing how to develop a more consistent SAR feedback mechanism.

My greatest concern about potential BSA enhancement legislation is any consideration to increase BSA CTR and SAR reporting thresholds. That would be devastating to law enforcement. With the current threat environment, especially with the terrorism threat of homegrown violent extremists, law enforcement needs as much financial intelligence as is legally available. Likewise, when you take into consideration the bandwidth of drug trafficking, the nuances of human trafficking and the challenge of trade-based money laundering, coupled with the variations of financial crimes, especially Ponzi schemes, raising BSA reporting thresholds will greatly diminish law enforcements capability to respond to these and other crime problems and to protect our national security and economy.

Financial intelligence, derived from financial institutions, enables law enforcement to better protect us. AML professionals have told me that increasing BSA reporting thresholds for CTRs and SARs would not likely save money and does not cause a burden. This is because financial institutions have automated systems set at the current thresholds. According to the FBI, and I have not been able to verify the statistics, if the CTR threshold is raised from the $10,000 threshold to $30,000,

the FBI would lose 78 percent of financial intelligence derived from CTRs. In addition, the FBI advised that if the SAR threshold were raised to $50,000 they anticipate an 80 percent loss in SAR filing intelligence. Finance is one of the biggest vulnerabilities of criminals and terrorists. The significant loss of any financial intelligence is a troubling detriment to law enforcement. The BSA is intended to support law enforcement, not to deter it.

I was advised by FBI executives that the FBI conducts data analysis of BSA filings, including CTRs and SARs, to enhance existing cases and to predicate new investigations. All FBI main subjects are searched against BSA data on a monthly basis. According to the FBI, they average hits on 4,000 BSA filings per month. The FBI also proactively uses data analysis to identify new cases. The FBI refers to this as targeted suspicious activity reports (TSARs). Searches are run using search terms for money laundering, terrorist financing, human trafficking, fraud, corruption, Transnational Organized Crime and other schemes. I have also heard IRS case agents, making case study presentations, at recent conferences, discuss how they run similar BSA data checks to enhance their investigations. The loss of CTR and SAR reporting, especially above 50 percent would be extremely detrimental to law enforcement investigations.

I have been advocating for beneficial ownership legislation since 2012. I have testified at hearings or briefed Congressional members and staff dating back to October 2001, about the vulnerabilities shell companies present to our financial system. This is especially true in dealing with the threat of terrorism, spies and criminals. As an example, Iran has been able to circumvent sanctions by using shell companies to provide them with access to the financial system. In one specific case, shell companies were used to allow the Alavi Foundation, Assa Corporation and the 650 Fifth Avenue Company (a partnership of Alavi and Assa) to hide the Iranian ownership of the 36 story building at 650 Fifth Avenue in New York City.

Perhaps the most compelling reason to enact beneficial ownership legislation comes from the 2016 Mutual Evaluation of the United States conducted by FATF. FATF found that the United States has a well-developed anti-money laundering regime. However, FATF noted that the system has serious gaps that impede timely access to beneficial ownership information.

Conclusion

Our threat environment is extremely concerning. Finance is one of the most important vulnerabilities to bad actors, and consequently, the threat environment. We must do whatever we can to exploit the vulnerability of bad actors and not allow them to succeed. When we consider enhancements to BSA reporting we must ensure we get it right. Those enhancements must be in the best interest of our country. That means ensuring law enforcement has the tools they need to protect national security and our economy.

Thank you for taking the time to hold this hearing and for affording me the opportunity to share my perspective on this important topic.

PREPARED STATEMENT OF TRACY S. WOODROW

SENIOR VICE PRESIDENT AND BANK SECRECY ACT/ANTI-MONEY-LAUNDERING DIRECTOR, M&T BANK CORPORATION

JUNE 20, 2018

Chairman Sasse, Ranking Member Donnelly, and Members of the Subcommittee, thank you for holding today's hearing to discuss the U.S. anti-money laundering and combating the financing of terrorism regime and its impact on the way U.S. banks employ technology to counter illicit financial activity. My name is Tracy Woodrow and I am a Senior Vice President, Bank Secrecy Act Officer and Anti-Money Laundering Director at M&T Bank. M&T Bank is a U.S. regional bank with approximately 780 domestic banking offices in eight States and the District of Columbia. Since 2013, I've overseen the bank's AML/CFT and sanctions compliance efforts. I also chair a working group at The Clearing House[1] that is analyzing the resources banks devote to AML/CFT and sanctions compliance. We are seeking to understand whether the current legal and regulatory regime is effectively addressing present-day illicit finance risks and enabling banks to use their resources to proactively identify illicit activity. I will present some of the findings from this working group

[1] The Clearing House is a banking association and payments company in the United States and is currently owned by 25 large commercial banks. The Association is a nonpartisan advocacy organization dedicated to contributing quality research, analysis and data to the public policy debate.

during my testimony as well as some insights regarding the resources M&T devotes to such efforts.[2]

As M&T's BSA/AML Officer, I lead a team of over 300 professionals who are dedicated to the cause of detecting and deterring money laundering and terrorist financing, while ensuring that our customers can conduct transactions in a safe, secure and private manner. We use a variety of standard tools in this fight, including rules-based monitoring, customer screening, enhanced due diligence for higher risk customers, and tips sent to us from fellow bank employees. In addition, we are beginning to use more modern, innovative tools. For example, we are using flexible data analytics to understand emerging risks and patterns of similar suspicious behaviors across customer groups. In some cases, we are working directly with law enforcement to identify red flags that may indicate suspicious activity in the communities we serve and have achieved great success in cases where we have worked collaboratively with law enforcement to thwart criminal activity. We are also exploring the use of automation, artificial intelligence and shared utilities across financial institutions as tools which may allow us to better assess huge amounts of data and identify unusual financial transactions.

While we have achieved significant success in the fight against money laundering, which in some cases has led to the detection of illicit finance and ultimately criminal convictions, I believe that the financial industry can be even more effective. Increased effectiveness can be achieved if we are given the tools and flexibility to increase innovation, focus on the most serious risks and collaborate closely with law enforcement and peer institutions. Criminal actors who seek to use the U.S. financial system to do harm in our communities are well financed, highly motivated and agile. To effectively combat this threat, we must continue to evolve and strengthen our anti-money laundering regime. We must re-evaluate the expectations placed on financial institutions so that we do not inadvertently place a higher value on the ability to precisely and comprehensively document the evaluation of routine transactions than we place on the ability to provide meaningful information to law enforcement.

As you are aware, the Bank Secrecy Act was passed by Congress in 1970 and has been added to, but not significantly reformed, by the legislature since. The Act requires financial institutions to provide law enforcement with leads that are of a "high degree of usefulness"[3] while also setting basic requirements for AML/CFT programs at financial institutions, including (i) the development of internal policies, procedures and controls; (ii) designation of a BSA or compliance officer; (iii) ongoing training requirements; and (iv) a robust audit or independent review function. The Act also introduced the requirement to file Currency Transaction Reports ("CTRs") on cash transactions over $10,000. Legislation enacted since the Bank Secrecy Act, including the USA PATRIOT Act, have added requirements to file reports on suspicious transactions ("SARs"), verify the identity of bank customers and to conduct enhanced due diligence on a subset of those customers—notably correspondent banks, private banking clients, foreign senior political officials and other customer categories that have been deemed higher risk. Most recently, the requirement to identify ultimate beneficial owners of legal entity customers has been added through regulation.

Criminal organizations move money through the financial system in many ways. They use all forms of finance including cash, ACH, wires, investments and trade finance—and now, even emerging technologies such as virtual currencies and person-to-person funds transmittal applications. They use shell companies to hide identities or to create the false impression of legitimate business activity. They use front companies and money mules to hide the real people behind the transactions. With so many varied and ever-changing techniques to move illicit funds, it is critical that financial institutions, law enforcement and banking regulators never become complacent or satisfied with yesterday's methods of identifying this activity.

It is also important to ensure that financial institutions are using their compliance resources efficiently and effectively. Under the current regime, banks like M&T are required to perform extensive evaluations of customers and transactions. We are required to carefully document every aspect of these evaluations and to compile large amounts of supporting documentation, even where it is determined that no

---

[2] The Clearing House has conducted a survey of its members that is intended to provide an empirical basis upon which to assess current BSA/AML/OFAC requirements. TCH expects to release the results of that survey shortly.

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

suspicious activity is present. This focus on documentation of that which is not suspicious results in a huge amount of resources devoted to satisfying the intense focus of our regulators to such matters, resources that could be used to further the mission of detecting illicit activity.

Each year M&T files thousands of SARs[4] and tens of thousands of CTRs.[5] However, feedback from law enforcement regarding the quality or usefulness of these filings is rare. At my institution, we receive post-SAR filing followup requests for information on a SAR (such as a subpoena or other legal process) from law enforcement about 5 percent of the time. Followup on CTR filings almost never occurs. Results of a survey recently conducted by The Clearing House indicate that our experience is not unique. In discussions with some law enforcement agencies, it appears that the lack of consistent agency policy or legislative authorization makes law enforcement reluctant to provide feedback on SAR filings, possibly due to concerns about the confidential nature of SARs, and there is no official mechanism through which to provide feedback.[6] Thus, it is difficult to know whether our filings provide law enforcement with leads that are of a "high degree of usefulness," as required by the statute. Therefore, we are compelled to calibrate our monitoring systems to the only tangible data we have—our decision to file a SAR. As a result, we fine-tune our systems to reflect our own work product, rather than to reflect law enforcement's priorities.

Let me give you an example of the resources M&T expends on its SAR filings. We use both automated and manual processes to monitor for suspicious activity, which trigger tens of thousands of alerts each year that are investigated further by AML compliance employees, who ultimately make a determination to either close out the alert or designate it as a case in need of further review. If an alert becomes a case, resources will then be devoted to investigating the case which, depending on the activity under investigation, could take anywhere from a few hours to a few weeks to conclude. Once an investigation is complete, we make a determination to either file a SAR or document our decision not to file a SAR. Of the thousands of cases we investigate, only 39 percent become SARs. However, each investigation must be meticulously documented to meet regulatory expectations. On average, an investigation consists of seven pages of narrative text and 50 attachments, which average 250–280 pages total, regardless of whether that investigation results in a SAR.[7]

This is why I believe it is essential for policymakers to reform the AML/CFT regime so that institutions are able to deploy resources more efficiently and improve efforts to provide useful information to law enforcement, national security and intelligence officials. This change should be founded on greater coordination and communication between the public and private sector. The U.S. Department of the Treasury should establish annual priorities for the regime, which could in turn form the basis for financial institution supervision and exams. Within this effort, it could also rationalize the broad reporting requirements implemented under the BSA, which would allow institutions to further tailor the resources they deploy to AML/CFT priorities. In addition, greater information sharing between law enforcement and financial institutions would allow institutions to calibrate their monitoring systems and to detect suspicious activity that is meaningful to law enforcement. Furthermore, institutions should have the legal and regulatory flexibility to explore innovative technological solutions to AML/CFT compliance, either individually or in concert with their peers. Finally, Congress should consider changes to beneficial ownership rules in order to facilitate more transparency and the collection of consistent data to prevent companies from obscuring their ownership, thereby providing them with the

---

[4] In 2017, U.S. depository institutions such as banks, thrifts, savings and loans and credit unions alone filed 916,353 SARs. Many more were filed by nonbank financial institutions such as money services businesses, casinos and securities firms. See "SAR Stats," available at: *https://www.fincen.gov/fcn/Reports/SARStats.* Accessed June 14, 2018.

[5] From 2012–2014, the average number of CTRs received per year by FinCEN was 15,283,950. See FATF Anti-money laundering and counter-terrorist financing measures, Mutual Evaluation of the United States, December 2016, pg. 54; available at: *http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.*

[6] Disclosure of the existence of a SAR to unauthorized persons may result in criminal penalties. 31 U.S.C. § 5322. While this prohibition should not apply to a communication between a bank that filed a SAR and law enforcement as they are both authorized persons, the strict nature of the SAR confidentiality rule leads some to err on the side of caution in the absence of explicit permission.

[7] Attachments to an investigation may include copies of account statements, results of internet and database searches on the customer and transaction counterparties, Secretary of State filings for legal entities and documents evidencing transaction reviews.

means to hide illicit proceeds. I will address each of these recommendations in the remainder of my testimony.

Treasury Should Set Priorities for, and Rationalize, the Regime

As I noted previously, The Clearing House recently surveyed its members to better understand the resources institutions are devoting to AML/CFT compliance in the United States. Of the 19 TCH members surveyed (with assets ranging from 50 billion to over 500 billion dollars), 17 institutions employ a total of over 14,000 individuals, with 14 institutions collectively spending nearly $2.4 billion on AML/CFT compliance. With all of these resources invested in compliance, 18 institutions reported that they collectively filed more than 640,000 SARs and 17 institutions indicated that they filed 5.2 million CTRs in 2017. Furthermore, a median of 14 respondents indicated some form of law enforcement contact (including subpoenas, national security letters or requests for SAR backup documentation) on only 4 percent of the SARs they filed in 2017, whereas 10 institutions reported hearing from law enforcement on roughly 0.44 percent of the CTRs they filed.

Institutions of all sizes are devoting substantial resources to AML/CFT compliance, yet, in the current regime, little feedback is provided to determine whether those efforts are useful or reflect law enforcement's priorities. Moreover, the absence of specific measures of effectiveness, has led some to focus on the auditability of procedures and level of documentation of decisions as an inexact proxy for effectiveness, which encourages financial institutions to invest heavily in activities that reduce criticism of records, rather than in activities aimed at identifying suspicious activity in innovative ways.

Furthermore, U.S. financial institutions often have more than one regulator examining their AML program, with each individual regulator having their own priorities and viewpoints. At M&T alone, we have five regulators that evaluate us for compliance with AML laws and regulations. This is why it is important for Treasury, working with law enforcement, to establish a process for prioritizing the matters investigated by financial institutions subject to the BSA. This prioritization effort would convene relevant public sector actors that are the end users of the BSA information financial institutions provide to the Government—notably law enforcement, national security and intelligence officials, regulators and other stakeholders, with the resulting priorities forming the basis for AML/CFT examinations at covered institutions. Such a process would further encourage banks to devote resources to activities that proactively address regime priorities, rather than focusing their resources on proxies like auditability and documentation. It would also ensure greater AML exam consistency across financial institutions and amongst examining agencies. I understand that FinCEN, a division of the Treasury Department, has begun to have these discussions with relevant stakeholders, an effort that should be encouraged and expanded.

In addition, the Treasury Department, in consultation with law enforcement and the Federal banking agencies, should conduct a review of the current BSA/AML reporting regime with the goal of de-prioritizing the investigation and reporting of activity of limited law enforcement or national security consequence to allow financial institutions to reallocate resources to higher value AML/CFT efforts. Analysis of how SAR data is actually used by law enforcement could lead to the streamlining and automation of data submissions, rather than the current highly manual and cumbersome reporting process for some types of suspicious activity. This review is possible because FinCEN has data that banks do not have—namely, information as to what SARs are accessed by law enforcement and at what frequency. Such a review could also investigate how to modernize, tailor and clarify BSA reporting requirements while increasing law enforcement feedback within the system. For example, the review may find that provision of data to law enforcement in a streamlined format, rather than the narrative format required by the SAR form, may actually be more useful as law enforcement increasingly uses modern tools to "data mine" the SAR database, rather than performing manual SAR reviews. Thus, a data-driven review of SAR usefulness may both enable institutions to better calibrate their monitoring system to provide law enforcement with higher value information and provide that information in a more efficient and useful manner. Again, I understand that FinCEN is working on such an analysis and I hope that the results will be shared with a broad group of constituents so that meaningful and workable changes can be identified and implemented.

The Public and Private Sector Should Exchange More Information

As this hearing is meant to focus on barriers to successful illicit threat identification and mitigation, it is important to highlight that one of the greatest barriers to an effective regime is the lack of communication between the public and private

sector—notably between law enforcement and financial institutions. I have already described how feedback from law enforcement with respect to SAR filings can help financial institutions to better target their transaction monitoring toward better identifying suspicious activity. Financial institutions can also use investigative data provided by law enforcement such as IP addresses, geographic locations, names of suspected foreign shell companies and other items to develop targeted leads on potential suspicious activity.

There are examples of this type of information sharing in the United States, but the examples tend to be ad hoc and not consistently applied across financial institutions.[8] For example, some law enforcement agencies and prosecutor's offices have held industry outreach conferences with select banks to share high-level information from recent cases as examples of certain typologies of illicit finance. FinCEN has issued periodic Advisories to notify financial institutions of high-level red flags associated with some kinds of criminal activity. FinCEN has also recently embarked on an effort to share more detailed information with some banks in the United States, through a program called "FinCEN Exchange." In addition, law enforcement agencies can seek information regarding specific AML/CFT suspects through the USA PATRIOT Act's 314(a) provisions and other legal means. However, there remains a need for greater and more routine sharing and collaboration between the industry and law enforcement to better address the illicit finance risks facing our country. More routine sharing of specific and actionable information to a broader set of financial institutions could improve the effectiveness of the entire regime. Expansion of 314(a) to allow broader secure and confidential sharing with participant banks, which should be able to voluntarily participate based upon their risk profile and individual circumstances, would facilitate this communication.

Financial Institutions Should have the Flexibility to Adopt Innovative Technologies

In addition to setting AML/CFT priorities, rationalizing regulatory requirements, and improving public-private sector information sharing, it is important for institutions of all sizes to be able to embrace the innovative technologies available to them to better detect and report on suspicious activity. We must be cognizant of the fact that money laundering happens at banks of all sizes with differing levels of resources and sophistication. We also know that illicit finance often moves between multiple financial institutions as criminal actors work to complicate and conceal the money trail. Therefore any effort to encourage technological innovation within the industry should be flexible enough for institutions of all sizes to investigate them further—whether through a shared utility model or as an individual investor.

Congress should explore whether expansion of the "safe harbor" language within Section 314(b) of the USA PATRIOT Act, which presently provides a legal pathway for financial institutions to share information on potential money laundering or terrorist financing investigations with each other in certain circumstances, could facilitate these efforts.[9] Explicitly allowing banks to share information with each other under 314(b) for the purpose of working to detect potential suspicious activity would help to ensure that such efforts do not encounter legal or regulatory hurdles to innovation.

Congress Should Pass Beneficial Ownership Legislation

Finally, I support Congressional efforts to establish a nationwide framework for the collection of beneficial ownership information by a trusted Government body and to provide that data to qualified financial institutions and law enforcement. During my time at M&T, my team has investigated instances where shell companies appear to have been used to attempt to obfuscate the real actors behind transactions to move funds secretly to illicit actors. Based upon discussions with law enforcement and former prosecutors, shell companies are routinely used for this purpose. While the new CDD rule requires banks to ask their legal entity customers to certify as to their ownership, banks cannot independently verify that the information provided

---

[8] The U.K.'s Joint Money Laundering and Intelligence Taskforce (JMLIT) and Canada's Project Protect are two international examples of such efforts. For more information on JMLIT, Project Protect and other public-private sector information sharing partnerships, see Nick J Maxwell and David Artingstall, The Role of Financial Information-Sharing Partnerships in the Disruption of Financial Crime, Occasional Paper, Royal United Services Institute for Defence and Security Studies, October 2017, available at *rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_artingstall_web_2.pdf.*

[9] Section 314b of the USA PATRIOT Act allows participant financial institutions to share information "regarding individuals, entities and organizations engaged in or reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering activities." This permission to share confidential information is known as a "safe harbor."

is accurate. A nationwide secure database of ownership information would be a useful investigative tool.

Conclusion

AML/CFT reform is needed to make the U.S. regime more effective and to allow institutions, like M&T, to redeploy or invest their limited resources in efforts and technology that will allow them to provide information that is of greater utility to law enforcement. I applaud the Subcommittee's interest in this important topic. Discussions such as these will assist in allowing banks to continue to support law enforcement's efforts to keep our communities safe and to cutoff the flow of illicit funds through the U.S. financial system. I thank you for the opportunity to testify and look forward to your questions.

PREPARED STATEMENT OF CHIP PONCY

PRESIDENT AND CO-FOUNDER, FINANCIAL INTEGRITY NETWORK, AND SENIOR ADVISOR, CENTER ON SANCTIONS AND ILLICIT FINANCE

JUNE 20, 2018

Chairman Sasse, Ranking Member Donnelly, and other distinguished Members of the Senate Banking Subcommittee on National Security and International Trade and Finance, I am honored by your invitation to testify before you today.

This hearing on money laundering and innovative techniques to counter such criminal activity comes at an important time. Today's criminal organizations continue to exploit the U.S. and international financial system to launder criminal proceeds and finance illicit activities ranging from terrorism to the proliferation of weapons of mass destruction. Such exploitation capitalizes on the growing complexities of the international financial system and weaknesses in institutional, jurisdictional, and global counter-illicit financing regimes. Some of these weaknesses stem from a failure to implement global standards designed in large part by U.S. leadership to combat crossborder money laundering and other financial crime. Other weaknesses stem from outdated approaches to combating these threats. Congressional attention and action is urgently needed to address these challenges.

In recent years, Congress has indicated interest in strengthening the U.S. anti-money laundering and countering the financing of terrorism (AML/CFT) regime to meet these challenges. Over the past year alone, several hearings in both the Senate and the House have focused on systemic reform to modernize U.S. efforts to combat money laundering and all forms of illicit financing activity. I am hopeful that my testimony today will assist this Subcommittee in supporting and accelerating these reform interests.

Such reform should be grounded in an understanding of how money laundering, financial crime, and corresponding AML/CFT regimes have evolved to become clear matters of national and collective security. Such reform should also be informed by an understanding of how criminal organizations and other national security threats continue to exploit the financial system to launder criminal proceeds and finance illicit activity. Such reform should close critical gaps in the U.S. AML/CFT regime, including by ending the creation of anonymous companies in the United States. Finally, such reform should encourage innovative approaches and capitalize on new technologies to buildupon and improve U.S. and global AML/CFT frameworks.

The United States has one of the most effective AML/CFT regimes in the world. Yet many of the global and systemic challenges to AML/CFT regimes abroad also confront our own AML/CFT regime. These challenges present opportunities for criminal organizations and other threats to launder money and finance illicit activities that undermine our collective security, the integrity of our financial system, and corresponding confidence in our markets. Our capability and willingness to address these challenges at home will substantially impact our credibility and capability in driving other countries to do the same—and in holding accountable those countries that fail to meet such standards. Given the increasingly globalized nature of organized crime and illicit finance, our AML/CFT reform efforts must consider these important ramifications.

My testimony today focuses on each of these points as follows:

- Section I summarizes the modern evolution of money laundering and financial crime and the growing importance of AML/CFT regimes in combating these threats to protect our collective security and safeguard the integrity of the financial system.

- Section II presents characteristics of money laundering, terrorist financing, and other financial crime and describes how these threats chronically exploit systemic challenges to financial transparency and accountability.
- Section III outlines reforms that Congress should pursue to modernize and secure a more effective and sustainable AML/CFT regime. Such reforms should capitalize on U.S. leadership that has guided and galvanized a common commitment to combating money laundering and financial crime across nearly all financial centers and jurisdictions over the past several generations.

My testimony draws in large part from prior testimony that I have provided before other Congressional committees and subcommittees considering these issues over the past 3 years. As with such prior testimony, I am grateful for the incredible dedication of my partners, colleagues, and friends at the Financial Integrity Network, the Center on Sanctions and Illicit Finance, the Treasury and across the U.S. Government, and in the global AML/CFT community—including the other expert witnesses who are testifying before you today. The primary basis of my testimony is the experience that I have gained in working with these experts and stakeholders to help shape and implement AML/CFT policy over the past 16 years in the U.S. Government, the international community, and the private sector.

I. The Modern Evolution of Money Laundering, Financial Crime, and the AML/CFT Regime

Since the initial adoption of the Bank Secrecy Act (BSA) almost 50 years ago—and particularly since the terrorist attacks of 9/11—money laundering, financial crime, and AML/CFT regimes have evolved dramatically. This evolution is fundamentally characterized by an expansion of money laundering and AML/CFT scope, stakeholder interest, and objectives. This evolution is also characterized by the growing complexity, importance, and globalization of money laundering and AML/CFT regimes.

Understanding this evolution, described in greater detail below, is critical to understanding how modern criminal organizations launder money and finance other illicit activity. Such an understanding also provides an essential basis for prioritizing and guiding AML/CFT reform efforts.

(i) Expanding substantive scope, stakeholder interest, and objectives

As described in greater detail below, the expanding scope, stakeholder interest, and objectives of money laundering, financial crime, and corresponding AML/CFT regimes is reflected by:

a. The expansion of money laundering predicate offenses to encompass virtually all forms of serious criminal activity;

b. The increasing reliance of sanctions compliance and broader risk management on effective implementation of AML/CFT regimes; and

c. The emergence of national security and financial integrity objectives of AML/CFT regimes.

a. Expansion of money laundering predicate offenses. Our AML/CFT regime, launched with the introduction of the BSA, initially focused on reporting bulk cash movements to assist in tax compliance, the criminalization of drug money laundering, and the detection and confiscation of drug trafficking proceeds. Through the expansion of predicate offenses, our AML/CFT regime now encompasses practically all serious criminal activity—including various forms of fraud, corruption, terrorist financing, sanctions evasion, and WMD proliferation achieved through the violation of export controls or smuggling.

This expanded scope has significant consequences for traditional AML risk management across our financial system, as these different types of predicates expose additional financial products, services, relationships, institutions, markets, and sectors to different kinds and degrees of illicit financing risk. It also expands the range of law enforcement agencies that rely upon financial information to pursue various criminal networks that launder their proceeds through our increasingly globalized financial system.

b. Increasing reliance of sanctions compliance and broader risk management on effective implementation of AML/CFT regimes. The scope of AML/CFT regimes has also expanded as sanctions compliance has increasingly relied upon and blended with AML/CFT risk management. It is often impossible to know whether any given financial account or transaction may involve a sanctioned party, activity, or jurisdiction without performing robust due diligence driven by AML regulatory requirements.

As sanctions programs have become more complex, their effective implementation relies upon more sophisticated development, integration, and application of underlying AML programs to assess and manage sanctions risk. Consequently, sanctions policy, targeting, compliance, and enforcement authorities—as well as sanctions compliance programs and officers in financial institutions—have become increasingly reliant upon and integrated into AML/CFT regimes and AML compliance programs.

This reliance presents challenges and opportunities for integrating the governance, implementation, and enforcement of AML/CFT regimes with sanctions compliance and risk management.

c. Expanding objectives of AML/CFT regimes. The objectives of AML/CFT regimes have also evolved, consistent with the expansion of such regimes' scope and stakeholder interests. Following the terrorist attacks of 9/11, Congress expanded the purpose of the BSA "to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism." While this expansive criminal justice, tax compliance, regulatory, intelligence, and counterterrorism set of objectives is more important than ever, it is also incomplete.

Protecting the integrity of the financial system has also become an essential objective in its own right. Such integrity is fundamental for the financial system to maintain not only the security of the customer assets it holds, but also the confidence of markets and the general public as an industry protected from criminal abuse. In addition to law enforcement and other investigative and intelligence authorities, financial institutions—together with the customers, markets, and global economy they service—are direct beneficiaries of AML/CFT regimes. Financial institutions are end users of BSA/AML recordkeeping and reporting, relying on such information to identify and manage all manner of illicit financing risk for purposes of protecting the integrity of the financial system.

This reality is evident in the way we talk about actions taken under various AML/CFT authorities—both under our own AML/CFT regime, and in concert with AML/CFT authorities abroad. Such actions are intended in large part to protect the integrity of the financial system.

Recognizing this expansive objective underscores the primary role of financial institutions in both implementing and informing our AML/CFT regime. It also underscores the importance of establishing robust public-private partnerships, including at policy and operational levels, to effectively implement and inform our AML/CFT regime.

Perhaps most importantly, AML/CFT regimes have evolved more broadly into a financial security regime, essential to protecting our national and collective security. The financial transparency and accountability created through AML/CFT regimes enable effective development and implementation of sanctions policies and other targeted financial measures to combat a growing array of national and collective security threats. Such transparency and accountability also generate financial information that intelligence and national security communities increasingly rely upon to identify and disrupt these threats.

(ii) Heightened complexity and importance

As criminal organizations, money laundering activities, and corresponding AML/CFT regimes have expanded across scope, stakeholder interest, and objectives, they also have become more complex and important. This is true for public sector authorities, the private sector, and the general public.

a. Heightened complexity of transnational crime and corresponding AML/CFT regimes. The heightened complexity of AML/CFT regimes has inevitably followed the globalization and increased sophistication and intermediation of the financial system and the criminal organizations that exploit it. This includes within and across financial products and services; banks, nonbank financial institutions, and designated nonbank financial businesses and professions; and countries, sub-national jurisdictions, and supra-national jurisdictions.

In combating various forms of illicit finance, AML/CFT authorities and financial institutions are increasingly challenged to understand and keep pace with these evolving complexities of the modern financial system. Such an understanding is required as a baseline for identifying and combating all manner of illicit finance that exploits the vulnerabilities presented by such a complex financial system.

The heightened complexity of AML/CFT regimes has also been driven by the globalization of criminal and illicit financing networks and the blending of illicit financing risk—including across money laundering, terrorist financing, sanctions evasion, bribery and corruption, proliferation finance, tax evasion, and state and

nonstate actors. Addressing such heightened complexity requires more specialized and integrated expertise across the core stakeholders of AML/CFT regimes. Such expertise, in turn, demands targeted and integrated training about how the financial system works, how illicit actors abuse it, and the particular roles and responsibilities that stakeholders must fulfill to effectively combat such abuse.

b. Heightened importance of transnational crime and corresponding AML/CFT regimes. As AML/CFT regimes have expanded and become more complex, they also have become more important—for law enforcement, national and collective security, and the integrity of the financial system itself.

The heightened complexity and globalization of criminal and illicit financing networks has made financial information more important than ever before to law enforcement agencies pursuing serious criminal activity. Federal law enforcement agencies have repeatedly testified that the BSA database is among the most important sources of information they have in combating various forms of serious and organized crime, from drug trafficking and fraud to tax evasion and terrorist financing.

In addition, the post-9/11 development and integration of CFT strategies and policies into the AML regime and the rise of transnational organized crime have attached clear national security importance to our AML/CFT regime. As sanctions and other national security authorities have become more reliant upon financial information and disruption in the post-9/11 era, the AML/CFT regime has become a crucial foundation for applying financial and economic pressure as an instrument of national and collective security. This is evident in the financial and economic pressure, isolation, and disruption campaigns the United States has led against al Qaeda, Iran, ISIS, North Korea, and rogue financial institutions such as Banco Delta Asia or Liberty Reserve. It is now difficult to think of any response to a national or collective security threat that does not involve a significant financial element reliant on implementation of AML/CFT regimes.

The pervasive rise of transnational organized crime has also emerged as a clear threat to our national security. This is most evident in our 2011 National Security Strategy to Combat Transnational Organized Crime, including Executive Order 13581. Quite simply, we now need national security authorities to complement traditional law enforcement authorities to combat this threat. Given the expansion of AML predicates across the full spectrum of transnational organized criminal activity, our AML/CFT regime has clearly become an integral part of protecting our national security, including through the use of national security authorities to attack criminal activities through the expansion and leveraging of AML/CFT regimes.

Finally, as discussed above, our AML/CFT regime is crucial to protecting the integrity of the financial system itself. This importance is underscored by the rise of cybercrime, identity theft, and other forms of fraud that increasingly and systematically target our financial institutions and our financial system as a whole.

(iii) Globalization of money laundering, financial crime, corresponding AML/CFT regimes, and the broader financial integrity and security mission

For the past three decades, the United States has led the globalization of AML/CFT regimes in regions and jurisdictions around the world, including with its partners in the G7, the G20, the Financial Action Task Force (FATF), nine FATF-Style Regional Bodies (FSRBs), the World Bank, the IMF, and the United Nations. This sustained effort and commitment has been grounded in the recognition of the growing transnational and ultimately global threat presented by an expanding range of money laundering and other illicit financing. This effort has also created a truly global framework essential for combating serious criminal activity, protecting our national and collective security, and safeguarding the integrity of the international financial system.

After 9/11, the global CFT campaign led by the United States became an instrumental factor in accelerating a global understanding of the importance of AML/CFT regimes to our collective security. Combating financial crime, protecting the integrity of the financial system, and promoting effective implementation of sanctions against threats to our national and collective security have since become central to Treasury's mission and to that of finance ministries around the world. Together with partner jurisdictions and organizations around the world, the United States has led a global commitment to expanding AML/CFT regimes and strengthening their implementation to advance these objectives.

This commitment is evident in the rapid evolution of the global counter-illicit financing framework. This framework continues to drive development and implementation of comprehensive jurisdictional AML/CFT, counter-proliferation, and financial

sanctions regimes. This framework, largely led by the work of the FATF, manages jurisdictional participation in conducting the following sets of activities:

- Developing typologies of illicit financing trends and methods;
- Deliberating counter-illicit financing policies and issuing global counter-illicit financing standards;
- Conducting and publishing regular peer review assessments of jurisdictional compliance with the FATF's global standards; and
- Managing follow-up processes that both assist jurisdictions and hold them accountable in implementing the FATF standards.

Through the FATF network of assessor bodies, the overwhelming majority of countries around the world are incorporated into this counter-illicit financing framework.

The global standards issued by the FATF and assessed through this global framework cover a broad range of specific measures to protect the integrity of the financial system from the full spectrum of illicit finance—including money laundering, terrorist financing, proliferation finance, serious tax crimes, and corruption. These global standards create a conceptual and technical roadmap for countries and financial institutions to develop the capabilities required to advance and secure the integrity of the global financial system.

Implementing the FATF global standards requires a whole-of-government approach in collaboration with the private sector, particularly financial institutions. It is a massive undertaking. And it is essential to combat transnational organized crime, safeguard the integrity of the financial system, and protect our national and collective security.

Peer review assessments over the past several years demonstrate that most countries have taken substantial steps toward implementing many if not most of the requirements covered by the FATF global standards. Collectively, this work represents a tremendous accomplishment in creating a firm global foundation for financial integrity and security, based on effective development and implementation of comprehensive AML/CFT regimes.

Nonetheless, these comprehensive jurisdictional assessments also reveal a number of deep-seated, systemic challenges to AML/CFT regimes. These challenges, discussed and addressed in the next two sections, are also evident from consistent typologies and cases of money laundering and illicit finance, as well as from U.S. enforcement actions taken against financial institutions in recent years.

II. Financial Vulnerabilities Exploited by Criminal Organizations and Other Collective Security Threats

Strengthening our AML/CFT system against money laundering and other financial crime requires an understanding of how such illicit activity is perpetrated. The details of such methods and schemes will depend on the particular form of financial crime and the criminal or other illicit organizations involved. This requires subject matter expertise across various types of illicit finance as well as various illicit actors and groups and the regions in which they operate. However, all forms of money laundering and financial crime exploit vulnerabilities in the financial system and in AML/CFT regimes. Many of these vulnerabilities represent challenges to financial transparency and accountability based on the evolution of the financial system and AML/CFT regimes as described in Section I.

In the sub-sections below, I will briefly outline characteristics of money laundering, terrorist financing, and other forms of illicit finance. I will then explain and provide examples of how these characteristics drive all manner of illicit financing to exploit vulnerabilities stemming from systemic challenges to financial transparency and accountability.

(i) Characteristics of money laundering, terrorist financing, and other forms of illicit finance

Criminal organizations generally launder money by placing, layering, and integrating the proceeds of their criminal activity into the international financial system and, ultimately, the global economy. Terrorist organizations may finance their operations through various criminal activities or noncriminally derived funds (*e.g.*, state sponsorship, charitable donations, or taxes on local populations under terrorist control), but they commonly exploit the financial system to efficiently move such funds in support of terrorist activity, actors, or networks. Both criminal and terrorist organizations escape detection through techniques that facilitate anonymity and obfuscate meaningful financial investigation into the source or destination of their funds. In addition, these organizations generally seek to create a perception of legitimacy

with respect to their financial transactions, laundered proceeds, and their beneficiaries.

These features of anonymity, obfuscation, and apparent legitimacy also commonly characterize other forms of illicit finance, including proliferation financing, sanctions evasion, and tax evasion.

Depending on the specific criminal activity and organization, money laundering and other forms of financial crime may assume any one or combination of a variety of particular methods or techniques. Some of these may be especially relevant to cash-based predicates (*e.g.,* structured cash placements by drug trafficking organizations). Others may be more prevalently associated with noncash-based predicates or schemes (*e.g.,* third-party wire transfers in a financial fraud scheme). More specific money laundering predicates or types of illicit financing may have more particular characteristics—such as the involvement of senior government officials or related parties (generally known as politically exposed persons, or PEPs) in significant corruption-related money laundering cases.

Effectively combating sophisticated financial crime networks today requires a significant investment to understand detailed methods and techniques associated with different illicit financing typologies employed by different criminal organizations and illicit actors. Targeted investigative, intelligence, and analysis resources are necessary to understand the financial operations of particular criminal, terrorist, or other illicit groups. As the scope, complexity, and importance of this work has grown, corresponding investments in AML/CFT regimes are required to address these needs.

Yet the general characteristics of money laundering and other financial crime described above drive all manner of illicit finance to exploit systemic challenges to financial transparency and accountability.

(ii) Exploitation of systemic challenges to financial transparency and accountability

Despite variances in specific money laundering and illicit financing methods, criminal organizations and other collective security threats consistently exploit vulnerabilities stemming from systemic challenges to financial transparency and accountability. These challenges emerge largely from the complexities of the international financial system discussed in Section I above. They also emerge from weaknesses in the implementation or approach of AML/CFT regimes.

Three particular financial transparency and accountability vulnerabilities chronically exploited by all manner of illicit finance include:

(a) Anonymous companies created in the United States and other jurisdictions that fail to adopt meaningful beneficial ownership disclosure and maintenance requirements for legal entities;

(b) Financial intermediation coupled with inadequate AML/CFT coverage of the financial system; and

(c) Information-sharing constraints that prevent financial institutions and counter-illicit financing authorities from identifying, pursuing, and capturing illicit financing networks and assets increasingly spread across multiple financial institutions and jurisdictions.

These vulnerabilities, and examples of how they are exploited by criminal organizations and other illicit financing actors, are briefly discussed below.

a. Anonymous Companies

For far too long, anonymous companies created in the United States and abroad have masked and enabled terrorist organizations, human traffickers, drug smugglers, and proliferators of weapons of mass destruction to access and exploit the international financial system. The range of abuse does not end there. Money laundering, tax evasion, grand scale corruption, sanctions evasion, fraud, and organized crime at large are regularly perpetrated or enabled on a worldwide basis through the systematic creation and use of anonymous legal entities. Even as the United States continues to enhance and expand its financial tools and power to combat money laundering and various national security threats, these efforts are increasingly undermined by such exploitation of anonymous legal entities.

The continual creation of such legal entities right here at home may represent the most dangerous systemic vulnerability that the United States presents today to the global counter-illicit financing mission. Closing this vulnerability requires congressional action to reform company formation processes in the United States. In accordance with global standards that our country has urged others to adopt, such reform efforts must generally require the collection, maintenance, and disclosure of

accurate beneficial ownership information for certain legal entities created under laws in the United States.

Beneficial ownership requirements for legal entities will provide immensely valuable information for law enforcement and other counter-illicit finance authorities. As elaborated below, an abundance of testimony and evidence over the past several years demonstrates that investigations of legal entities implicated in all manner of criminal activity are all too often frustrated by a lack of meaningful beneficial ownership information.

In certain higher risk scenarios, financial institutions should verify the beneficial ownership information obtained from their legal entity customers through independent corroboration of the beneficial owner's status. This presents significant challenges for financial institutions that lack independent sources of information about their legal entity customers. To assist financial institutions in conducting such verification, countries should demand beneficial ownership information as a condition for granting legal status to those entities formed under their authorities. For these reasons, the FATF global standards clearly require jurisdictions to impose beneficial ownership disclosure and maintenance requirements for legal entities formed under their authorities. Yet many jurisdictions fail to require companies to disclose their beneficial ownership as a condition of obtaining or maintaining their legal status. Of those jurisdictions that do require such disclosure, few have meaningful verification or enforcement processes to ensure the credibility of the beneficial ownership information they collect.

Cases demonstrating criminal and other illicit abuse of such anonymous legal entities created in the United States and elsewhere are all too common. For decades, law enforcement and others have presented many of these cases to Congress as a basis for enacting company formation reform. Significant cases involving such abuse have been listed in various testimonies and preambles to draft legislation, including in a hearing earlier this year by the House Financial Services Committee. My own testimony in that hearing included prominent reporting of the following cases of criminal organizations laundering funds or financing illicit activity through anonymous legal entities created in the United States:

- Members of Venezuela's cabinet used an Andorran bank to launder $2.5 billion in bribes. The money was concealed in 37 accounts under the name of Panamanian shell companies before being moved to tax havens such as Switzerland and Belize. *(El Pais)*
- Between 2011 and 2014 well-connected Russians used 5,140 shell companies that had accounts with 732 banks in 96 countries to move $20.8 billion out of Russia. The anonymous companies signed "loan agreements" between themselves and used fake "defaults" to obtain orders from corrupt courts that allowed them to transfer the money out of Russia. *(Organized Crime and Corruption Reporting Project)*
- Reuters reported that 118 U.S.-based shell companies in 25 States served as "phantom companies" for an Armenian crime ring whose members posed as medical providers and billed Medicare for than $100 million.
- Convicted cocaine trafficker Darko Saric used the names of associates to register at least four companies in Delaware. Profits from cocaine smuggled from South America to Europe were channeled through those shell companies and were then used to invest in businesses in Saric's native Serbia. (Organized Crime and Corruption Reporting Project)
- According to the Panama Papers, a single Nevada firm formed over 2,400 shell companies, all headquartered at the same residential address and used by customers to evade over $30 million in Federal taxes.
- Corrupt FIFA official Chuck Blazer is alleged to have used five shell entities, registered in the United States and the Cayman Islands, to hide the bribes he extracted from companies seeking to do business with the global soccer association. Among other frauds, Blazer, hiding behind a shell company, would make himself the beneficiary of "consulting agreements" in order to receive illegal commissions on broadcasting rights. *(EDNY Indictment)*
- In a $6 million human trafficking scheme, a Moldovan gang ran employment companies that supplied hundreds of foreign nationals to hotels, resorts, and casinos across the United States. The gang hid their real identities behind a web of shell companies registered in Kansas, Missouri, and Ohio. *(International Bar Association)*
- Kingsley Iyare Osemwengie of Las Vegas, Nevada, was part of a sophisticated drug trafficking organization that diverted legitimate medicine such as oxycodone into the black market. He laundered profits through six bank

accounts, including those for two Nevada shell companies: High Profit Investment and First Class Service. *(The Oregonian)*

- Teodoro Nguema Obiang Mangue, the vice president of Equatorial Guinea, was convicted of money laundering and embezzlement of more than $100 million, which was hidden in California-based shell companies. *(Time)*
- On June 17, 2017, the U.S. Department of Justice reported that Malaysian sovereign wealth Fund officials and their associates diverted more than $4.5 billion using fraudulent documents and representations to launder funds through a series of complex transactions and shell companies with bank accounts located in the United States and abroad. Among other purchases, conspirators used a New York shell company, headquartered at an accommodation address, to purchase a $4.5 million apartment. The shell company was itself a wholly owned subsidiary of a private wealth-management firm, so that the transaction was completely anonymous. *(DOJ Complaint)*
- As widely reported last year, hackers allegedly tied to North Korea stole $81 million from accounts maintained by the Federal Reserve Bank of New York for the Central Bank of Bangladesh. The hackers used the SWIFT messaging system to send more than three dozen fraudulent money transfer requests for the benefit of invented individuals and entities in the Philippines, who then laundered it through casinos. *(Reuters)*
- The Islamic Republic or Iran Shipping Lines, or IRISL, a state-owned enterprise, has used a web of shell companies stretching across Europe and Asia to obscure the true ownership of its fleet by changing the country of registration and names of companies and owners in order to evade sanctions. *(The New York Times)*
- Over a period of 6 years, Zhongxing Telecommunications Equipment Corporation (ZTE) engaged in a scheme to ship more than 20 million U.S.-origin items to Iran. ZTE used multiple avenues to evade U.S. sanctions and export control regulations, including establishing shell companies and falsifying customs documents. *(U.S. Department of the Treasury)*
- Room 2103, Easey Commercial Building, Wan Chai, Hong Kong, is the registered office of Unaforte Limited, a company accused by the United Nations of violating sanctions North Korea. When CNN visited the office, it found neither Unaforte nor its listed company secretary, Prolive Consultants Limited. Instead, room 2103 was home to a seemingly unrelated company: Cheerful Best Company Services. *(CNN)*
- A 2017 asset forfeiture suit against Velmur Management, a Singapore-based "real estate management firm" with no physical office space, shows how a layered network of shell companies with access to the U.S. financial system was used to allow North Korea to buy $7 million in petroleum from a Russian company. Velmur would receive payments made on behalf of North Korea and transfer them to the Russian seller. *(DOJ Complaint)*
- On August 22, 2017, OFAC designated Mingzheng International Trading Limited, a China- and Hong Kong-based front company, for its involvement in evading sanctions and laundering funds on behalf of North Korea.
- Thompson Reuters reported that former Ukrainian Prime Minister Pavlo Lazarenko, once listed as the 8th most corrupt leader in the world, ultimately controlled a shell company that, itself acting through other shell companies, owns an estimated $72 million in real estate in Ukraine.
- Jose Trevino Morales, the brother of two kingpins of Mexico's infamous Zetas drug cartel used their main shell company, named "Tremor Enterprises" and registered in Texas, to launder at least $16 million over the course of 3 years. *(CNBC)*
- Mihran and Artur Stepanyan used several anonymous companies to distribute over $393 million in drugs and launder the profits. *(U.S. Department of Justice)*
- In 2014, Business Insider reported that Semion Mogilevich, listed on the FBI's list of the Ten Most Wanted Fugitives, used a vast network of Russian shell companies to cheat the U.S. stock market and steal over $150 million from investors in the United States and overseas.

These and numerous other high-profile cases present a strong argument against allowing the ongoing creation of anonymous legal entities, whether in the United States or abroad.

The far more powerful argument lies in the cases we do not see.

For decades, law enforcement officials have testified before Congress and other authorities about their consistent inability to pursue high priority cases involving anonymous legal entities that present a dead end for investigators. Similarly, sanctions authorities and compliance officers in financial institutions around the world struggle to track the myriad of shadow companies ultimately created and controlled by designated national and collective security threats.

For these reasons, it is entirely unclear just how pervasive the exploitation of anonymous companies is. What is clear is that the ability to pursue investigations implicating such companies is severely limited by incorporation practices in the United States and other jurisdictions. What is also clear is that this limitation contributes to the broader inability of law enforcement to identify and pursue the overwhelming majority of illicit financing activity. Various estimates of money laundering, testimony from law enforcement, and the official recognition of organized crime as a national security threat all demonstrate that we may be losing the battle against transnational organized crime and illicit finance in the criminal justice domain.

To reverse this sobering trend, we must assist rather than hinder the efforts of law enforcement and other counter-illicit financing authorities responsible for identifying, tracking, and tracing illicit actors that access and exploit the international financial system and global economy. Congressional legislation to end the creation of anonymous legal entities in the United States through company formation reform is essential to do this.

b. Financial Intermediation and AML/CFT Coverage of the Complete Financial System

Financial transparency is complete only to the extent that it applies across the entire financial system. All financial institutions—including nonbanking financial institutions such as broker dealers, investment advisors, and money services businesses—should be subjected to effective AML/CFT regulation, examination, and supervision. In addition to nonbank financial institutions, certain industries that can operate as *de facto* financial institutions or that facilitate access to financial services for their customers may present systemic vulnerabilities to illicit finance. Such industries include casinos, real estate agencies, dealers in precious metals and stones, lawyers, accountants, and trust and company service providers.

Failure to extend meaningful AML/CFT regulation to these nonbank financial institutions or vulnerable industries can allow illicit financing networks to obtain the financial services they need without detection. Once illicit actors gain access to any part of the financial system, the highly intermediated nature of the system facilitates their access to other parts, including by sector or geography.

Any unregulated or under-regulated financial sector or vulnerable industry also puts more pressure on those sectors that are regulated. It is much more difficult to detect illicit financing risks that are intermediated through another financial institution or through a customer or account that represents unknown third-party interests. Correspondent relationships with unregulated financial institutions or vulnerable industries that lack AML/CFT controls allow criminals to access even well-regulated financial institutions through the back door.

For this reason, correspondent relationships are generally considered high risk under FATF global standards, even between financial institutions that are well-regulated for AML/CFT.

Correspondent relationships with financial institutions that lack AML/CFT regulation may be prohibitively high risk. The same may also be true of accounts with businesses from other vulnerable industries that lack AML/CFT regulation.

In light of these concerns, FATF global standards direct countries to extend AML/CFT preventive measures across all financial sectors and vulnerable industries, including the legal and accounting professions. Covering all of these sectors and industries can challenge considerable political interests and entails substantial costs. As a result, many countries, including the United States, lack full AML/CFT coverage of their financial systems or vulnerable industries. These gaps in coverage put more pressure on banks and other sectors that are covered and present systemic challenges to financial transparency.

Cases demonstrating criminal exploitation of these systemic vulnerabilities through financial intermediation are also common, including those involving unregulated gatekeepers such as law firms holding escrow accounts for underlying client interests. A particularly prominent case in recent years is the civil forfeiture action involving the 1Malaysia Development Berhad Sovereign Wealth Fund (1MDB). Founded in 2009 by Prime Minister Najib Razak, 1MDB was created as a development fund to boost Malaysia's economy. However, a multinational investigation involving the United States Department of Justice indicates that high-level officials

at 1MDB and their associates misappropriated more than $3.5 billion from the development fund between 2009 and 2015.

In this case, law firms provided relatively anonymous channels for laundering a significant portion of misappropriated funds. Between approximately October 21, 2009, and October 13, 2010, 11 wire transfers totaling approximately $368 million were sent from a shell company account in Switzerland to an Interest on Lawyers Trust Account (IOLTA) held by a prominent global law firm headquartered in the United States. Participants in the scheme then withdrew funds transferred to the IOLTA, which were then used to purchase assets and invest in business interests for their personal benefit. Purchases included luxury real estate, a Beverly Hills hotel, a private jet, and a major Hollywood motion picture.

In this case, criminals were able to launder money through a law firm not subject to the AML requirements applicable to the financial services industry. Through IOLTA accounts, members of the 1MDB scheme could do an end-run around customer due diligence and suspicious activity reporting requirements, bringing criminal proceeds into the United States through a *de facto* back door correspondent. To decrease these risks, gatekeeper accounts held for the benefit of third parties (such as IOLTAs) should be required to comply with basic AML requirements such as CDD and AML programs, in accordance with global standards.

c. Information-Sharing Constraints

Illicit financing networks, like the business of most enterprises, almost always implicate more than one financial institution. Whether in the process of raising, moving, using, or laundering funds associated with illicit activity, such networks almost invariably transact across multiple financial institutions. For the illicit financing networks of most pressing concern, transactions also often cross multiple jurisdictions. Identifying, tracking, and tracing these networks therefore depends critically upon information-sharing across financial institutions and across borders.

FATF global standards require or encourage countries and financial institutions to share information in many ways. However, implementation of such information-sharing measures is routinely constrained or prohibited by data protection, privacy, or business interests, or by liability concerns associated with these interests. Many counter-illicit financing professionals in governments and in financial institutions consider data protection and privacy to be the "new bank secrecy" that was the genesis for much of interest in creating the FATF almost three decades ago.

The systemic challenge posed by these information-sharing constraints is perhaps most evident in the risk management programs of global banks and large financial groups. FATF global standards direct countries to require such banks and financial groups to develop risk management programs that cover their entire enterprise. The wide scope of these programs is deliberately aimed at identifying and addressing illicit financing risks across all branches and affiliates of the bank or financial group, wherever located. Yet data protection, privacy, and other restrictions in many countries prohibit such banks or financial groups from sharing much of the information that is relevant or even essential to such enterprise-wide risk management programs. These restrictions apply even when the information sought is intended to be kept entirely within the financial group's enterprise.

Even more problematic for these institutions, information-sharing requirements and prohibitions from different countries can conflict with one another, making it impossible to comply with the laws or expectations of different financial centers in which global banks and financial groups operate.

Information-sharing challenges associated with financial intermediation and illicit finance are not limited to cross-border scenarios or to risk management programs. Even within jurisdictions, many of the same constraints prevent financial institutions from sharing information that can be critical in identifying or addressing illicit financing risks. This presents opportunities for countries, including the United States, to begin addressing these challenges through domestic information-sharing enhancement processes, in partnership with their financial institutions.

The sensitivity of financial information and the legitimate interests behind data protection and privacy raise important considerations for policymakers in determining how best to address these information-sharing challenges. Although more work is needed to better understand these challenges and how best to overcome them, it is clear that the lack of proactive or even reactive information-sharing between and among financial institutions presents a systemic challenge to financial transparency.

It is also clear that criminal organizations and actors exploit or benefit from these information-sharing weaknesses to launder substantial amounts of money. The Madoff Ponzi Scheme securities fraud case exemplifies how poor information-sharing creates blind spots where money launderers can act for years without

consequence. Between 1986 and 2008, one of the largest global banks headquartered in the United States maintained accounts for Madoff's company and invested proprietary and customer funds in derivative securities products based on Madoff's own fund. Due to legal information-sharing ambiguities, a lack of formal policies and procedures, and a stove-piping of due diligence functions, the bank's individual lines of business, geographic regions, and compliance units failed to effectively communicate with each other. Thus, while individual branches, compliance officers, and executives understood that their customer could be orchestrating a multi-billion dollar international fraud scheme, either this information would not be shared with other offices or, when sharing occurred, the offices and personnel who received this information would not act upon it.

As with the examples provided above demonstrating criminal exploitation of other systemic transparency challenges, numerous other cases reflecting criminal exploitation of information-sharing barriers exist. These cases collectively show that criminal organizations and other illicit actors—regardless of their specific methods and characteristics—will continue to launder money and perpetrate other financial crimes by exploiting systemic challenges to financial transparency and accountability.

III. Congressional Action Required To Encourage Innovation and Enhance the Effectiveness and Sustainability of AML/CFT Regimes

The evolution of money laundering, financial crime, and AML/CFT regimes—coupled with the consistent criminal exploitation of systemic vulnerabilities described in Section II—provides a clear basis and direction for modernizing and reforming AML/CFT regimes. Such reform should fundamentally encourage innovation to enhance the effectiveness and sustainability of AML/CFT regimes in combating the full range of illicit financing activity and actors. In the United States, these efforts should include Congressional action amending the BSA.

In a hearing before the House Financial Services Subcommittee on Terrorism and Illicit Finance last November, I outlined a comprehensive approach for Congress to lead such BSA modernization and reform. My testimony offered detailed recommendations for Congress to consider in developing legislation.

These recommendations were broadly guided by the following three fundamental principles of AML/CFT reform:

- Promote more complete, effective, and efficient financial transparency, including by facilitating systemic reporting and sharing of information at a lower cost to financial institutions;
- Exploit such financial transparency and information more effectively and consistently by investing in targeted financial investigative and analytic capabilities; and
- Create an inclusive and clear management structure that empowers Treasury to govern the ongoing development and application of our expanded AML/CFT regime.

In accordance with these three fundamental principles of AML/CFT reform, my recommendations for congressional action may be summarized as follows:

1. Expand the objectives of the BSA to explicitly include protecting the integrity of the international financial system and our national and collective security.
2. Swiftly enact company formation reform to require the systemic reporting and maintenance of beneficial ownership information for legal entities created or doing business in the United States pursuant to an effective and workable framework.
3. Restructure and enhance financial investigative expertise at Treasury, including with respect to the Criminal Investigative Division of the Internal Revenue Service.
4. Provide protected resources to law enforcement, the intelligence community, and counter-illicit financing targeting authorities to pursue illicit financing activity and networks.
5. Direct Treasury to enhance financial transparency in a methodical, systematic, and strategic manner that: (i) addresses longstanding and substantial vulnerabilities in our financial system; and (ii) pursues reporting obligations based on straight-through processing that leverages new technologies, provides more bulk data for counter-illicit financing authorities, and ultimately reduces burdens on financial institutions.
6. Clarify, expand, and strengthen, information-sharing between and among financial institutions and governmental authorities under Section 314 of the

USA PATRIOT Act to encourage the broadest innovation and application of new technologies to combat illicit finance.

7. Direct and provide resources for Treasury to strengthen, expand, institutionalize, and lead consultations with the AML and broader counter-illicit financing community—including financial sectors and other industries covered by AML/CFT regulation—in establishing and implementing priorities for U.S. AML/CFT policy.

These recommendations are discussed in detail in my prior testimony before the House Financial Services Subcommittee on Terrorism and Illicit Finance. In addition, my testimony before the Senate Committee on the Judiciary in February earlier this year provides a detailed explanation and proposal for company formation reform. This proposal would preserve effective and pragmatic company formation processes in the United States while addressing the national security threat presented by anonymous companies through beneficial ownership collection and reporting requirements.

The urgency and importance of such reform is grounded in an understanding of the expanding role that our AML/CFT regime plays in protecting our national security and financial system from an expanding range of complex threats. We must be clear-eyed about the resources required to advance and protect such complex and important interests. We must also be attentive to the fair distribution of costs and responsibilities across the beneficiaries of our AML/CFT regime—including AML/CFT and national security authorities, financial institutions and other vulnerable industries, the customers they service, and the general public. And we must focus on directing our AML/CFT policies and resources in a manner that drives efficiency and effectiveness. Congressional action and leadership is essential to securing interests.

Thank you for time and consideration of these issues. I look forward to any questions that you may have.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN SASSE FROM DENNIS LORMEL

Q.1. What incentives do financial institutions have to develop innovative AML techniques and consult typologies to stop human trafficking and fight MS–13? Are financial institutions ever punished for leveraging these techniques? For example, could a regulator punish a financial institution that found that human traffickers were using their services because the financial institution did not find the criminal activity earlier? How can this issue be fixed?

A.1. The questions you pose above buildupon each other. I will address each in progression. However, I'd like to first set the stage with a broad overview of the primary issue central to each question. Financial institutions are faced with regulatory requirements and regulatory expectations. What is required and what is expected or perceived to be expected often places financial institutions in precarious situations. From my perspective, that places financial institutions in the position of being less proactive and less willing to be innovative. As I frequently state in training I provide, the regulations are written in black and white. However, the interpretation or perceived interpretation of the regulations can be extremely gray. What is required and what is expected can become blurred. As a result, financial institutions are less inclined to be innovative. Regulators do not provide leadership or real guidance. Their response is usually that it is up to the financial institution to manage their risk and to have an anti-money laundering (AML) program that is reasonably designed to identify suspicious activity. That poses the question of how do you define "reasonably designed." That is where requirements and expectations tend to become more subjective. In addition to the issue of regulatory requirements versus regulatory expectations, there could be a significant cost consideration for developing and implementing innovative technologies.

Regarding incentives to develop innovative technologies and typologies to identify human trafficking and fight MS–13, incentives are outweighed by real or perceived regulatory expectations. We need to distinguish between human trafficking and the fight against MS–13. MS–13 is one of the most notorious street gangs in the Western Hemisphere. They are involved in a myriad of criminal activities. Among their criminal activities, MS–13 is engaged in human trafficking, especially sex trafficking involving young women from the Northern Triangle of Central America including the countries of El Salvador, Guatemala and Honduras. Unfortunately, human trafficking is a much broader problem than the trafficking activities involving MS–13. Financial institutions are more inclined to look at the broader human trafficking issue, without specific focus on MS–13. Regardless, financial institutions should be monitoring for touch points they may have to facilitate

human trafficking and activity involving MS–13. AML compliance professionals are extremely dedicated and committed to disrupting human trafficking and transnational criminal activity. One incentive AML professionals share, on a more personal level, is doing the right thing. From an institutional level, incentive should be to ensure your institution maintains an AML program reasonably designed to identify and report suspicious activity. Financial institutions serve as facilitation tools or detection mechanisms. In detection, they protect the integrity of their institution. In facilitation, they risk reputational and financial harm. Innovation, such as targeted monitoring, where you identify specific typologies, and set monitoring rules to specific typologies can enhance the hit rate of identifying suspicious activity regarding human trafficking. This is in addition to the baseline transaction monitoring. Unfortunately, there is little incentive for financial institutions to develop such proactive measures.

With respect to if financial institutions are ever punished for leveraging these techniques, the answer goes back to regulatory requirements versus regulatory expectations. I'm not sure I would characterize the concern of financial institutions about being punished as opposed to being questioned or second guessed and potentially becoming the subject of regulatory action because the technology upgrade either alerts more or less transactional activity as being potentially suspicious. One of the concerns here, again either real or perceived, is that the regulators would want the financial institution to run both the old technology and the new technology side by side to assess why more or less transactional activity gets flagged as potentially suspicious. In addition to regulatory concern, this would present the financial institution with additional cost and resource requirements, which could be prohibitive.

This leads to the next part of your question as to whether a regulator could punish a financial institution for identifying the human trafficking activity they facilitated earlier. Real or perceived, the regulatory expectation is that the regulators would take an adverse action. The real issue is whether the earlier transactional activity was adequately monitored and the financial institution had a reasonably designed AML program. It would appear logical that enhanced technology would improve transaction monitoring that the financial institution should be credited for. Unfortunately, even if the financial institution was credited for the enhanced technology, they would be expected and/or required to take remedial action to identify the earlier transactions that were missed. Thus, taking innovative steps and enhancing technology in this scenario serves as a deterrent and not an incentive.

Finally, how can this issue be fixed? In my view, this will require the regulators to provide leadership and/or guidance in incentivizing innovation and technology enhancements and working with financial institutions who strive to improve their AML programs. Where remediation is required to identify the earlier missed transactions, it should be done in a manner less detrimental than is currently experienced, unless the financial institution was not acting in a reasonable manner.

Q.2. Do smaller financial institutions have sufficient incentives and resources to use artificial intelligence technology? What can be

done to make it easier for smaller financial institutions to use such technology?

A.2. Much like described in the above responses, from an AML perspective, there is little or no incentive for smaller financial institutions to take steps to enhance their technology. From the cost and resource perspective, it's even more prohibitive and challenging for smaller financial institutions to be innovative. Incentives must be developed to encourage financial institutions, large and small, to become more innovative.

This leads to another industry-wide AML vulnerability. In part, because of real or perceived regulatory expectations, financial institutions tend to be more conservative and predictable. Bad actors, who are proficient in gaming the system and identifying systemic vulnerabilities, exploit those institutional vulnerabilities to facilitate their illicit activity. This is exacerbated by the fact that AML programs and fraud detection are inherently reactive. We must do more to become innovative and proactive. This requires more forward thinking that should be spurred on through meaningful incentives.

Q.3. What would it look like for a Federal AML regime to better prioritize particular law enforcement targets? What—if any—AML priorities should be de-emphasized? How could a system still ensure that a basic level AML competence was met so that still-important law enforcement priorities did not fall through the cracks?

A.3. As with your first group of questions, let me respond first, more broadly, and then more specifically to each related question. There is no easy answer to better prioritizing or de-emphasizing crime problems. You need to assess this from both the law enforcement and financial institution perspectives. From the law enforcement perspective, crime problems must be prioritized at a national level from a program perspective and at the local or grass roots level from the local or grass roots problems encountered in that jurisdiction. Criminals and crime problems evolve. Crime problem surveys or assessments must be conducted at the national and local or grass roots levels in order to monitor current and emerging crime trends. These surveys or assessments cannot be static and must be ongoing to better identify emerging trends. At the financial institution level, financial institutions must conduct ongoing risk assessments to assess their institutional risk and to identify potential touch points with national and local or grass roots crime problems and priorities. Risks and potential criminal touchpoints will be institution specific in accordance with an institutions customer base, geographic footprint, and product and service offerings. Financial institutions should be familiar with the general law enforcement crime problem priorities at the national and local or grass roots level. In terms of prioritizing law enforcement crime problem priorities, each law enforcement agency has different or similar priorities in accordance with their investigative jurisdiction and mandate. The major national priorities are terrorism, drugs, and human trafficking. In my experience, every crime problem, which goes beyond terrorism, drugs and human trafficking, other than violent crimes, all have elements of fraud and require money laundering. Thus, in my experience, fraud and money laundering

are linked together and are ingrained in all such criminal activity or predicate offenses. Financial institutions not only need to be familiar with relevant crime problems but also, importantly, the facilitation tools used in furtherance of such criminal activities. Included as facilitation tools are shell companies (beneficial ownership), the internet, electronic mechanisms, informal and illegal money remitters, correspondent banks and other facilitation tools.

It is incumbent that law enforcement, at all levels, and financial institutions establish, and maintain sustainable partnerships and working groups to share information and to understand the crime problems and law enforcement priorities, at the national and local or grassroots levels. In working with law enforcement, financial institutions should develop typologies for crime problems that are more specific to their institutional risk. Such typologies should be used for targeted monitoring initiatives and to enhance baseline transaction monitoring.

With respect to a Federal regime to better prioritize particular law enforcement targets, it would be extremely challenging and unproductive to develop a viable single national regime. This is due to the number of law enforcement agencies, varying jurisdictions and priorities and how these crime problems would touch financial institutions. The bottom line here is there can be no one size fits all policy, its contingent on risk, which impacts law enforcement agencies and financial institutions differently.

De-emphasizing AML priorities cannot be uniform across the financial services industry. De-emphasis of AML priorities should be left to the discretion of each financial institution on a risk-based assessment.

In terms of law enforcement priorities falling through the cracks with financial institutions' AML programs, I do not consider that as a problem or concern. Overall, law enforcement publishes crime problem priorities through their websites and outreach programs. As I mentioned earlier, it is incumbent that law enforcement and financial institutions establish partnerships and working groups to share information and better understand crime problems and systemic vulnerabilities. There are a number of national and grassroots working groups that serve as great models for success. An example at the national level includes the FBI's Terrorist Financing Operations Section (TFOS), national working group that they refer to as the Bank Security Advisory Group (BSAG). It involves a number of financial institutions meeting bi-annually with representatives of TFOS, regarding terrorist financing and through ongoing information sharing to develop typologies. An example of a local or grassroots working group is monthly meetings held by the Northern Virginia SAR (suspicious activity reports) Review Team. The SAR Review Team holds monthly meetings to discuss typologies and crime problems specific to the local Northern Virginia regional area. These are two examples of many such working groups. It would be very difficult, if not impossible, to template such groups. They need to be specific to the investigative mandate of the law enforcement side and the risk or touch points to involved financial institutions.

Q.4. One potential hurdle to creating an effective feedback loop between law enforcement officials and financial institutions is that

law enforcement officials are reluctant to share information about ongoing investigations.

Is that a legitimate concern that should prevent law enforcement officials from sharing information with financial institutions?

A.4. I am a huge proponent for developing consistent and broad feedback mechanisms. When I ran the FBI's Terrorist Financing Operations Section, I frequently met with then FinCEN Director James Sloan to develop viable and consistent feedback mechanisms. We were always confronted with a number of impediments to set up a consistent and broad feedback mechanism. That said, impediments should not be an excuse to develop meaningful feedback mechanisms.

There are legitimate concerns regarding law enforcement sharing information about ongoing investigations. If the investigations involve grand jury material, that information cannot be shared during an ongoing investigation. Likewise, any classified information developed during an investigation cannot be shared. Depending on the sensitivity of an investigation there could well be safety and security issues for law enforcement personnel, particularly in undercover scenarios or in situations involving confidential informants or cooperating witnesses. In situations where information could be shared or feedback provided, consideration should be given to doing so. In most situations involving ongoing investigations, it would be more likely not appropriate to share information.

Q.4.a. How could those concerns be mitigated?

A.4.a. For the most part, as explained in the prior response, these concerns cannot be mitigated. Where there could be room for information sharing or feedback could be in situations where indictments or convictions or other legal process has been issued and information is in the public record through court filings. The fact a SAR was filed should not be disclosed but information and evidence developed as a result of the SAR filing could be in the public domain. In such cases, feedback should not be a problem other than investigative resource considerations.

Q.4.b. Even if law enforcement officials could not provide feedback about SARs relating to ongoing investigations, could they at least provide feedback about SARs relating to completed investigations?

A.4.b. Feedback regarding completed investigations should result in fewer impediments and could be more viable. However, there are certain considerations to take into account. First is how time consuming might this be and does law enforcement have the time to provide such feedback or are they dealing with other matters that must be prioritized? Hence, are they legitimately lacking the capacity to provide feedback? This impediment should not be a consistent issue. The greater challenge is that the investigation could have gone on for one or more years and the feedback may no longer be relevant or as relevant or law enforcement does not keep track of the importance of SARs at that point in time.

Q.4.c. What—if any—other mechanisms should be developed to improve the feedback loop between law enforcement officials and financial institutions?

A.4.c. At the national level, law enforcement and FinCEN should assess how to develop a consistent feedback mechanism. In speaking to officials at the FBI, I understand the Financial Crimes Section in the Criminal Division, is looking at this issue. What should be noted here and could be modeled after are the various public private partnerships, working groups and crime problem specific initiatives that involve meaningful feedback. I alluded to the FBI, TFOS working group. Meaningful information and feedback occurs there. As I stated in my testimony on June 20, 2018, great examples of feedback include:

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

Q.4.d. Should policymakers consider reforming Section 314(b)? If so, how?

A.4.d. As noted earlier in my responses, I am a huge proponent of information sharing. I believe that policymakers should consider reforming or enhancing both Section 314(b), which is the sharing of information between financial institutions, and Section 314(a), which is information sharing between law enforcement and financial institutions.

With respect to Section 314(b), I would encourage policymakers to assess the percentage of participating financial institutions by asset size. My sense is less small banks participate in the Section 314(b) program. I would want to know why institutions, especially small institutions, do not participate. It is likely it is due to concern for cost and the lack of resources to handle the requests. I would also consider how to incentivize banks to participate in the Section 314(b) program.

Q.4.e. Should policymakers consider reforming Section 314(a)? If so, how?

A.4.e. With respect to Section 314(a), I would encourage policymakers to go back and assess the original intent for Section 314(a). My understanding from interaction with individuals involved in the process, the intent was that information sharing be both ways. Section 314(a) currently only has information going from financial institutions to law enforcement. Would it be viable for law enforcement to also provide information to financial institutions? This is definitely a question that policymakers should assess. If an information sharing mechanism can be developed through Section

314(a) from law enforcement to financial institutions, it may offset the SAR feedback mechanism to an extent.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM DENNIS LORMEL

Q.1. I'm concerned by the apparent growing use of cryptocurrencies by bad actors to evade sanctions and anti-money laundering laws. Whatever their other potential benefits may be, cryptocurrencies are attractive to cybercriminals, drug cartels, darkweb consumers, and countries like Iran, North Korea and Russia, that are interested in evading sanctions. One recent study of Bitcoin transactions found that darknet marketplaces such as Silk Road and AlphaBay, were the source of almost all of the illicit bitcoins laundered through conversion services. A significant percentage of Bitcoin conversion services work to conceal where they operate, which complicates finding the right foreign governments to partner with to ensure AML/CFT enforcement.

A.1. I firmly believe we should embrace technology and the use of cryptocurrency. At the same time, we must demand transparency and accountability. Criminals have been fast to embrace new technologies in order to circumvent transparency and reporting requirements. Unfortunately, AML compliance and fraud prevention are inherently reactive, while bad actors are not restricted by regulations and can be proactive.

Q.2.a. Are FinCEN's existing cryptocurrency policies adequate to combat AML/CFT using cryptocurrency?

A.2.a. Cryptocurrency poses a significant challenge for regulators and law enforcement. That's because of the unknown and the challenge the inherent reactive nature of AML compliance. As cryptocurrency and technology advance we must continuously and objectively assess the effectiveness of regulations and our ability to deal with emerging criminal challenges.

I believe FinCEN's existing policies and authority are adequate but must continuously be assessed and enhanced. My bigger concern is whether FinCEN and the Internal Revenue Service (IRS) possess the resources necessary to meet and address the continuously emerging crime problems posed by cryptocurrency and the ability to use the dark web. Neither FinCEN nor the IRS have an abundance of resources to address the evolution of the problem. The crime problem is likely to evolve faster than the adequacy of regulations or the capacity to deal with the crime problem. That is why we must ensure FinCEN, the IRS and other regulators and law enforcement agencies have the resources and capacity to address this emerging problem.

Q.2.b. If not, what more could FinCEN be doing to combat this?

A.2.b. I believe FinCEN currently has adequate capacity but must continuously assess the emerging problems posed by bad actors and realistically and proactively address impediments, resource constraints and emerging trends.

Q.2.c. And if not, does FinCEN have adequate authority to address the issue?

A.2.c. In my opinion, FinCEN currently has adequate authority to address the issue but that capacity must continuously be assessed and enhanced because it can and will be overwhelmed much faster than can be dealt with.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN SASSE FROM TRACY S. WOODROW

Q.1. Much of the future of AML efforts seems to be in artificial intelligence and machine learning. 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 similar techniques to identity money laundering and how much more progress can be made in this front?

A.1. Responses not received in time for publication.

Q.2. What incentives do financial institutions have to develop innovative AML techniques and consult typologies to stop human trafficking and fight MS–13? Are financial institutions ever punished for leveraging these techniques? For example, could a regulator punish a financial institution that found that human traffickers were using their services because the financial institution did not find the criminal activity earlier? How can this issue be fixed?

A.2. Responses not received in time for publication.

Q.3. Do smaller financial institutions have sufficient incentives and resources to use artificial intelligence type technology? If not, what can be done to make it easier for smaller financial institutions to use such technology?

A.3. Responses not received in time for publication.

Q.4. I worry that law enforcement officials and regulators provide to financial institutions an insufficient indication of their priorities in the AML context. In practice, many financial institutions feel as if they must spend as many resources on minor crimes as they do human and drug trafficking. If everything is a priority, nothing is a priority. Financial institutions need to be able to focus their resources on human and drug traffickers without getting in trouble if they comply with fewer process-based regulatory requirements along the way.

A.4. Responses not received in time for publication.

Q.5. Is there a lack of regulatory and law enforcement prioritization in the money laundering context? If so, how does this impact our AML regime?

A.5. Responses not received in time for publication.

Q.6. What are the most prominent examples of a lack of prioritization in our AML regime?

A.6. Responses not received in time for publication.

Q.7. What would it look like for a Federal AML regime to better prioritize particular law enforcement targets? What—if any—AML priorities should be de-emphasized? How could a system still en-

sure that a basic level AML competence was met so that still-important law enforcement priorities did not fall through the cracks?

A.7. Responses not received in time for publication.

Q.8. One potential area that involves lack of prioritization is the current process of filing suspicious activity reports. Financial institutions in my State spend a lot of resources filing these reports, and rarely seem to get feedback on what is useful and what is not. This makes it hard for them to understand the point of our SARs system. What is the cost of our current SARs system for the average financial institution? Is there anything policymakers can do to right-size the SARs-based regulatory requirements without undermining law enforcement priorities? For example, in certain instances should financial institutions be able to file only the underlying data and not spend the time necessary to prepare a broader report justifying the SAR?

A.8. Responses not received in time for publication.

Q.9. One potential hurdle to creating an effective feedback loop between law enforcement officials and financial institutions is that law enforcement officials are reluctant to share information about ongoing investigations.

A.9. Responses not received in time for publication.

Q.10. Is that a legitimate concern that should prevent law enforcement officials from sharing information with financial institutions?

A.10. Responses not received in time for publication.

Q.11. How could those concerns be mitigated?

A.11. Responses not received in time for publication.

Q.12. Even if law enforcement officials could not provide feedback about SARs relating to ongoing investigations, could they at least provide feedback about SARs relating to completed investigations?

A.12. Responses not received in time for publication.

Q.13. What—if any—other mechanisms should be developed to improve the feedback loop between law enforcement officials and financial institutions?

A.13. Responses not received in time for publication.

Q.14.a. Should policymakers consider reforming Section 314(b)? If so, how?

A.14.a. Responses not received in time for publication.

Q.14.b. Should policymakers consider reforming Section 314(a)? If so, how?

A.14.b. Responses not received in time for publication.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM TRACY S. WOODROW

I'm interested in the ways in which technology can aid AML compliance efforts.

Q.1. What are some of the innovative technologies that you've seen that hold some promise for either the Government or the private sector?

A.1. Responses not received in time for publication.

Q.2. Are you aware of privacy-enhancing technologies that facilitate the sharing of information between parties without revealing personal identifying information?

A.2. Responses not received in time for publication.

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

A.3. Responses not received in time for publication.

Q.4. What can we be doing as legislators to ensure that we promote technological innovation in this sector?

A.4. Responses not received in time for publication.