EXAMINING THE BSA/AML REGULATORY COMPLIANCE REGIME

HEARING

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JUNE 28, 2017

Printed for the use of the Committee on Financial Services

Serial No. 115–26

U.S. GOVERNMENT PUBLISHING OFFICE

28–223 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. McHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
THOMAS MacARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
CHARLIE CRIST, Florida
RUBEN KIHUEN, Nevada

KIRSTEN SUTTON MORK, *Staff Director*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

BLAINE LUETKEMEYER, Missouri, *Chairman*

KEITH J. ROTHFUS, Pennsylvania, *Vice Chairman*
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANDY BARR, Kentucky
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
MIA LOVE, Utah
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York

WM. LACY CLAY, Missouri, *Ranking Member*
CAROLYN B. MALONEY, New York
GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
NYDIA M. VELÁZQUEZ, New York
AL GREEN, Texas
KEITH ELLISON, Minnesota
MICHAEL E. CAPUANO, Massachusetts
DENNY HECK, Washington
GWEN MOORE, Wisconsin
CHARLIE CRIST, Florida

CONTENTS

WITNESSES

WEDNESDAY, JUNE 28, 2017

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

EXAMINING THE BSA/AML REGULATORY COMPLIANCE REGIME

Wednesday, June 28, 2017

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:13 p.m., in room 2128, Rayburn House Office Building, Hon. Blaine Luetkemeyer [chairman of the subcommittee] presiding.

Members present: Representatives Luetkemeyer, Rothfus, Posey, Ross, Pittenger, Barr, Tipton, Williams, Love, Trott, Loudermilk, Kustoff, Tenney; Clay, Maloney, Scott, Velazquez, Green, Heck, and Crist.

Ex officio present: Representatives Hensarling and Waters.

Also present: Representative Davidson.

Chairman LUETKEMEYER. The Subcommittee on Financial Institutions and Consumer Credit will come to order. Without objection, the Chair is authorized to declare a recess of the subcommittee at any time.

Today's hearing is entitled, "Examining the BSA/AML Regulatory Compliance Regime." Before we begin today, I would like to thank the witnesses for appearing. We certainly appreciate you taking time out of your schedules to be here and participate today. I look forward to your comments.

I now recognize myself for 2 minutes for an opening statement. The goals of the Bank Secrecy Act and anti-money-laundering legal regime are laudable: Institutions and government agencies should work together to prevent money laundering and terrorist financing.

However, the reality is that well-intentioned regulation has spiraled out of control and resulted in a breakdown of what should be a collaborative relationship between law enforcement, financial regulators, and institutions. Today, regulators essentially deputize credit unions and banks as law enforcement and allow for a regulatory regime that is both opaque and punitive.

BSA/AML-related settlements have increased significantly in both amount and frequency. Institutions are reporting surges in total investment in AML. And their consumers, especially those conducting financial transactions internationally, bear the brunt of this regulatory cost. I fear the BSA/AML process oftentimes benefits no one, not the institution and not law enforcement.

Also concerning is that financial institutions are more risk-adverse than seemingly ever before, partially as a result of the regu-

latory structure. The rampant derisking seen in recent years actually, in my opinion, increases risk to the financial system, proving the BSA/AML regulatory regime to be ineffective and, to some degree, dangerous.

To be clear, the intent of today's hearing is not to discuss opportunities for financial institutions to more easily skirt the law or to help nefarious actors participate in illegal activity. We are here today to discuss improvements that could benefit both law enforcement and financial institutions while simultaneously creating a more effective BSA/AML regulatory construct.

I look forward to a robust conversation with our distinguished panel and thank them for their participation.

The Chair now recognizes the ranking member of the subcommittee, the gentleman from Missouri, Mr. Clay, for 5 minutes for an opening statement.

Mr. CLAY. Thank you, Mr. Chairman, for holding today's hearing to review the compliance regime for the Bank Secrecy Act and related anti-money-laundering requirements.

And I thank the witnesses for sharing their perspectives on this topic.

A 2016 GAO report found that from 2009 to 2015, Federal agencies assessed roughly $5.1 billion in fines, forfeitures, and penalties against financial institutions for violations of BSA/AML requirements. In one notable case, HSBC was required to enter into a deferred prosecution agreement with the Justice Department and forfeited more than $1.2 billion for violations of the Bank Secrecy Act and illegally conducting transactions with Iran and other sanctioned countries.

A 2012 bipartisan staff report issued by the Senate Permanent Subcommittee on Investigations found that HSBC exposed the U.S. to money laundering, drug trafficking, and terrorist financing risk by operating its corresponding accounts for foreign financial institutions with longstanding severe AML deficiencies, including a dysfunctional AML monitoring system for account and wire transfer activity, an unacceptable backlog of 17,000 unreviewed alerts, insufficient staffing, inappropriate country and client risk assessments, and late or missing suspicious activity reports (SARs).

The Senate staff report also criticized the OCC for weakly enforcing BSA/AML requirements with respect to HSBC and included a series of recommendations that I think should be part of our discussion on this topic.

So as the subcommittee examines the effectiveness of the current BSA/AML compliance regime and reform proposals, these facts should help remind us that we still need a strong system that stops bad actors and prevents the criminal exploitation of financial systems to conceal the location, ownership, source, nature, or control of illicit proceeds.

There are a number of proposals that Congress should consider. Ranking Member Waters introduced legislation last term that would, among other things, significantly increase civil monetary penalties for both institutions and individuals for willful and negligent violations of the BSA. And Congresswoman Maloney has introduced legislation on beneficial ownership that would eliminate

the ability of bad actors to conceal their activities in shell corporations.

And, Mr. Chairman, at this time, I yield my time to Congresswoman Maloney.

Mrs. MALONEY. First, I want to thank my colleague, the ranking member and my good friend, for yielding to me, and to thank the chairman for holding this hearing. I would like to also thank Chairman Hensarling for creating, first, the antiterrorism task force and the antiterrorism financing committee. I think it is critical, and reflects, really, the challenges that we confront.

The anti-money-laundering rules for financial institutions are an incredibly important tool for combating terrorism financing. And if they can't finance their terrorist activities, they are not going to have them. So it is a very important part of our national security strategy.

But because criminals and terrorists are constantly changing their strategies to elude law enforcement and to hide their identities from financial institutions, the anti-money-laundering obligations also require financial institutions to do a great deal of work. So to the extent that we can streamline this process without letting our guard down and making it easier for criminals and terrorists to access the U.S. financial system, that would be a win-win for everyone.

The Clearing House, which is represented on the panel today, published a lengthy set of recommendations in February on how to streamline the anti-money-laundering framework, and I think it is a serious report that deserves our consideration and support.

I would like to highlight one section of the Clearing House report in particular. Section 2 of the report recommends that Congress pass the Beneficial Ownership bill, which is bipartisan, introduced today by Chairman Ed Royce, former Chairman King, and myself. The bill, called the Corporate Transparency Act, will require companies to disclose their true beneficial owners when a company is formed. States would have the option to collect this information themselves under our bill. But if the State isn't doing it, then the Treasury Department would collect beneficial ownership information as a backup.

This information would be available to law enforcement and, importantly, to financial institutions as well with customer consent. This is important because it helps financial institutions comply with their know-your-customer obligation. If the customer is a company, financial institutions can't know who their customers really are unless they know who the beneficial owners of the company are.

This would also reduce the regulatory burden on financial institutions, because they wouldn't have to spend an enormous amount of resources investigating their own customers and trying to figure out their beneficial owners. Instead, they could just refer to the Treasury database to figure out who the owners of these companies are.

So this bill is a win-win. It is good for our financial institutions, good for law enforcement, and good for our national security. Thank you.

Chairman LUETKEMEYER. With that, we yield 2 minutes to the gentleman from Pennsylvania, the vice chairman of this subcommittee, Mr. Rothfus.

Mr. ROTHFUS. I thank the chairman for yielding, and I want to thank him for having this hearing today.

Getting our Bank Secrecy Act and anti-money-laundering policies right is a very important issue for me and my district. In fact, it is a life-or-death issue.

Just a few days ago, we marked the International Day Against Drug Abuse and Illicit Trafficking. It was a time to reflect on the drug epidemic that has destroyed so many lives and continues to ravage our hometowns. It was also an opportunity to take stock of how our current policy framework fails to achieve its objectives.

This committee's effort to interrupt the finances of the transnational criminal organizations and gangs that pump the heroine and fentanyl poison into our communities can ultimately save lives. If we can cut off the flow of cash, we can greatly hinder the ability of these groups to do us harm.

I am looking forward to hearing from stakeholders today as to how we can create a more potent BSA/AML regime that makes the best use of scarce public and private sector resources. It is clear to me that our existing framework puts heavy burdens on financial institutions and appears to emphasize compliance with rigid standards over efficacy. We need to be looking at how technology, innovation, and greater cooperation can be employed to yield better results in this fight.

President Trump wrote in his letter marking the International Day Against Drug Abuse and Illicit Trafficking, "We will not stand idle as our families are devastated, our communities are hollowed out, and our Nation's future is diminished." I could not agree more with that sentiment. And the work that we are doing here today is an example of Congress taking action to bolster our defenses against illicit financing and to bring down the criminals who cause so much pain in communities across this country. We have a moral obligation to achieve these ends.

I thank the chairman, and I yield back.

Chairman LUETKEMEYER. The gentleman yields back.

The Chair recognizes the gentleman from North Carolina, the vice chairman of our Subcommittee on Terrorism and Illicit Finance, Mr. Pittenger.

Mr. PITTENGER. Thank you, Mr. Chairman. And I appreciate you holding this important examination of the Bank Secrecy Act and our AML/CFT compliance regime.

In addition to serving on this subcommittee, as you stated, I do serve as vice chairman of our Subcommittee on Terrorism and Illicit Finance, which is also strongly engaged in this topic. I am also encouraged that both subcommittees are taking a hard look at BSA modernization. We will need both subcommittees' expertise if we are to establish a streamlined and effective regime to protect our financial system from illicit use.

As we examine the BSA, this committee should explore innovative technologies and policies that can facilitate compliance and targeted information sharing. The goal should be getting the most relevant, timely, and actionable information into the hands of our

financial regulators and law enforcement while providing targeted data sharing from the government to financial institutions with privacy and civil liberty protections that will limit the focus and oversight of financial institutions.

We have a great opportunity to achieve this goal, and I look forward to the testimony of our witnesses and their suggestions for where we can improve and modernize our current system.

Thank you, and I yield back.

Chairman LUETKEMEYER. The gentleman's time has expired.

Today, we welcome the testimony of Ms. Faith Lleva Anderson, senior vice president and general counsel for American Airlines Federal Credit Union, on behalf of the Credit Union National Association; Mr. Greg Baer, president, The Clearing House Association; Mr. Lloyd DeVaux, president and CEO of Sunstate Bank, on behalf of the Florida Bankers Association; and Ms. Heather Lowe, legal counsel and director of government affairs, Global Financial Integrity.

Before we recognize the witnesses, I would like to ask unanimous consent that the gentleman from Florida, Mr. Ross, be recognized for the purpose of making a brief introduction. Without objection, the gentleman from Florida is recognized.

Mr. ROSS. Thank you, Mr. Chairman. And it is my pleasure to introduce one of our witnesses today, Mr. Lloyd DeVaux, president and CEO of Sunstate Bank in Miami, Florida.

In addition to his position with Sunstate, Mr. DeVaux serves on the Board of Directors and Executive Committee of the Florida Bankers Association (FBA), and he is testifying today on behalf of more than 100 Florida banks represented by the FBA.

Mr. DeVaux brings over 25 years of experience in the banking industry to today's hearing, including 12 years as chief operating officer with BankAtlantic and City National Bank of Florida prior to joining Sunstate Bank in July of 2014.

Founded in 1999, Sunstate Bank is one of Florida's most vibrant community banks—and we want to see you continue to be a vibrant community bank—with 3 locations and 45 employees serving the Miami-Dade County region.

We are fortunate to have Mr. DeVaux here today to provide us with insight into the role of community banks in Florida and across the Nation in the fight against money laundering and terrorist financing. I want to thank the chairman for calling upon Mr. DeVaux to share with us the community and the Florida bank perspective on this important issue.

And thank you to Mr. DeVaux and the rest of the witnesses today. We look forward to your testimony.

I yield back.

Chairman LUETKEMEYER. Thank you, Mr. Ross. That is such compelling testimony there, I might want to make a deposit to Mr. DeVaux's bank. Thank you.

Each of the witnesses will be recognized shortly here for 5 minutes to give an oral presentation of your testimony. And without objection, each of your written statements will be made a part of the record. Briefly, the lighting system, for those of you haven't been here before, green means go. When the yellow light comes on,

it means you have a minute. So be ready to start wrapping up. And when you hit the red, that means we need to stop and move on.

A couple of quick notes. We may be interrupted by votes—we are looking at votes sometime around 4:00, 4:15. If we do, and we are not done, we may ask the witnesses to please return or stay put here, and then we will return as quickly as we can. If not, we will hopefully be able to wrap up shortly.

The other thing is, for those Members who are asking questions, we have a large turnout today, so if you can keep it within the 5 minutes, that would be great.

Ms. Anderson, you are recognized for 5 minutes.

STATEMENTS OF FAITH LLEVA ANDERSON, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, AMERICAN AIRLINES FEDERAL CREDIT UNION, ON BEHALF OF THE CREDIT UNION NATIONAL ASSOCIATION (CUNA)

Ms. ANDERSON. Thank you, Chairman Luetkemeyer, Ranking Member Clay, and members of the subcommittee. Thank you for the opportunity to testify on this important topic.

I am Faith Lleva Anderson, the senior vice president and general counsel for American Airlines Federal Credit Union, headquartered in Fort Worth, Texas. I am also the Vice Chair of the Consumer Protection Subcommittee of the Credit Union National Association, on whose behalf I am testifying today.

American Airlines Federal Credit Union proudly serves over 274,000 members. We began as a single-sponsor credit union for American Airlines over 80 years ago. Following 9/11, we extended our membership beyond American Airlines employees to include air transportation groups, such as TSA and FAA employees.

My credit union's asset size is $6.5 billion, which is quite small compared to regional or national banks. Like all credit unions, we are a not-for-profit institution owned by the very members we serve and are established to promote thrift and provide access to credit for provident purposes.

American Airlines Federal Credit Union is committed to financial security compliance and applies whatever resources necessary to ensure our operations are solid and our members are protected. However, since the 2008 economic crisis, credit unions have been subject to more than 200 regulatory changes totaling nearly 8,000 Federal Register pages. The new regulatory regime makes Bank Secrecy Act and anti-money-laundering regulatory compliance even more daunting.

Nevertheless, my credit union has a staff dedicated to ensure we fully comply with BSA/AML requirements. We conduct detailed recordkeeping and spend thousands of hours and dollars on due diligence. In fact, due to increasing BSA requirements, we have split our BSA department into two separate sections, one to work on the investigative side and one to work on the risk side. This adjustment was made so my credit union could efficiently keep up with the many filing and recordkeeping requirements.

Of all the requirements on BSA/AML, the most burdensome and time-consuming are investigating open suspicious activity report cases, monitoring the members' accounts and transaction activity for unusual behavior, conducting the exhaustive research on an av-

erage of 600 potential suspicious activity scenarios per month, and filing these reports, as well as currency transaction reports.

It generally takes my credit union 3 to 5 days to process an average suspicious activity report for one case, and we have about 30 to 40 filings per month.

In addition, quality control is costly and time-consuming. Preparing for our annual exam on BSA/AML compliance requires the work of 3 full-time professional staff members and takes about 2 full months. This time is dedicated to ensuring reports are filed accurately, the risk assessments are completed, and there have been no mistakes made to the process and filings.

My credit union dedicates a great amount of time, staff, resources, and money to BSA/AML requirements. The median size of a credit union is less than $30 million in assets with a total staff of just 8 employees. The reality is the cost of technology for monitoring and ensuring compliance with BSA/AML regulations is disproportionately burdensome on smaller and less complex institutions.

Nevertheless, with the changes outlined in my written testimony, the Federal Government can ease the compliance burden for financial institutions while maintaining the protections needed. We urge legislative and regulatory changes to address the redundancies, unnecessary burdens, and opportunities for efficiencies within the BSA/AML statutory framework.

In particular, we support changes to minimize the duplication of the same or similar information, provide additional flexibility based on the reporting institution type or level of transactions, curtail the continually enhanced customer due diligence requirements, increase the currency transaction reporting threshold, reduce defensive filings, simplify the reporting requirements of suspicious activity reports, and allow for greater regulatory and examination consistency among regulators.

My written testimony provides details on issues that credit unions face regarding BSA/AML compliance and also outlines common-sense changes. Credit unions are committed to the fight against terrorism and related crimes. I hope my testimony will help this subcommittee find the balance between protection and undue burden.

Thank you.

[The prepared statement of Ms. Anderson can be found on page 46 of the appendix.]

Chairman LUETKEMEYER. Thank you, Ms. Anderson.

Mr. Baer, you are recognized for 5 minutes.

STATEMENT OF GREG BAER, PRESIDENT, THE CLEARING HOUSE ASSOCIATION

Mr. BAER. Thank you, Chairman Luetkemeyer, and members of the subcommittee.

Over the past year, The Clearing House has devoted substantial resources to analyzing the current system for anti-money-laundering and countering the financing of terrorism. Today, I will present some of the conclusions that we have reached.

Our current AML/CFT system is broken. It is extraordinarily inefficient and outdated and driven by perverse incentives. Funda-

mental change is required to make that system an effective law enforcement and national security tool and reduce collateral damage it is doing to global development, financial inclusion, and other U.S. policy interests.

I will begin with an analogy. Imagine an army where officers are evaluated based not on how their units behave in battle, but rather based on the accuracy and punctuality of their expense reports and the casualties suffered by the unit. The auditors do not have sufficient security clearance to be briefed on the battles that have occurred or read any after-action report. Thus their audits reflect only the losses suffered by the unit itself, not the casualties inflicted by the enemy.

What sort of an army would this system produce? One led by officers averse to outside-the-box thinking and risky advances and more inclined to entrench their positions and excel at paperwork. This army inevitably would be led by a George McClellan, not an Eisenhower or a Patton.

The U.S. AML/CFT regulatory regime circa 2017 is not dissimilar. Law enforcement and national security officials are the end users of the information that banks produce. They value a risk-based approach to AML/CFT with banks using innovative approaches that detect the most dangerous crimes. But compliance with AML/CFT rules is not examined or enforced by law enforcement or national security officials, but rather by bank examiners.

These examiners are in a no-win position. On the one hand, they are excluded when the bank they examine is pursuing real cases with law enforcement and national security and receive no credit for those cases. But if something goes wrong, if a corrupt official or organization turns out to be a client of the bank they examine, the examiner takes the blame.

Thus the rational response is to focus on what they know and control, extremely detailed policies and procedures and simple metrics, for example, the number of computer alerts generated, the number of suspicious activity reports filed, and the number of compliance employees hired.

What gets measured gets done, and providing valuable intelligence to law enforcement or national security agencies does not get measured. Writing policies and procedures and filing a lot of SARs does.

So almost 2 million SARs are filed per year now. The largest banks file one SAR per minute. Even then, the value of those SARs to their end users is not measured, so the measure of success is generally volume alone.

The greatest cost of this dysfunction is an opportunity cost. Emerging technology has the potential to make the AML/CFT regime dramatically more effective. Artificial intelligence and machine learning could revolutionize this area, and banks continue to discuss ways to utilize those technologies.

But those strategies require feedback loops which do not exist in the current SARs system. They also require a mandate from government to shift resources from investigating and filing SARs on low-dollar crimes and instead investing in modern methods for detecting high-impact crimes and terrorist activity. Law enforcement

and national security currently have no authority to provide that mandate.

Another cost to the current system comes as banks are pushed to eliminate clients in countries or industries that end up creating political risk, so-called derisking. Here, a whole other group of government stakeholders has concerns: global development officials concerned about human suffering in countries cut off from correspondent banking and remittances; trade officials worried that American business will have to retreat along with American banks; and diplomatic officials concerned about a lack of influence when U.S. companies leave.

Again, though, these agencies play no role in the current system, and Federal prosecutors seeking record fines when a problem does develop do not internalize those costs.

In 2016, the Clearing House convened at two symposia a remarkable group of stakeholders, including foreign policy, development, and technology experts. Their goal was not to save banks money, but to do what is right for this country. The resulting report is attached to your testimony.

You will see numerous recommendations in that report. The most important one, though, is for the Department of the Treasury to play a strong leadership role in setting priorities for the system. This should include reclaiming, through FinCEN, supervisory authority over the largest internationally active banks which filed a majority of SARs and present the toughest issues. A dedicated FinCEN examination team for this group of firms could receive appropriate security clearances, meet regularly with law enforcement, and work to develop metrics in this area. Most importantly, it could establish priorities and stick to them.

Finally, one important change to the current regime does require legislation: ending the use of shell companies with anonymous ownership. I was pleased to appear this morning with Congresswoman Maloney to endorse the Corporate Transparency Act that she is cosponsoring with Congressman King and a bipartisan group of Members. I hope to discuss it further this afternoon.

Thank you very much for your time, and I look forward to your questions.

[The prepared statement of Mr. Baer can be found on page 59 of the appendix.]

Chairman LUETKEMEYER. Thank you, Mr. Baer.

Mr. DeVaux, you are recognized for 5 minutes.

STATEMENT OF LLOYD DEVAUX, PRESIDENT AND CHIEF EXECUTIVE OFFICER, SUNSTATE BANK, ON BEHALF OF THE FLORIDA BANKERS ASSOCIATION

Mr. DEVAUX. Chairman Luetkemeyer, Ranking Member Clay, and members of the subcommittee, my name is Lloyd DeVaux. I am president and CEO of Sunstate Bank, a community bank founded in 1999 with $200 million in assets and 3 locations in Miami-Dade County in south Florida. Sunstate Bank has 45 employees and focuses on the needs of small businesses, consumers, and real estate investors, including nonresident aliens.

I appreciate the opportunity to be here today to discuss the challenges in complying with the Bank Secrecy Act. Clearly, BSA com-

pliance is an important building block for our national security. But the world has drastically changed since it was first adopted in 1970. As the United States takes steps to combat terrorism and financial crime, now is the time to update BSA compliance in order to develop a system suited for the 21st Century.

The resources devoted to compliance, especially BSA compliance, are significant for a bank our size. Sunstate Bank has seven people in compliance, six of whom are just in BSA. BSA is our largest department. We have only four full-time lenders. That means we have fewer staff devoted to making loans that benefit the community than we have devoted to compliance.

Our experience is not unique. In 2007, 14 percent of the Florida banks had 5 or more BSA officers. Today, 38 percent have 5 or more. While some of this increase is due to acquisitions, much has been driven by regulatory pressure and the heightened regulatory risk of enforcement actions.

This is not a recipe for success. Direct BSA expenses were more than 10 percent of the bank's total expenses in 2016. The more we spend on compliance, the less we spend on services for our communities. Every $100,000 spent on compliance translates to a million dollars less that we can lend.

The added cost of BSA compliance on top of the significant cost of the Dodd-Frank Act has led to the disappearance of many smaller banks in Florida. For example, 111 banks merged or sold after Dodd-Frank was enacted. That is a consolidation of 50 percent of all Florida banks in just 7 years.

Even more important than the direct cost of BSA compliance is the impact on our customers. For example, many legal businesses are labeled high risk by the regulators. This means banks must collect more data, do more analysis, provide more oversight, and engage in more site visits, all of which translates to higher costs for us and our customers.

The best option in many cases is not to bank certain industries and certain customers and to even ask existing customers to close their accounts. From the bank's perspective, the economics of compliance make it unprofitable to maintain certain accounts.

This has serious drawbacks. First, it makes no sense to create a system that drives legitimate customers outside the formal banking system to less regulated or even unregulated providers. Second, it creates a series of financial transactions that may not be reported or available to law enforcement. Third, it can create a shadow financial system that is readily available for criminals and terrorists.

We need to modernize our approach. Banks should not be serving as undeputized law enforcement agents. For example, rather than doing a full-blown investigation on a suspicious transaction, banks should file a short suspicious activity report and let law enforcement agents do what they are trained and qualified to do.

Moreover, the partnership between law enforcement and the private sector needs to be a two-way street to succeed. Banks produce a huge amount of information but seldom get any feedback on its use or its effectiveness. More communication from law enforcement is needed to help banks focus resources in more useful ways. We also need to eliminate red tape that restricts bank from sharing information with each other.

Finally, we need to focus on real risk appropriate to the institution. For example, many of the 5 to 10 percent of our customers who are considered high risk by the regulators would not even be on the radar of very large banks. Our customers complain all the time that small banks are asking questions that larger banks never ask.

We all want to fight money laundering and terrorist financing. We only asked that regulation be sensible so that resources are used in a wise and efficient manner to combat the crime.

Thank you for holding this hearing today. I look forward to answering your questions.

[The prepared statement of Mr. DeVaux can be found on page 102 of the appendix.]

Chairman LUETKEMEYER. Thank you, Mr. DeVaux.

Ms. Lowe, you are recognized for 5 minutes.

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

Ms. LOWE. Chairman Luetkemeyer, Ranking Member Clay, and members of the subcommittee, thank you very much for the opportunity to address you here today. You have my biographical details in front of you, so I won't belabor that.

I hope my contributions to today's hearing will help you make measured and informed decisions that are really in the public's interest as well with respect to the U.S.'s AML regime. In my written testimony, which is about 17 pages, I provide information and opinions regarding trends in compliance, suspicious activity reports, know your customer (KYC) and customer due diligence, and balance of activity and obligations between FinCEN, the regulators, and the private sector.

And I would stress balance. I do think that is really important here, and that is something that has been mentioned by other panelists today. Some of my remarks also directly address some of the proposals by The Clearing House.

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

Equally, however, it is critical that Congress understands and carefully weighs the potential benefits against the potential ramifications that may be negative before making decisions in this area. Regulation and enforcement are primarily dissuasive measures because they can carry potential liability and we should be very careful when we decrease those dissuasive measures.

The second point I really wanted to stress here is that AML compliance and reporting is undertaken by a really wide range of entities and persons going far beyond the banking sector. You have bankers in front of you today. But any proposed changes being considered should really be looked at in light of that wide range of actors, those types of entities and persons.

Third, some types of entities and persons should be required to have AML programs in place but currently don't, such as those in-

volved in real estate closings, lawyers, and others. The banking sector cannot and should not carry this responsibility alone, especially where these persons act as proxies to open the door to the U.S. financial system for criminals and their money.

Fourth, Congress should request from the various regulators data regarding formal and informal enforcement actions pertaining specifically to AML/BSA violations and deficiencies so that they are better able to independently assess the appropriateness of the enforcement regime currently in place.

Fifth, I wanted to point out as well that both small banks and large banks have been the subject of major money laundering cases. You don't often see the smaller banks in the news and hitting the national news, because they tend to be considered a local matter.

Sixth, enforcement against money laundering is primarily through the identification of regulatory infractions as opposed to through criminal charges of actual money laundering. This may be because it is easier to find the evidence of regulatory infractions, the burden of proof is lower, the cost of doing so is far less than pursuing criminal money laundering charges. But the dissuasive effect is just as great.

However, when one looks at the cases where enforcement was merely through identification of deficiencies of AML systems and filing requirements, the hallmarks of serious criminal money laundering are in those cases. As a result, decreasing the ability to enforce using the regulatory approach may have serious negative repercussions on compliance and ultimately criminal access to the U.S. system.

My seventh point is that suspicious activity reports are meant to be just that, reports of suspicious activity. Requiring bank employees to determine if activity is, in fact, illegal before filing a SAR, as has been recommended by The Clearing House, would actually be counterproductive, I think, in a lot of ways, including increasing the burden on bankers who would have to then actually make a legal determination that they didn't previously have to make.

I do think that there are some issues with respect to how much information needs to be provided on SARs and how much background work banks need to do before filing those, and I think that is something that we should really seriously discuss. But that bright line, illegal/legal line, I think, is very counterproductive.

Eighth, The Clearing House also recommends that greater information-sharing take place among banks and with the government in a number of ways. We generally support that greater sharing of information in the AML area, but it has to be done with appropriate privacy safeguards. Where it may result in people being, essentially, debanked, there has to be some sort of system for redress for people to be able to prove that what they are doing is legitimate activity, and we need to be taking that into account.

Ninth, it is critical that information about the natural persons who own and control companies, otherwise known as the beneficial owners, is finally collected by either the State or the Federal Governments and that it is made available to so both law enforcement and to the financial institutions. Companies with unknown or hidden ownership are the number one problem in the AML world, and

the U.S. cannot continue to allow our failure to act here to put the U.S. and the global financial system at risk.

I am really pleased that this morning a bipartisan bill was introduced in both the House and the Senate to do just that. We wholeheartedly support the Corporate Transparency Act and thank Representatives Maloney, King, and Royce for introducing the House bill.

Tenth, I would strongly caution against transferring responsibility for setting AML priorities for individual banks from those banks to FinCEN. Banks really are best placed to understand their business and their systems and the money laundering risks that are inherent in those things. They really need to be able to create—

Chairman LUETKEMEYER. Can you wrap up pretty quickly?

Ms. LOWE. Don't I have another minute? No?

Chairman LUETKEMEYER. You had 5 minutes.

Ms. LOWE. Oh, I'm sorry.

Chairman LUETKEMEYER. Everybody else had 5 minutes.

Ms. LOWE. Am I—

Chairman LUETKEMEYER. You are way over.

Ms. LOWE. I am on the wrong side of 5 minutes. That would explain it. I apologize. I thought I had a minute left.

Chairman LUETKEMEYER. We thank for your testimony. Hopefully, you can delve into more of your suggestions here as we go through the discussion.

Ms. LOWE. Sure.

[The prepared statement of Ms. Lowe can be found on page 114 of the appendix.]

Chairman LUETKEMEYER. Thank you.

Without objection, the gentleman from Ohio, Mr. Davidson, is permitted to participate in today's subcommittee hearing. Mr. Davidson is not a member of the subcommittee, but he is a member of the full Financial Services Committee, and we appreciate his interest in this topic, and welcome his discussion here when he returns.

With that, I recognize myself for 5 minutes for questions.

It was interesting to hear your discussion, and I certainly appreciate everybody's testimony this afternoon. There were lots of interesting comments from the standpoint of Mr. Baer's analogy to the army with regards to how this whole structure is working, I thought that was pretty enlightening, and bankers have become law enforcement officers instead of being bankers. I think we need to put everybody back in their own pew.

But I was interested in your discussion, Mr. Baer, when you talked about some of the technology that can actually help detect some of this stuff. I know with the fintech explosion here it seems like there is a lot of ability to go in and assess data. And is there a place for that, are we doing that now, or are we not doing that?

Because it would seem to me that we can figure out what kind of magazine I would like to read based on all the things in my background here—where I do business, what I eat, where I go—and yet, we are not doing that with regards to suspicious activities.

Mr. BAER. It is a great question. Among the experts we considered or consulted in our work were folks who were experts in big data and AI.

And just as background, I think what is important to understand is the SAR database was created 25, 30 years ago for a very different purpose. It was a suspicious activity report where there were a sufficiently small number of them that one of them was read by an Assistant United States Attorney (AUSA) somewhere in this country. So they were actually written to be read, every one read by someone.

Now that we have almost 2 million filed per year, there is no one reading them in the first instance. Instead, what law enforcement does is word searches against that database. The banks also do searches against the database, basically looking for patterns.

So we have gone from sort of providing leads in a very personal way to a prosecutor to basically having a big bunch of data, and what do you do with that data? And that is where the system has never caught up, because the first thing we heard from the big data folks is you have to have a feedback loop. If you want your algorithms to get smarter, you have to know for a given SAR, is that a good SAR or a bad SAR?

They have even proposed you should just have law enforcement have a green button and a red button for good SAR or bad SAR. That would actually make things work a lot better. But there are a lot of other concepts like that that you could apply once you start thinking about that database in terms of a searchable bunch of data as opposed to an individual lead.

Also, you could think about—and I think Mr. DeVaux was talking about this—the format of it. When it was an individual lead to be read, it had to be very carefully written in great syntax and reviewed at three levels. But if it is just going to be searched, do you even need a paragraph? Can you just dump in the data from the underlying account?

So those are the kinds of questions that aren't being faced now.

Chairman LUETKEMEYER. Okay. Very good.

Mr. DeVaux, you are in the trenches every day. You deal with this every day. So can you explain to me the impact of the rules and regulations presently on your—you kind of outlined it with regards to the numbers of people in there. But are you finding problems? Are you finding people who do illicit activities with the process that we have? Or can you give us ideas on how to do something different that would actually streamline the process so that you don't have to have more compliance officers than you do loan officers?

Mr. DEVAUX. Thank you, Mr. Chairman.

To give you an example, when you set a customer up in your system, you build a profile on that customer. If that customer deviates from the profile, the BSA area gets an alert. We got 7,100 alerts last year. We filed 29 total SARs, 15 from alerts. We had to go through every one of those alerts. And any alert that creates suspicious activity is then turned into an investigation.

Chairman LUETKEMEYER. Okay. Let me interrupt for just one second. Do you the investigating or does law enforcement do the investigating?

Mr. DEVAUX. The bank.

Chairman LUETKEMEYER. The bank does the investigating.

Mr. DEVAUX. The bank's BSA department does an investigation. And it may eventually lead to a SAR. Last year, we filed 29 SARs; 15 were generated from the alerts. So we did 7,100 alerts turning into 15 SARs. That is a lot of work. About 7 or 8 percent of our accounts are high risk, and that is what generates a lot of our alerts.

Chairman LUETKEMEYER. Okay. Very good.

I think you made a comment also with regards to the consistency of the rules. I think you made the comment with regards to being a small bank, that a lot of times, you are looked at differently than larger banks with regards to your client base. Can you expand on it for just a second?

Mr. DEVAUX. Yes, sir. Thanks.

We run our database to determine how many high-risk accounts we have. And we have had regulators come back and tell us that number is not high enough, you can't just have 4 percent high risk, you need to have 6 or 8 percent high risk. A high-risk account is a high-risk account. It shouldn't be determined by an arbitrary number.

Chairman LUETKEMEYER. So they are asking you to go in and fudge the numbers, then, so you get to a higher number? Because I would assume you are giving the actual amount of high-risk business in your book of business.

Mr. DEVAUX. The way the high risk is built is by parameters associated with the country they are doing business with, the amount of money they are running through the account, etc. So if you set the level of account transactions at a higher or lower level, you will generate more or less alerts. So, they are saying, and I wouldn't use the word "fudge," but they are basically saying you need to decrease your high-risk account parameters to pick up more alerts.

Chairman LUETKEMEYER. Okay. Thank you very much. My time has expired.

With that, we will recognize the gentleman from Georgia, Mr. Scott, for 5 minutes.

Mr. SCOTT. Thank you very much, Mr. Chairman.

Mr. Baer and Mr. DeVaux, I would like to, first of all, direct this to you two to respond.

Last month, in May, we received a report from the FBI's Internet Crime Complaint Center. And according to this report, attempts at cyber wire fraud globally surged in the last several months of 2016. Fraudsters sought to steal some $5.3 billion in schemes where they pretended to be trusted business associates requiring wire transfers. And this spike in fraud saw a total number of business email companies' cases almost doubled from May to December of last year, rising to 40,000, up from just 22,000.

So, Mr. Baer, I listened to your testimony, and I want you to address the issue of these financial innovation units. It seems to me that you are sort of plowing down this road as a possible way of dealing with this. And so my understanding is—don't get me wrong—is that we need to provide regulatory safe harbors to these financial innovation units or institutions so that these units can operate in a sandbox outside of bank examiners' sanctions.

Now, that is a lot. What is the sandbox? How well does this work? Is this a pattern we have to follow on?

And then, Mr. DeVaux, I would like for you to agree or disagree. Mr. Baer?

Mr. BAER. Sure. In some ways it is unfortunate that you actually have to request a safe harbor or a sandbox in order to do the right thing, which is to innovate and try to find more interesting ways—or more effective ways to catch very bad people doing bad things.

The problem that has arisen, however, and we have heard this from multiple banks, is that—and to some extent this gets back to Mr. DeVaux, where there is a certain number of alerts that are expected or a certain number of SAR filings—when you are trying out a new way of identifying criminal behavior, you don't have policies and procedures for that. You are experimenting. You may not know what the yield is supposed to be. If you have a new algorithm, you don't know how many alerts that is supposed to trigger.

And yet banks do face criticism when they do that. And so what they are really saying is, yes, we will comply with all the rules that we are complying with currently, but we want to have the chance to innovate and find new ways to do this, which I would hope could be relatively uncontroversial.

Mr. SCOTT. Let me tell you a little bit of my concern about this. In providing a regulatory sandbox approach to combating terrorism, could we be hurting the very people we are trying to help if financial institutions can operate in a sandbox like this?

Mr. DeVaux?

And, Mr. Baer, you can chip in too.

Mr. DEVAUX. I think fighting BSA crime is a team effort across-the-board. The question for me is which members of the team should be doing what. For banks, we get very little feedback on what works and what doesn't work.

Mr. SCOTT. You get very little feedback from whom?

Mr. DEVAUX. From law enforcement, from FinCEN, from the people who actually receive our BSA product, our SARs, any reports, our OFAC hits, our 314 hit lists of suspected terrorists.

So if we get no feedback, it is very hard for us to know what works and what doesn't work. But if we make a mistake, we know very quickly what we did wrong. And it may not have been any type of transaction or illegal money moving. It could have been just that they didn't like our policy, they didn't like our program.

It seems there has to be some kind of safe harbor to say, you have a decent program. One of the analogies I use from my old farming days is we are looking for a needle in a haystack with BSA. If we can make that haystack smaller, we have a better chance of finding that needle.

So why don't we look at the things that work and do those and maybe do more of those, and look at the things that don't work and let's stop doing that.

Mr. SCOTT. So one of the things that you are saying that has worked are these financial units. You don't see a problem there?

Mr. DEVAUX. No, not at all.

Mr. SCOTT. Okay. And the fact that so many of them are manned by former law enforcement people certainly could help with getting the communications.

Is that right, Mr. Baer?

Mr. BAER. Yes. And I wanted to add too, although there aren't really policies and procedures for it, banks of all sizes are very good, I believe, about alerting law enforcement when they actually see something that is truly suspicious, as opposed to just an alert you have to file because it hit some parameter. There is actually a term for this now called "super SAR." And banks actually walk those into the U.S. Attorney's Office or the FBI, or whomever, and say, look, we filed the SAR like we always do, but this one really means it.

Mr. SCOTT. All right. Thank you, sir.

Chairman LUETKEMEYER. The gentleman's time has expired.

The gentleman from Pennsylvania, Mr. Rothfus, is recognized for 5 minutes.

Mr. ROTHFUS. Thank you, Mr. Chairman.

Mr. Baer, in your testimony, you described the current AML regime as, "inefficient and outdated and driven by perverse incentives." You described a system where financial institutions face broad reporting requirements and file large numbers of SARs, some of which are purely defensive in nature.

I think we can all agree that our BSA/AML regime should seek to provide law enforcement with actionable intelligence that they can actually use rather than volumes of SARs that waste resources and provide minimal value to law enforcement.

With this in mind, do you believe that the provisions of the Bank Secrecy Act with respect to required reports of suspicious activity by financial institutions are overly broad and, as a result, produce too many reports that are not particularly useful to law enforcement?

Mr. BAER. It is a great question and it is very difficult to answer. There was a time when we used to say there were too many SARs and it was adding hay to the haystack and making it more difficult to find needles. That was when someone was actually reading every SAR.

You can actually argue now that no one is reading them in the first instance and you are just running word searches against them. Why not have more SARs? That is just more data to search.

The real problem there, though, and with a SAR database is—again we have heard this from the big data folks—that the SAR database is filled with noise because you're filing a bunch of SARs on low-level, low-dollar offenses that no Federal prosecutor would ever look at, and then it is really the absence of a feedback loop.

It is just not a smart database. It is not necessarily more or less, it is more, how are you going to search that database and how are you going to get feedback so that you are searching it smarter and smarter every day?

Mr. ROTHFUS. Are there any changes you would suggest to the reporting requirements, or is it more the feedback loop that you are looking at here?

Mr. BAER. On the reporting requirements, for example, there is no dollar limit for insider abuse. So if you think a teller is taking some money and decide to let him or her go, you actually have to decide whether to file a SAR on that, even though, again, there is no Federal law enforcement official in the world who will ever bring a case on that.

The dollar limits have not been raised, I believe, since the BSA was originally enacted with regard to other low-level offenses. So for a $2,000 theft, you are filing a SAR.

And I think as both Ms. Anderson and Mr. DeVaux noted, that is a lot of resources, because you actually have to investigate those like a law enforcement agency. And so you could take massive resources away from those low-product, low-utility efforts and put them to much more useful purposes.

Mr. ROTHFUS. The report that The Clearing House issued, "Redesigning the U.S. AML/CFT Framework," discusses the possibility of setting up a no-action letter procedure at FinCEN. This would allow financial institutions to query FinCEN on enforcement issues. Could you describe how you would envision no-action letters working in this context?

Mr. BAER. I will give you one example. With respect to sharing of information among firms under 314(b), that is actually permitted with respect to two categories of offenses: anti-money-laundering; and terrorist financing.

It is not quite clear what anti-money-laundering means with respect to that exception, because just about any crime involves having to launder the proceeds of it. So, for example, in that area, you would be able to write in and say, "Is this sort of offense the kind where I could share information with another financial institution to the extent I am investigating that conduct?"

But there are millions of questions like that where firms have a very difficult time knowing what the exact right answer is and are at great risk if they get it wrong.

Mr. ROTHFUS. Mr. DeVaux, in your testimony, you suggested that there are deficiencies in how Section 314(b) of the USA PATRIOT Act has been implemented. As you know, this section encourages banks to share information with each other. Specifically, you wrote, "The restrictions and red tape surrounding its use make it impractical."

What are some of these restrictions that hinder bank-to-bank cooperation?

Mr. DEVAUX. There are always privacy issues related to sharing information. In order to share information with another bank, you have to first file with FinCEN. And before you share, you have to also be certain that the other institution has filed with FinCEN. And then you can share information.

And the process is not as smooth as it should be in terms of having to go through that procedure. Many banks do not do it. They just don't share the information.

Mr. ROTHFUS. Ms. Anderson, in your testimony, you wrote that it takes your credit union 3 to 5 days to process an average SAR for one case from beginning to end, and American Airlines Federal has 30 to 45 filings per month. How has technology helped to mitigate this compliance burden?

Ms. ANDERSON. We use a system that generates the cases. And so what we do to eliminate false positives is once a year, we look at the rules that we have established in the system so that we can eliminate the false cases, which takes time, because the ones that I mentioned where it takes 3 to 5 days to research, it takes that long for a true SAR, because you have to look at the deposits, you

have to look at the lending system, you have to look at what is in your imaging system.

There is a lot of research in the background to truly grasp what is going on, especially if a lot of individuals are involved. And then you have to look at all those accounts.

So what we try to do once a year is we do a quality review, and we look at our rules to eliminate those that have false positives.

Mr. ROTHFUS. I yield back. Thank you, Mr. Chairman.

Chairman LUETKEMEYER. The gentleman yields. His time has expired.

The gentlelady from New York, Mrs. Maloney, is recognized for 5 minutes.

Mrs. MALONEY. Thank you very much, Mr. Chairman.

And I thank all the panelists for your testimony.

Mr. Baer, I would like to ask you about the Beneficial Ownership bill. You and your organization, The Clearing House, have been extremely helpful on this bill and we deeply appreciate your support. And I want to thank you for that. But we both share a common goal, which is to prevent terrorists and criminal organizations from using the U.S. financial system to move their money around.

And as you know, the Corporate Transparency Act will allow financial institutions to have access to the same beneficial ownership information that law enforcement has, because we want financial institutions to know their customers, and they can't know their customers if they don't know who owns the corporation.

Can you talk about why it is important for both law enforcement and financial institutions to have accurate beneficial ownership information?

Mr. BAER. Sure. Thank you, Congresswoman.

Actually, I think you noted this morning, which I think is a really important point, that the greatest benefit from that legislation is actually outside the banking system. As you noted, sophisticated criminals, or kleptocrats, know not to use the banking system. So they use LLCs to set up—to hold real estate or diamonds or art or whatever it is. So even if you left aside the banking system, there would be a great reason to enact the bill.

For banks, they already are under, as we have discussed, a customer due diligence requirement from FinCEN, that they know their customers, and if it is a corporate customer, that they know the beneficial owners of that corporation.

Currently, that is a game of hide-and-go-seek where they have to ask and then investigate. If they had access to an established database filed under penalty of law where a corporation had to identify to the State or to FinCEN who the beneficial owners are, obviously that would reduce the burden on the bank, it would reduce the risk of getting it wrong, and that is all to the good.

But I think the primary reason we support the legislation goes beyond those marginal reductions in cost and risk and is more just to having a much safer system and a much safer country.

Mrs. MALONEY. But it would be a substantial benefit to financial institutions as it would reduce the regulatory burden on those institutions?

Mr. BAER. No. Absolutely.

Mrs. MALONEY. It was interesting in the "60 Minutes" show that was done on the hiding of money in America, that in that show they interviewed 15 lawyers, and all of them were cooperating in trying to hide money in America.

What I thought was very interesting was they all said, don't go to a bank, whatever you do, don't go to a bank, because they are going to know their customer, and that is not a good place to hide your money.

It was disturbing to me to see the American legal system cooperating with an alleged criminal on how to hide money, but it shows that the banks have been successful in knowing who is there. But every single one of them said, "Don't go to a bank, go to these LLCs, we will help you set it up."

How many banks are part of your clearinghouse?

Mr. BAER. It is basically the 25 largest commercial banks in the United States.

Mrs. MALONEY. And are they all supporting this legislation?

Mr. BAER. As well as we can determine, yes. We have asked them repeatedly, and they are all for it, yes.

Mrs. MALONEY. I appreciate it. I represent an area that has a lot of terrorism financing. And any way we can crack down on it makes America safer. So thank you so much.

I would also like to ask the gentlelady, Ms. Lowe, and you have been very supportive of this bill too, which we introduced today with your support. And can you talk a little bit about why you think it is important? And how will this help crack down on terrorism financing in America?

Ms. LOWE. The issue of anonymous companies and beneficial ownership is not simply a U.S. issue. It is, certainly, a global issue.

The U.S. started off actually quite strong many years ago, trying to push to make it more difficult to create anonymous companies, but has actually fallen quite far behind many other countries in actually operationalizing that.

The U.K. today, for example, has a completely publicly available register of beneficial ownership information that, for example, U.S. law enforcement could access, U.S. banks could access now as they wish.

So terrorism finance today, as you have heard in many of your hearings last year, is not something that is done only by terrorists. There are a lot of people working together among the criminal systems around the world, and that is terrorism folks working together with organized crime, working together with human traffickers, because they are all using the same systems.

And a fundamental vehicle for moving any of this criminal money is unanimous companies. Again, that is global.

The U.S. is particularly important in this area—

Chairman LUETKEMEYER. Very quickly.

Ms. LOWE. —because we do incorporate the largest number of companies in the world, and the rest of the world thinks that they are very legitimate.

Chairman LUETKEMEYER. The gentlelady's time has expired.

The gentleman from North Carolina, Mr. Pittenger, is recognized for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman.

And I thank each of you for your expert testimony today.

Previously, I had drafted legislation to strengthen and clarify Section 314, information sharing mechanisms that were written in the USA PATRIOT Act.

How important is it for us, in our anti-money-laundering regime, that we fully enable vital information-sharing between the government and financial institutions, and between the financial institutions themselves? And in this legislation, part of our objective, of course, was to streamline this process, enabling the government to focus in on those entities that would be a strategic importance to them.

Yes, sir?

Mr. BAER. Yes. Congressman, I think it is very important. I think it is important, under the current paradigm, where I think it is more a matter of banks picking up the phone and calling each other to the extent that they share a customer and want to know if they are seeing the complete picture.

I think in a future paradigm, where there was, again, more use of data. I have been taught by the data folks that the importance is not the algorithm, it is how much data you are running that algorithm against.

If you have a customer who has four bank accounts, you would certainly want to see the behavior in all of those accounts in order to determine whether it is truly suspicious or troublesome. So, whether it is the informality now and picking up the phone, or whether it is a future state where you are actually sharing data in real time, I think it is important in both cases.

Of course, there are privacy concerns here, and we respect those. I think those should be addressed, but they seem solvable.

Mr. PITTENGER. In respect to that, and when you consider—and I will get to the privacy issues, if the government was able to identify those particular entities that they wanted you to respond back to, that in itself, it seems to me, would provide greater privacy for those relieving you of others that you would not have to be engaged with.

Would you concur with that?

Mr. BAER. Yes. I agree, Congressman.

Mr. PITTENGER. Ms. Lowe?

Ms. LOWE. Thank you. Just to add, moving forward and looking at this issue, I think you need to be looking at the international data privacy regulations in place. The internationally-operating banks are very much bound by those, and what they can and cannot share. The European Union, in particular, has had the strictest regime, and that is a pretty wide-ranging regime. And they just adopted a new directive in May on this that will come into effect in May of 2018.

Around the world, countries generally have adopted either this sort of European approach or the American approach, and so it is sort of a hodgepodge out there in the world as far as how these data policy restrictions interplay with the information-sharing. But I think it is something that this committee should look at in that sort of much wider context, understand what we can and cannot do and how to make that better.

Mr. PITTENGER. Mr. DeVaux?

Mr. DEVAUX. Yes. I agree 100 percent. The 314(a) list is a list of people of interest, and I would like to get that list. That is a very efficient activity. We can just run it against our database. If we get a hit, we report it.

I think about the situation where you may have people who are criminals—or doing criminal activity, and they are not banking at just one bank. They are banking at four or five banks, and they could be moving money around.

You can imagine the scenario where five banks are writing a SAR on the same person. If there were ways to better share this information so we could get the information out there, we might save a lot of that redundant work.

Mr. PITTENGER. And part of your objective is to have a safety capacity where you would be protected from litigation sharing information one with another as well. Is that correct?

Mr. BAER. I probably reaffirm Ms. Lowe's point, in the sense, internationally, there are now currently restrictions on the ability of a given bank to share even within the bank to the extent there is a foreign affiliate, or even branch involved. So that is a very real concern.

Mr. PITTENGER. Ms. Anderson, do you have a comment?

Ms. ANDERSON. I just wanted to echo the remarks made by Mr. Lloyd DeVaux. We would also like to share information, but as was previously mentioned, you are limited to only two instances where you can share information.

And at credit unions, we have what is called shared branching, where if they are involved in a system, they could go to another credit union and make a deposit or withdrawal. And so it would be great if we could openly share that type of information so that we are not spending so much time trying to call them, or they are trying to call us so they can file a proper SAR or a CTR.

Mr. PITTENGER. You have a safe harbor where you are able to provide information with each other?

Ms. ANDERSON. Yes.

Mr. PITTENGER. Thank you very much. I yield back.

Chairman LUETKEMEYER. The gentleman yields back his time.

Ms. Velazquez from New York is recognized for 5 minutes.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

Ms. Anderson, Mr. Baer, and Mr. DeVaux, I am hearing from real estate title and settlement professionals in my district that criminals are doctoring up fraudulent wire instructions and sending them to home buyers. They make the instructions look legitimate as if they were coming from the title insurance company.

The buyer then goes to the bank and sends a wire using the incorrect instructions. These funds, then, get transferred to the criminal before a series of transfers sends the money offshore. So my question to you is, can each one of you tell me what you are doing to prevent your institutions from being used by these criminals?

Ms. ANDERSON. I would like to start. Thank you, Congresswoman.

What we do when a member wants to send a wire is that they have to complete a form, and we verify their identity. And so, to make sure that we send funds from their account, because funds can go so quickly. And so we do authenticate our members, and we

also contact them. And then depending on the dollar amount, it might have a second level of approval. That is what we try to do to discourage fraud. But also what we do, is we also have alerts that we send our members. If we see a pattern of a type of fraud, we try to send newsletters to them.

Ms. VELAZQUEZ. Thank you.

Ms. ANDERSON. Thank you.

Ms. VELAZQUEZ. Mr. Baer?

Mr. BAER. I think I will defer to the real bankers here, although The Clearing House runs a payment system. It is actually a bank-to-bank, very large dollar payment system, which I don't think would be relevant.

Mr. DEVAUX. From our perspective, one of the beauties of being a community bank is we know our customers. So when we get a wire request, in addition to the comments Ms. Anderson made, we call every customer on every wire, and we have a conversation with them. They complete a wire authorization form, and the information we call is in that form. And we verify using that form, if we don't recognize the voice, which it would be very rare that we wouldn't recognize the person on the other end.

Ms. VELAZQUEZ. Does your AML program detect these crimes? And if so, how?

Mr. DEVAUX. Every wire in and out of the organization is run through OFAC, first of all. Also, we run OFAC every single night on every single customer, and on every transaction that comes in and out of the organization. I talked about the 314(a) list, which is a list of people of interest to FinCEN.

I like OFAC. OFAC is easy for us. We run the list against our database, so we know the people they are looking at, and the places they are trying to avoid sending money to; therefore, it is very, very efficient.

Ms. VELAZQUEZ. Thank you.

Mr. DeVaux, how can Congress help facilitate greater communication from FinCEN and a better relation between law enforcement and financial institutions?

Mr. DEVAUX. The first thing, as I said earlier in my paper, would be to share information with us, to tell us what is working and what is not working.

It is very difficult for us to know the things we do that are valuable and the things we do that are not valuable. And sometimes, everybody gets busy and doesn't take the time to step back and take the bigger view and say, okay, what is working?

I think if we could focus on the things are working and maybe even do more of the things that are working and stop doing the things that don't provide value, I think it would help the entire system be better.

And I mentioned earlier, there is so much redundant work going on, so if we had the ability to share through some type of database, or some type of sharing agreement where we could not have to repeat all the work that has been done dozens of times by other organizations, it would save us a lot of resources.

Ms. VELAZQUEZ. Thank you.

I yield back, Mr. Chairman.

Chairman LUETKEMEYER. The gentlelady yields back.

The gentleman from Colorado, Mr. Tipton, is recognized for 5 minutes.

Mr. TIPTON. Thank you, Mr. Chairman.

I thank the panel for participating today, on a very important issue. We appreciate the efforts you all are making on this.

Mr. DeVaux, you commented that your compliance department has grown significantly. In fact, you have the largest compliance department when it comes to the AML. Is that accurate?

Mr. DEVAUX. Yes, Congressman. That is accurate. In fact, it has doubled since 2011. But what I am talking about here is the compliance department and the direct expenses related to compliance.

We have 45 employees, and all 45 employees are in BSA, not just the 6 who are in the compliance department. Every customer who walks through the door, you have to follow the know-your-customer rules in the CIP program. You have to go through an extensive process to identify who that customer is.

The frontline officer who is dealing with that customer has to build a profile of that customer to know what type of activity, where every dollar is coming from and where every dollar is going to go, and the level of dollars and types of transactions.

And we have to train across the entire organization on the four pillars of BSA. You have to train every person in the organization specific to their responsibilities in the organization. So when they should be out developing business and trying to generate new customers, they are spending a lot of time trying to onboard customers. And if an alert comes up, they are the ones who make that phone call back to the customer to get more information.

If a lender is trying to do a loan, they have a lot of responsibility around gathering BSA information. So instead of being able to call on five customers that day, they can maybe call on two, because the process takes so much longer.

Mr. TIPTON. Great.

Ms. Anderson, Mr. DeVaux, maybe you both would like to be able to address this. Earlier this month, the Treasury Department released a report on the current state of the financial system. And following the release, I wrote a letter, which is currently being circulated among membership or cosigners encouraging Federal regulators to institute policies requiring greater coordination for supervisory exams.

In your testimony, you recommended that BSA/AML reform include minimizing duplication of some or similar information as well as greater regulatory examination consistency among regulators to minimize the regulatory overlap.

Can you expand, perhaps, on why this is an important issue, not only for supervised entities, but also for the regulators themselves?

Ms. ANDERSON. Yes. The reason that it is a burden is because from the regulator's point of view, they usually have agreements with FinCEN on the examination process. And there is such a high threshold with BSA that if you have one minor inadvertent mistake, you are written up. So what our compliance department does is prior to our examiner coming in, we review the whole BSA program from top to bottom, and that is where we have three people dedicated to reviewing that we filed all the SARs timely, that we didn't have to file any amendments, that our CTRs look right. We

look at all our risk assessments. Because, unfortunately, the way that it appears that the agreement is between the regulators is that BSA has a higher threshold than if you would have, for example, errors in lending.

In lending, they may make informal comments, the examiner will. But if it is something to do with BSA, they will automatically make it a finding, or they could raise it to a letter of understanding, or a DOR. So that is where we spend so much time on quality control besides doing the day-to-day investigating and filing.

Mr. TIPTON. Anything to add, Mr. DeVaux?

Mr. DEVAUX. We are a State-regulated bank, a State-chartered bank, which means we are regulated by the State and by the FDIC, and by FinCEN—a lot of regulators.

We just had a CRA compliance exam that started in early April. And when it finished, by the end of April, our safety and soundness exam started, and it continued until just last week.

So we have actually had over 60 days of regulators in the bank, a $200 million bank, going through everything we do. It was the FDIC in both cases, but the exam reports then go to the State, and the State may call us up, and want to come in for a visit, and relook at some of the things that we did. So we are put through a lot of hoops in order to comply with regulation.

And, we understand as banks, we need to be regulated. We are dealing with people's money. But at the end of the day, we would rather be out enabling the dreams of our community, enabling the small businesses, creating jobs, revitalizing the economy. So let's eliminate some of the duplication so we can do that. We can spend more resources on developing our economy and developing the small businesses in our area.

Mr. TIPTON. Thank you.

And, Mr. Chairman, I think I have 22 seconds left?

Chairman LUETKEMEYER. I think you are 22 seconds over.

Mr. TIPTON. That is okay. Thank you. I yield back.

Chairman LUETKEMEYER. We are going to have to go back to basic 101 math here. Fortunately, we are Congressmen. We don't take education well.

The gentleman from Texas, Mr. Williams, is recognized for 5 minutes.

Mr. WILLIAMS. Thank you, Mr. Chairman.

And thanks to all of our witnesses today for your testimony.

And, Ms. Anderson, it is good to see you. I always appreciate when the committee brings in a Texan, and I am from Fort Worth. So thank you for being here.

Ms. Anderson, let me start with you. Banks, credit unions, are in an era of compliance. I have seen this in my own personal life. I hear this from small business owners like myself across my district. Every business is worried about making sure they comply with whatever regulatory authority oversees them.

So along those lines, let me start by simply asking this: What is involved with preparing for your Federal regulatory agency examination of BSA/AML compliance?

Ms. ANDERSON. Thank you, Congressman.

As I mentioned earlier, what we do is we—the three people do a top-to-bottom review of the whole program. And so we look at all the filings, all of the—we make sure that the risk assessment that we have is final and complete. We look to make sure that we don't have—we didn't have any errors. And if we have to file any amendments, we will file amendments.

We make sure that everyone has taken their required annual training, because when the examiner comes in, they want to make sure that besides the employees taking the training, that also the board of directors has been given training, and that if someone wasn't there, for example, at a board meeting, that we sent them the presentation that was given. We make sure that they don't have questions.

So, it does take a full 2 months. We get all the documents ready for the examiners. And we have a stack this high of the documents that we have ready for them. So it is a very time-consuming process, but we do that because we want to be in compliance with BSA.

Mr. WILLIAMS. Okay. Let me follow up.

What kind of training—you touched on this—do your employees go through on a regular basis to make sure they are up-to-date on the most current rules? You kind of touched on that. Go ahead.

Ms. ANDERSON. We do online training, because we have branches in 13 States and the District of Columbia. But what we also do is we supplement that training with personal training specific to that department, whether it be a loan officer, or the wire department, or with the teller. We do a lot of training when we see there may be deficiencies.

So we are always training our folks to make sure they are always catching and reporting to us any suspicious activities.

Mr. WILLIAMS. And every now and then you try to do some business, right?

Ms. ANDERSON. Yes. Thank you.

Mr. WILLIAMS. Let me follow up. I have always said that banks, credit unions, and small businesses are the first people you turn to when you need something in your local community, whether it is sponsoring the Little League team or donating an item for charity. And you all are certainly pillars of our community, and people know that.

In your testimony, you said that the American Airlines Credit Union was previously able to conduct online training for employees spread out over the 13 States. But now you must supplement that online training with one-on-one customized training, combined with the BSA/AML training every year for all 600 employees. This is, obviously, a huge burden to all employees.

So my question is this: In general, have the increased, BSA/AML compliance costs caused your credit union to miss out on opportunities to serve your community like we are talking about?

Ms. ANDERSON. Yes. I always feel, and I am sure other financial institutions do, that you never have enough people who are working in BSA. So I always try to ask for an additional head, or we always try to make sure we have the best technology so that we can support the BSA regulations.

Mr. WILLIAMS. My last question would be, how do these burdens that we are talking about, BSA/AML compliance and reporting, affect the credit unions, aside from just the training commitment?

Ms. ANDERSON. It takes resources away from the credit union as a whole, because those resources could be spent elsewhere on providing better products and services for our members.

We could do more. Other types of services, like offering to maybe beef up and hire more loan officers, or maybe hire more credit counselors, but because of the BSA regulations, we are staffed up for BSA, because it is such an important area, and it is looked at very closely.

Mr. WILLIAMS. Thank you. I appreciate you being here, and I yield my time back.

Chairman LUETKEMEYER. The gentleman yields back. With that, we go to the gentlelady from California, the ranking member of the full Financial Services Committee, Ms. Waters. You are recognized for 5 minutes.

Ms. WATERS. Thank you very much, Mr. Chairman.

And I would like to thank our witnesses who are here today.

I have wrestled with what we can do to deal with violations of the BSA/AML. And at the same time, I share some of the concerns about the smaller banks and smaller institutions that are having difficulty, for any number of reasons that have been identified today.

But here is what is causing us to be very concerned in this general area. In recent years, we have witnessed a seemingly endless stream of money laundering violations by some of the largest global banks, with Deutsche Bank being the most recent large global financial institution to disregard the anti-money-laundering requirements contained in the Bank Secrecy Act. Given that large mega banks continue to treat our current BSA/AML enforcement penalties as merely the costs of doing business, it is what is driving our concern.

When I take a look at some of the banks, big banks that have been involved with the money laundering, or at least disregarding any efforts that should be made to do the kind of detection that has been discussed here today, for example, in 2014, BNP Paribas, the world's fourth largest bank, agreed to pay $8.9 billion for knowingly and willfully moving over $8.8 billion through the U.S. financial system on behalf of three countries the U.S. had already sanctioned for acts of terrorism and other atrocities.

In 2012, HSBC agreed to pay $1.9 billion in U.S. fines while allowing itself to be used by money launderers in Mexico and terrorist financiers in the Middle East. HSBC allowed Mexican and Colombian drug cartels to launder at least $881 million. And in another case, HSBC instructed a bank in Iran on how to format payment messages so that its transactions would not be identified as an Iranian entity, and be blocked or rejected by the United States. Again, with Deutsche Bank, it was $41 million for anti-money-laundering deficiencies.

So given all of that, and our concerns about the smaller banks, what would you recommend that we do that could be helpful to smaller banks and credit unions, but at the same time, not interfere with our ability to deal with what I have just described?

Ms. Lowe?

Ms. LOWE. Thank you, Congresswoman Waters. There is no doubt that there have been some very willful and very egregious cases over the past several years that have come down in this area. And as I noted in my testimony, they are almost entirely based on what are, essentially, violations of the BSA/AML procedures. But when you look at the cases, you see so, so many hallmarks of actual money laundering, but there is no criminal prosecution related to these, not of the individuals nor of the banks.

There are a number of reasons for that, as I mentioned, potentially. But what the DOJ tells me is that they don't have enough evidence to actually bring a prosecution against a person. I find that very difficult to believe when I read the statement of facts, because those statements very often contain things like emails, where people are exchanging emails about exactly what they are doing, and they know they shouldn't be doing it, right?

So I find that difficult to believe. I want to really understand better why we are not prosecuting the individuals who are actually perpetrating these actions.

I think that when a bank is fined, its bankers say, Oh, that is terrible. I think when a banker goes to jail, his fellow bankers say, Oh, that is not going to happen to me, and I am not going to do that. So I think we need to be focusing a lot more on individuals.

Sally Yates made a memo in 2015 to this effect. I would like to see us, actually, following through on that.

Ms. WATERS. Ms. Lowe, I understand that some of the drug dealers that these banks were dealing with have gone to prison for long periods of time, but their enablers in the banks have not been penalized personally. No head of a bank, no CEO, has been placed in prison for knowingly laundering drug money.

Ms. LOWE. That is correct. With respect to the very large cases, that is correct.

Ms. WATERS. I yield back the balance of my time.

Chairman LUETKEMEYER. The gentlelady's time has expired.

The gentlelady from Utah, Mrs. Love, is recognized for 5 minutes.

Mrs. LOVE. Thank you so much for being here today.

As a former mayor of a growing city, when I first started off at the city council, our city had a population of about 7,000 people. And it may seem like it is an easy task, because there wasn't very much going on. You tend to learn that all of the decisions you make at the very beginning you end up either reaping the benefits of, or suffering the consequences of the decisions that you make very early on.

But it is really interesting, as the city grew, the first people who were in our cities were our credit unions and the banks. And a lot of people kept asking, why do we have so many banks, and why do we have so many—they were the ones that were coming.

And it wasn't until later that we realized that the small banks that were there, and the credit unions that were in our community, were the ones that were the lifeblood of our community. They were the ones that were helping support all the city events. They were the ones that were actually the financial credit. They were the ones giving the financial credit to all of our businesses that were there,

and our city grew from, at that time, 7,000 to, when I left, over 27,000, a viable, growing city.

And I am so glad that I didn't listen to all of the people who were saying, we don't need any more banks, just start getting other businesses, because they were the ones that were a great foundation for our city.

So I want to focus on striking the right balance of oversight and regulation. And I guess the question that I have—and, Ms. Anderson, if you can help me answer this, and we can go down the line as quickly as we possibly can, what kind of analysis must an institution conduct to provide adequate oversight and monitoring in compliance with BSA? I haven't been here for the whole hearing, so if you answered this already, please forgive me.

Ms. ANDERSON. What we look at, when we look at suspicious activity, is we look at if there is a lot of money being transferred. We look to see whether that person has the salary from our records to justify that amount of cash in their account. And then we look to see does the cash stay—does the money stay in their deposit account, or is it quickly moved out? And then, is there more than one individual? Is there more than one individual who has access to the accounts? And where is the money going? Is it going overseas? How long does it stay there?

And so that is, for example, when we would file, because the funds are unknown. When we determine from our system that they are trying to avoid us filing a currency transaction report, when they deposit, like, more than $10,000, we also then file suspicious activity report, as do others here.

Sometimes it is more complicated, because you have to look at many accounts if there is more than one individual, or the individual may have other accounts where they are joint with other people. And so that is why it takes so long to investigate when it is a true SAR filing, because it just looks suspicious on our end. We don't know if it is legal, but it doesn't look right based on what we know about our members.

Mrs. LOVE. Okay. So, obviously, a lot goes into that. And, also, what is the result of the failure to comply?

Ms. ANDERSON. So if you don't file, then there is no safe harbor. You are written up. There could be fines, especially if they find it to be willful. And so, I know some institutions, if—sometimes if we are not sure whether we should file or not, we will file, because there is a safe harbor for filing.

And then if we decide not to file, we keep a spreadsheet of the reasons why we didn't file so that our examiner can see that we have good reasons for not filing.

Mrs. LOVE. Okay.

Mr. Baer, Did you have something you wanted to add to that?

Mr. BAER. I think that was very well-stated. I think the only information I would add, and Mr. DeVaux and I were talking about this earlier before the hearing began, is that most of these banks are running proprietary systems that they purchase from a vendor, that basically generates the alerts, and then it is up to them to investigate. A lot of the burden comes around, where do you set those dials? You can set those dials to generate 100 alerts a month, or 1,000 alerts a month. And I think one of the concerns that banks

of all sizes have is the regulators will tell you, you know what, you only generated 100 alerts. We want you to generate 500.

But we are not aware of any analysis around why that is. And certainly, we are not aware of any analysis about the quality of the SARs that are being filed and how many of them are actually leading to prosecutable cases. And that is where, when I talked earlier about, sort of, the big data problems here, it is a system that is just fundamentally lacking in rigor in terms of the metrics for assessing whether it is being successful or not, and that is not a very good system.

Mrs. LOVE. Right. As I look at all of this—my time has expired, but as I looked at all of this, striking that right balance is incredibly critical, because again, these institutions in the small communities can make or break that community.

And, again, thank you for your expertise. I really appreciate it.

I yield back.

Chairman LUETKEMEYER. The gentlelady's time has expired.

The gentleman from Washington, Mr. Heck, is recognized for 5 minutes.

Mr. HECK. Thank you, Mr. Chairman.

I would like to preface this by stipulating to the consensus point of view that anything we can and should do in this area does not compromise our efforts in fighting terrorism. I think that is something on which we all agree.

That said, I am among those who believe that there is fertile soil here to cultivate regulatory modernization, as I would call it. And that has been brought about, my point of view that part has been brought about by two things. The first is I took it upon myself earlier to go on a tour of all the banks, big and small—not all, but many, many credit unions, big and small, in my district, to ask about what had happened to their regulatory compliance burden over the years.

As you might imagine, it had increased very substantially, most graphically represented by piles of paper. I wish some of you had brought the piles of paper in.

And probably the most common complaint I got, frankly, was about SARs and compliance with the Bank Secrecy Act and anti-money-laundering, in fact, the preponderance over majority. And I am not trying to pick a fight at all, but I found it interesting that in the main regulatory relief bill we passed here, the CHOICE Act, there were—count them—exactly zero words related to bank secrecy, or anti-money-laundering, and that was the chief complaint that I got.

And it just seems to me, however—and I will offer this as a friendly suggestion to the Chair, because I am grateful for this topic being heard, that it would be nice to hear from law enforcement as well. We learn more when we hear from both sides.

I think about the CTRs. It defies my comprehension that we cannot update that to reflect inflation, but I want to hear what the other side says. I think other work product would be better if we had had an opportunity for that conversation.

I also want to suggest, Ms. Anderson, I have asked over and over and over again for people to give me concrete examples of how we can improve regulatory burdens on financial institutions, and I

found your testimony to be refreshingly specific and concrete. And I thank you for it very sincerely.

The second reason I got very involved in this was when FinCEN published their guidance for banks serving marijuana businesses in the State of Washington, which the voters approved, as you know, they chose to legalize it and to regulate it; that guidance says that banks are required to check to make sure that marijuana businesses aren't violating any of—yes, count them—14 Federal priorities on marijuana. They are intuitively obvious: Don't sell to minors, don't sell across State lines, et cetera. That struck me as an incredible compliance burden, frankly, on these organizations. But you know what, our State regulators had an unbelievably clever solution. Because the DOJ, the other hand, asked the State regulators to check against the same 14 Federal priorities.

So here is what happens in our State: The banks are able to look directly into the database of the Liquor and Cannabis Board, our State regulator, to see if there are any red flags for businesses. They are able to largely rely on the State to check for conformance with the 14 priorities, and then piggyback on that work instead of duplicating it.

And so my question is, how can that be a model for reform for other SARs filings? What statutory changes would be required in order implement it if there is a possibility of doing this kind of creative database sharing very efficiently, very quickly? Any of you?

Mr. BAER. This sort of gets to the questions about AI, at least with regard to the largest firms that are my owners. We think there is extraordinary potential for—"utility" may be the wrong word—sharing of expense whether it is around account opening or account monitoring. And also, sharing of data in order to make the algorithms work better. So, we think that is clearly the future here. That is where this database is going to end up going. As I said earlier, you are having 2 million SARs filed a year. So this is no longer a personal need law enforcement proceeding.

Mr. HECK. If I may, sir, on the issue of the number of SARs filed per year, when the financial institutions submit SARs, if there are multiple financial institutions involved in that SARs, we are required to do duplicate investigations, and if there is a correspondent bank, a triplicate investigation, why doesn't it make sense to just kick it up to the financial institution in that chain and say, It is your responsibility to do this? What benefit is there to multiple SARs, when it is the same transaction?

Mr. DEVAUX. Right. There isn't. And then I think there is another case where you may have somebody who is banking at four different banks. None of them file a SAR. But if they all had shared the information about that customer, the lights would have gone on, and they would have said Oh, yes, we should all be filing a SAR. So that is also a potential concern.

Mr. HECK. Thank you. My time has long expired.

Thank you for your indulgence, Mr. Chairman.

Chairman LUETKEMEYER. Thank you. The gentleman's time has expired.

And to respond to your suggestion, Mr. Heck, the problem with bringing in law enforcement to this particular committee, is that it actually goes into the purview of the Terrorism and Illicit Financ-

ing Subcommittee. And so our intention is to work with the bank side of the issue here, and then marry this with, perhaps, a bill or suggestions or guidelines with the other subcommittee, which is doing very similar work. And that is what we want to try to accomplish here. So I appreciate your suggestion.

Mr. HECK. And I appreciate the explanation very much, Mr. Chairman.

Chairman LUETKEMEYER. The gentleman from Georgia, Mr. Loudermilk, is recognized for 5 minutes.

Mr. LOUDERMILK. Thank you, Mr. Chairman.

And I thank the panel for being here. I would like to direct my question, really, around the transaction amount, the amount that triggers the reporting and the investigation.

I believe it was 1970 when this was enacted. The first time I found out about the BSA was when I left the Air Force in 1992. I was living in Alaska, and moving back to my home State of Georgia, so we sold our house. Fortunately, we made a little equity on it. I had a truck with a trailer packed full of everything that I owned, and I was leaving Alaska to go to Georgia—and, actually, I was going to start over, start a new business, open a bank account. So I asked the bank to give me all of my money, and they wouldn't. They said all we can give you is less than $10,000. I ended up getting my money through multiple transactions, but that is when I found out that they were reporting it.

And as I was thinking about this, around 1970 I was still in elementary school. My dad bought a house, paid $25,000 for this house. When my dad passed away, we sold this house. And it was in much worse condition than when he bought it. The neighborhood had gone downhill. We sold it for over $100,000. When I am looking at $10,000 in 1970, $10,000 today is not the same thing. It has to be that transfer of $10,000 is done multiple times on multiple accounts, especially, when you think of somebody who has a sub S corporation, or some type of pass-through through the businesses has to happen.

I am a small business owner. Several times in a month, we would have transactions of $10,000 or more happen quite often.

I know two of you, in your statements, mentioned that if you adjust it for the rate of inflation, we are looking at somewhere around $60,000 today. Is that correct?

Mr. DEVAUX. So, $64,009.

Mr. LOUDERMILK. Okay. I believe the credit union said about $58,000 is what you guys calculated. You are using different interest rates now. So you may want to up yours. People invest more in credit unions. But let's start with Mr. DeVaux.

What do you think the appropriate threshold should be? Is this a crux of part of the problem that we are having?

Mr. DEVAUX. It is a good question. And the issue we have, without knowing how the information is used, what is valuable, what is not valuable, it is very tough for us to say that it should be $5,000 or it should be $25,000.

It came about in 1970. And if you run it through CPI, it is $64,000 today. Or in other words, as you stated, $10,000 buys $1,500 worth of stuff today.

So without us having feedback, saying, here is how we are using the currency transaction reports (CTRs), and here is what works and here is what doesn't work, it is very difficult for banks on their side to be able to pick a number that works.

Mr. LOUDERMILK. Okay. Ms. Anderson, would you like to respond?

Ms. ANDERSON. Yes, for currency transaction reports, that is where we would have to file if there is a deposit or withdrawal or $10,000 more in cash. I was looking at a recent month in our activity for what we receive. So if the currency transaction threshold was increased just to even $20,000, we filed 27 when it was $10,000 and above. But if it was increased to $20,000, our filing sort of dropped to just 5. So that would be of great benefit, because if you don't file a CTR within 15 days, there is a large penalty. So we are always on the clock to file that.

From the suspicious activity point of view, from the subpoenas that we have received that I am aware of, it seems that law enforcement goes for the larger dollar items. They are not concerned with $10,000 or $25,000. It seems like they go for a larger amount. So maybe just, in the interim, try doubling it just so see so that it is $10,000 minimum instead of the $5,000, where you know who the perpetrator is, then maybe instead of $25,000 where you don't know who the bad person is, you increase it to $50,000.

At least just try it, and we can at least determine if there is anything there. And it would be very helpful if when we respond to a subpoena and they finally do go after the bad people, that we do receive some validation that, Oh, yes, because of your institution, we were able to go after this person or that person or that ring of criminals.

Mr. LOUDERMILK. I'm running out of time here, but you do believe that we definitely need to address what this value is; I think that is what I am hearing. But we really don't know what it is unless we get proper feedback from law enforcement. Is that kind of a good summary?

Mr. Baer, I see you—

Mr. BAER. Yes. I refer to it in my testimony. It is the last piece of the puzzle argument. There will always be a case where an $11,000 transaction was the last piece of the puzzle in some investigation. Just the way you can end up arresting somebody for jaywalking, and they turn out to be a horrible criminal, but that doesn't mean you increase your jaywalking arrests. You actually have to do a cost-benefit analysis, and think, how much did that last piece of the puzzle cost you? And that is where Mr. DeVaux has it exactly right, which is we don't know because there are no metrics or analysis around it.

Mr. LOUDERMILK. Thank you, Mr. Chairman.

Chairman LUETKEMEYER. The gentleman's time has expired.

The gentleman from Michigan, Mr. Trott, is recognized for 5 minutes.

Mr. TROTT. Thank you, Mr. Chairman.

Before I begin my questions, I want to allow my good friend from Colorado to ask a follow-up question. So I yield to Mr. Tipton.

Mr. TIPTON. Thank you, Mr. Trott, for yielding.

And, Mr. DeVaux, I just want to be able to follow up a little bit on some of your testimony, in terms of some of the examination and compliance between smaller banks like yours, and larger banks on the reporting.

Do you basically feel that since you are smaller, some of the activity actually gets magnified, as opposed to a bigger bank, when it comes to some of the compliance?

Mr. DEVAUX. Yes, sir. It is a good question. And I think what happens is regulators are trained in a certain way. And they don't really see a lot of times the bank size or the risk of the bank. They just know how to do their exam. And so whether they are walking into a big bank or a small bank, they are applying all the same rules. They are looking for all the same percentages.

As I mentioned earlier, we had 7,100 alerts generated last year. From those alerts, we filed 15 SARs. And we feel like we could tune our alerts a little better, and probably still get 14 or 15 SARs out of it by not doing so much work.

A lot of times—and I am not trying to be critical of regulators—it comes down to personality or the person who comes through the door. What is their specialty? What is their expertise? You can go through an exam at a bank 3 years, 3 times. On the fourth time, you get a different regulator, and the whole story changes. And what was good before is now bad, and what was bad before is now good. So it is an issue for us.

Mr. TIPTON. Thank you.

I thank the gentleman for yielding to me, and I yield back.

Mr. TROTT. Thank you.

Mr. DeVaux, I want continue to follow up on what you just said. And one of my concerns is the heavy hand of the regulators. So very quickly, I heard stories that examiners tell institutions to file a certain number of CTRs and SARs or be written up for having a bad audit. Is that happening, to your knowledge?

Mr. DEVAUX. Yes, sir, it does happen. For clarification, on the CTRs, when the transaction is over $10,000, it is clear, you file a CTR. You file a currency transaction report. So if they ever come back and say, you are not filing enough, it is because you didn't file something that you are required to file. But when it comes to SARs, and when it comes to high-risk accounts and high-risk reviews and investigations, that is where the regulators want to see a certain number in a lot of cases.

You can run your database, you would get 3 or 4 percent high-risk accounts, and they can come back and say, you know what, this seems a little low. Maybe you should change your parameters and rerun your database again. But for me, a high-risk account is a high-risk account. It doesn't matter what your parameters are. It doesn't change just because you change dollar amounts and other things like that.

Mr. TROTT. Thank you, sir.

Ms. Anderson, on the same lines, do you ever feel that the government uses the complex regulations to set banks and credit unions up to fail, or if not to fail, but to find a supposed error and then use that error to try and leverage the bank or the credit union to make—get some other concessions as part of the audit?

Ms. ANDERSON. Yes. From just what I have heard from other credit unions, it does appear that Bank Secrecy Act exams are more—can become a "gotcha," especially when—if you are looking at the whole examination, not just BSA, but lending, the call report filing. And we have seen where you have just a minor discrepancy, for example, use a P.O. Box instead of the street address. Clearly, we had the street address, it was just a minor issue. But you don't fight it, because you don't want to argue on that. If that is all they found, I guess that is great.

Mr. TROTT. Thank you so much.

Mr. Baer, you worked with the 25 largest banks, as you mentioned. In my prior life, I represented most of those folks. And our biggest concern was reputational risk. If we didn't do something that didn't reflect well—I used to joke that my number one goal when representing Chase was to make sure Jamie Dimon didn't know my name.

So any concern that maybe reporting a suspicious transaction or a mistake could cause reputational risk to a bank, particularly a large bank, which would thereafter cause them not to want to report that because of the risk or because of government action.

I assume it is not happening, but that would be a terrible set of circumstances if the oversight caused them not to report something they should.

Mr. BAER. No. I think all of the incentives are to file. There is a safe harbor if you file, so you are protected if you file. And it just goes into a big database.

I want to add, though, to some extent, as Ms. Anderson was talking about, the regulators, the examiners here, are in a very difficult position, too. And as I highlighted in my testimony, it is not their fault that they are in a position where they don't get to know what law enforcement is doing with these SARs or what national security is doing with these SARs.

What they know is if they don't have enough people written up, or they don't have enough consent orders, they are going to be hauled to Washington and criticized for that. And then, God forbid, something goes wrong at the institution they are examining, they are going to be held to account. And their only defense can be, I have them under a consent order. I wrote them up for 50 MRAs. It is not my fault.

Mr. TROTT. Would an advisory opinion process help?

Mr. BAER. I'm sorry?

Mr. TROTT. Would an advisory opinion process help?

Mr. BAER. I hadn't thought about that. Yes, I think that could be helpful. Yes.

Mr. TROTT. Thank you.

I yield back.

Chairman LUETKEMEYER. The gentleman's time has expired.

The gentleman from Tennessee, Mr. Kustoff, is recognized for 5 minutes.

Mr. KUSTOFF. Thank you, Mr. Chairman.

Ms. Anderson, if I could ask you a question that is along the same track, but a little bit different relating to real estate, and real estate loans.

In the last 12 months or so, according to the FBI Internet Crime Complaint Center, there have been, supposedly, over 3,000 victims who reported the actual attempt or attempted theft of almost $400 million in assets through fraudulent wire transfers related to real estate transactions. That is a big increase over the last several years. And my concern is is that these funds represent, often, the large majority of savings that are held by families who are being victimized.

And if it is not detected within a few hours or several hours of the fraud taking place, as I understand it, it becomes almost impossible to recover that money as it gets laundered and transferred through a network of accounts and fraudulent schemes.

There are sophisticated hackers that mine data to identify the victims near the conclusion of these real estate transactions. And they often mimic trusted participants, such as a real estate agent, a mortgage lender, or a closing agent, to provide transfer information that the victim has little or maybe no reason to suspect.

With the real estate-related email compromise schemes, is it common, in your experience, for the nominal payee who is listed on the instructions in the payment order not to match the holder of the account at the receiving institution?

Ms. ANDERSON. Usually for us, when the name and the account number doesn't match, it is a red flag. And so we do more due diligence. And the fraud that you alluded to, where title—the customer will receive an email to transfer the funds somewhere else, it has just recently come to our attention that that does happen.

And so we try to be vigilant in informing our members who are purchasing houses, to know to be careful when they receive emails like that.

For example, they need to be more vigilant on the side of—with their title company. And the title companies need to also be vigilant in telling their customers, we would never send you an email telling you to transfer money from this account or to another bank.

Because we do what we can for our side, for our members on our side, but it is hard to also control what is going on on the other side, because we don't know what is going on on that other side. We don't have that information.

Mr. KUSTOFF. And I appreciate you saying that.

Would your particular AML program catch that discrepancy?

Ms. ANDERSON. How that is caught is through the training that we would give, for example, to the wire folks. So while it may be caught with our system, we get the cases at the beginning of every month. It is not a live system. Our fraud system may catch it the next day, but really, it is the training that you give to your employees that catches fraud right at the beginning.

Mr. KUSTOFF. And if I could follow up on that, do you know what your credit union does to double-check that both the account number and the payee's name matches before sending a wire and making the funds available for withdrawal after a wire transfer?

Ms. ANDERSON. If we are the receiving institution, we make sure that the name and the account match, the number, but generally, it is the account number that controls. But I know that when there is fraud, working with other financial institutions, sometimes when you are able to talk to them, if it hasn't processed yet on the other

side if we are sending. But we do what we can to make sure our members' money is safe and gets into the right accounts.

Mr. KUSTOFF. As it relates to these email schemes, I would assume you are seeing more and more of those type of emails and situations relating to your customers?

Ms. ANDERSON. Actually, I just heard of one just recently, and we were able to stop it.

Mr. KUSTOFF. Very good.

Thank you, Mr. Chairman. I yield back my time.

Chairman LUETKEMEYER. The gentleman yields back his time.

With that, we go to the gentlelady from New York, Ms. Tenney, for 5 minutes.

Ms. TENNEY. Thank you, Mr. Chairman.

And thank you to the panel. I know this is a very—it has, actually, turned into an interesting discussion. I sort of have even more questions than I had before. And I appreciate you being here and your expertise on this issue.

I recently took a trip to the Middle East, to Iraq, Afghanistan, and central Asia. And one of the issues that we came across was countering the financing of terrorism, which we discussed, and how many of these banking institutions end up being financed through porous borders in Central and South America getting all the way to the Middle East, and how these are happening through banking and financial institutions.

That was a concern to me, and we had a lot of interesting conversations about what to do about that, and international banks, how to regulate banks. And what was really interesting is that most of—a lot of it is cash. So there is no way, no matter how many regulations you put out, you are not going to be able to catch the virtual needle in a haystack, which it seems you are describing today, that we have been tasked with this enormous burden to try to find a needle in a haystack by combing through thousands of tiny transactions. As you indicated, a $10,000 transaction may not net something that maybe a $500 transaction would net.

And I might reference that in 2007, we brought a New York Governor down, who ended up resigning over a $4,000 transaction in another State.

So it really isn't the amount of the transaction. It is all the information that goes into it. And it just raised a lot of questions for me, and some of those are—what would be the approach that you would recommend? Because, honestly, I am a little leery about the idea of having a central network and worrying about a lot of concerns. Are we actually going to have an open case against an individual? Are there constitutional rights there, maybe a privacy right? And balancing that with, obviously, our need to find a lot of schemes through terrorism.

I just thought I would start maybe with Ms. Anderson, or the Credit Bureau, or any small banking institutions, because many rural areas rely on you.

What would you suggest that is a better way to make it more efficient for the bank, or the credit union, and still have—being meaningful into finding cases of illegal illicit money laundering, financial issues?

What would you suggest, quickly?

Ms. ANDERSON. I think as we have mentioned before, it would be good to know what law enforcement does with our information, because right now we don't know. So even though we are filing all these suspicious activity reports, we don't know if they are fruitless or if it is helping law enforcement. So that would be one step.

And to the extent that anything can be automated, we need to make sure that smaller financial institutions, such as credit unions, have access to that, because it can be expensive.

And then, if there is anything else, I will send in written testimony. Thank you.

Ms. TENNEY. And, Mr. Baer, I am just curious. It just seems like we have this metadata type of idea. I hate to bring that in, but it sounds like we are just collecting all this data when we don't really have a defined mission. And you said we could isolate that. If you had just a quick comment on that?

Mr. BAER. Sure. I think it is kind of interesting. On behalf of the largest banks, I think I would have pretty much the same observation as Ms. Anderson has on behalf of credit unions. A lot of it is about getting better feedback and being smarter about it.

I think with regard to the international issues you talk about, there is another component, which is there needs to be—and we believe it is the Treasury Department—somebody really has to be in charge and has to put everyone in a room and decide what is the cost-benefit of banks continuing to operate in Somalia, say. That may create terrorist risks, development risks on the other side, diplomacy risks.

But that is a decision that needs to be made by somebody with a very heavy title, we think in our government, but right now it is being made by default by bank examiners where the push is always to derisk and leave.

Ms. TENNEY. Right. The pressure on banks and the pressure on banks to actually be the law enforcement as opposed to just a tool for law enforcement.

And I thought maybe I could ask Mr. DeVaux, if you could just explain—how would you eliminate this idea—how would you enhance what Ms. Anderson had said about whether it is redundant or inefficient? And what can we do to eliminate this redundancy on banks that isn't really netting what we hope it would?

I am going to lose my time in a minute, but if you could answer quickly, I would appreciate it. Thank you.

Mr. DEVAUX. I think it really does come down to sharing of information and working together. I mentioned earlier that this has to be a team approach, and there are pieces of this work that need to be done in the most efficient place.

Ms. TENNEY. Can I ask quickly, is there a privacy issue with a private citizen, with bank information, that would expose banks to liability as well?

Mr. DEVAUX. There is a privacy issue today. The more you share information about customers, the more likely customers are to leave the banks. They may want to go underground if the information is being shared too much.

So we have to balance that. But we do have to share—I think we have to share and work together.

Ms. TENNEY. Excellent point.

Thank you very much, panel. I appreciate it.

Chairman LUETKEMEYER. The gentlelady's time has expired.

The gentleman from Florida, Mr. Posey, is recognized for 5 minutes.

Mr. POSEY. Thank you, very much, Mr. Chairman.

To the representatives of the banks and credit unions, do you feel that the Federal Government initiatives, such as Operation Choke Point, that seek to disrupt banking relationships with legal, yet undesirable, according to the Administration, businesses are concerning?

Mr. DEVAUX. Congressman, that is a good question, and one I talked about earlier. When it comes down to banking certain types of businesses and certain types of customers, the burden is overwhelming. And in a lot of cases these are legal businesses, and these are small businesses. And so if we turn them away, it becomes very difficult for them to do business.

There are businesses that the regulators have deemed as high risk, and it is very tough for us to spend extra time on them when we could focus more on our communities and developing the businesses that grow our communities and grow jobs rather than have to spend all our time trying to clear BSA issues on a business that has been deemed high risk by a regulator.

Ms. ANDERSON. I would like to add to that that, yes, there are certain types of businesses that are deemed high risk. And because of that, we know that under the regulations the amount of due diligence that we would need to really get to know that business and monitor them, it would be too burdensome and not fair to the rest of our members that we are spending so much time on a particular type of business. So we actually discourage that type of business from having accounts at our credit union.

Mr. POSEY. Okay. Do you think it is pertinent that financial institutions have due process and know if they are acting in compliance with applicable laws, not ideology or certain examiners who may personally disfavor a certain industry?

Mr. BAER. I will address that. One of the other members alluded earlier to the phrase, "reputational risk," which to me is the most troubling in bank supervision currently. Because what that really means is, what you are doing is legal, you seem to have the risk under control, but I just don't like it. Therefore, it poses a reputational risk to you. Namely, because I am going to say I don't like it as your regulator.

And so it can become very circular and basically just boils down to, I don't have a legal basis for saying don't do this, but don't do this. And so whether it is BSA or in other areas, I think what banks really want is certainty and due process.

Mr. POSEY. Anyone else?

How do you know who you don't want to do business with per the government's bias against that business? How do you determine?

Mr. DEVAUX. If we don't know before the examiners come in, we know after they come in, because they spend a lot of time digging through the high-risk businesses, such as money services businesses (MSBs). I could name a few, but I won't. The regulators con-

tinue to push and ask for more information and more due diligence and more oversight.

We had one customer recently where I actually had a friend who used to be at another bank that I knew had banked the business, and I was talking to him about it. And he said, "You know what, we even had an outside audit firm come in and do a full risk assessment of this business, and they said there is no risk in this business. The regulators never stopped pushing for more information." He said: "My recommendation is, don't bank them."

Ms. ANDERSON. I would like to add to that.

So, for example, if we file two or three suspicious activity reports because we don't know the sources of the funds, we will reach out to our member and ask them, "Would you please let us know where you are getting this money, where is it going?" So we have to dig into their business. And if they won't respond to us, we don't want to keep on filing suspicious activity reports, and so we limit services.

Mr. POSEY. What would you say if I was a manufacturer of pistols, say, and I wanted to open up an account with your bank? Would you open an account with me if you know that I was manufacturing pistols?

Ms. ANDERSON. In theory, if you answered all of our due diligence questions, then we would open the account. We just need to make sure that whatever you tell us at the beginning when you open an account, what you actually do once you have an account with us matches what you told us you would be doing.

And if it doesn't match, then we would—we may file a suspicious activity report or we may go back to you and ask you what changed in your business and how come you are using more cash or sending out more wires.

Mr. POSEY. Okay. I had a manufacturer in my district, and his bank told him, "The government said you can't bank with us anymore. You have to find somewhere else." And every bank that he went to told him the same thing. That creates a life hazard, obviously, even for bad guys who know, if you are in this business or this business or that business, you can't have a bank account, so you are going to have to be a target for a large amount of cash.

Have you ever heard—Mr. Chairman, my time is up. I yield back. I'm sorry.

Chairman LUETKEMEYER. The gentleman's time has expired.

The gentleman from Ohio, Mr. Davidson, is recognized for 5 minutes.

Mr. DAVIDSON. Thank you, Mr. Chairman.

Thank you all for your testimony today. Thank you for your written testimony as well.

Mr. Baer, in particular, you provided some good position papers. And one of the topics that has come up a fair bit is information-sharing. And Mr. Pittenger's topic that he and I don't agree on, we agree on lots of things, and the safe harbor that a lot of financial institutions want.

And, Ms. Lowe, I believe you were the only one who addressed the concern on privacy there. So we have just talked with Ms. Tenney and Mr. Posey expressing some concerns. And up until now we really hadn't heard much on the concern of privacy.

Just kind of an open question, in your assessment, should Americans have any expectation of privacy upon opening a bank account?

Mr. BAER. Congressman, of course they should. The question is how far that privacy extends. Clearly, it is privacy with regard to disclosing to non-law-enforcement. And the question is, does it extend to other affiliates of that bank? Does it extend to other banks? Does it extend to law enforcement?

There are clearly very difficult tradeoffs here, and every bit of sharing for a law enforcement or national security purpose is incrementally less privacy for the person whose information is being shared for sure.

But we have seen pilot projects. For example, there is one around human trafficking with a group of banks getting together and sharing customer information with the approval, I believe, of FinCEN, and saying, can we make more cases on human trafficking?

I think there you would say, "Yes." The cost-benefit analysis there would be, yes, there was incrementally less privacy accorded those customers, but they were able to make cases they never would have made. And I think the information was cabined among the institutions that were doing that sharing.

So I do think it is a very difficult issue. But I think our lean would be towards more sharing rather than less at this point.

Mr. DAVIDSON. Okay. So let's say, yes, of course, I am for catching human traffickers, we want to stop all the terrorists, all sorts of other things. But we have the constitutional safeguards in place because we can see things that happen, as Mr. Posey alluded to, disfavored speech, shaming, and not even against the law, just not liked by a regulator. I wonder if Bernie Sanders would be okay banking Mr. Vought's church or Wheaton College or something after his testimony in the Senate recently.

So we have these protections in the Bill of Rights for a reason, which was wise of our Founders. How do you provide those safeguards today?

Particularly, Mr. DeVaux, dealing with banks in Florida there, very similar to Ohio issues, just a different State, but a lot of the same challenges with the size of banks.

Mr. DEVAUX. Privacy is a big issue. We do not share with other banks. There is a mechanism for doing that. But we generally do our investigation and we file our suspicious activity report.

But I think the same question comes to the passport office and the driver's license office, do they share that information? We are talking about money, which is an enabler of terrorism.

So, for me, I think there should be some sharing at some point along the way. Why would five banks write a SAR on the same customer or investigate a customer who looks like they are doing illegal activity when maybe they could file, I think, as I mentioned earlier, a short SAR, shoot it off to law enforcement, and they have a database of the bad guys?

One of the things I talked about earlier, also, was a list called a 314(a) list that is provided by law enforcement to us. Those are the bad guys they are interested in. So they are sharing information with us, saying, we are interested in these bad guys. We like that list. We can run that list very quickly. And we know immediately if we have any criminals and we can report back to them.

Mr. DAVIDSON. And if the 314(a) list comes in, does that come in, in terms of a subpoena, or is that just regular flow of information covered under 314(a)?

Mr. DEVAUX. It comes in as a list. It comes in as a database multiple times during the year, and we just run our database against it.

Mr. DAVIDSON. Ms. Lowe, since you addressed privacy in your written remarks, your thoughts on privacy?

Ms. LOWE. Thank you.

Privacy is definitely an issue. I think redress, some sort of way to have somebody be able to get their rights restored should there be a problem on the other end, is important.

But I think, actually, the technology today allows us to do a lot of different types of encryption and anonymization of data. And I think we really need to be looking in those areas as well to see if there are solutions, technological solutions, that can be brought to bear to really protect privacy while also sharing information in a way that is useful for law enforcement

Mr. DAVIDSON. Distributed ledger is very promising.

Thank you all.

My time has expired. Mr. Chairman, I yield back.

Chairman LUETKEMEYER. The gentleman's time has expired. And with that, we are done with our questions. And we want to thank the panel for all of your great testimony and your answers today. You were very forthcoming. We certainly appreciate that.

Just a couple of closing comments and thoughts.

We appreciate what you have told us from the standpoint that—I think Mr. Heck probably said it best, from the standpoint of we want to make sure we catch the bad guys and prohibit folks from doing illegal, illicit things. At the same time, the laws and rules we are talking about haven't been "modernized," was his term—I thought it was a good term—for a long, long time. And so we need to take a look at streamlining, updating. I think we have talked about technology is a good way, perhaps, that we need to utilize it better, to streamline the process.

Mr. Davidson brought up some good points with regards to privacy. Somehow we have to thread the needle between what is the protection of the privacy of our customers yet be able to find ways to ferret out the bad guys' illicit activities.

What works, what doesn't work. I know you mentioned the "know your customer" program. Maybe we need to take a look at fine-tuning that to find some streamlining. I appreciate your thoughts on that.

Again, it was interesting, the discussion that was had by I think Mr. Loudermilk with regards to the level at which we decide to set the determination for, that $10,000 is really a good spot. And I appreciate it.

Somebody, I think, Mr. Baer, your testimony was that $10,000 in 1970 is $64,000 today. Is that what you said? Or Mr. DeVaux. There we go. I thought that was an interesting comment, and I appreciate that, because it gives us some perspective. Maybe we need to take a look at that and maybe we need to work with law enforcement and see where the sweet spot is there.

So I think, as Mr. Heck alluded to, we are on one side of this issue from the standpoint of the banks and the money folks, the financial services industry's rules and regulations. We need to go on the other side to also figure out law enforcement's perspective and how we can interface with them and find ways to come together.

Reputational risk is something that is frustrating to me as a result of working all of these years with what is going on and the different rules and regulations, and now we have examiners doing the Operation Choke Point stuff, which is all based on reputational risk. And a lot of it is not really on illicit activity. And so we need to find ways to curtail that.

So, again, sincerely thank you for your testimony. You have given us a lot of good ideas, a lot of good information. We want to continue to work with each of you and your associations to come to some solutions and we can take those solutions then, as I said, to the law enforcement sector and see how we can find ways to actually make this system better, streamline it for your benefit, while also, at the same time, helping them be able to do their job, which is to protect our country and our citizens.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

And with that, the hearing is adjourned.

[Whereupon, at 4:25 p.m., the hearing was adjourned.]

A P P E N D I X

June 28, 2017

WASHINGTON, D.C.
601 Pennsylvania Avenue NW
South Building, Suite 600
Washington, D.C. 20004-2601
Phone: 202-638-5777
Fax: 202-638-7734

TESTIMONY

OF

FAITH LLEVA ANDERSON
SENIOR VICE PRESIDENT & GENERAL COUNSEL
AMERICAN AIRLINES FEDERAL CREDIT UNION

BEFORE THE

FINANCIAL SERVICES SUBCOMMITTEE ON
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED,
"EXAMINING THE BSA/AML REGULATORY COMPLIANCE REGIME"

JUNE 28, 2017

Testimony
of
Faith Lleva Anderson
Senior Vice President & General Counsel
American Airlines Federal Credit Union
Before The
Financial Services Subcommittee on
Financial Institutions and Consumer Credit
United States House of Representatives
At a Hearing Entitled,
"Examining the BSA/AML Regulatory Compliance Regime"
June 28, 2017

Chairman Luetkemeyer, Ranking Member Clay, Members of the Subcommittee:

Thank you for the opportunity to testify on this important topic. My name is Faith Lleva Anderson, and I am the Senior Vice President and General Counsel for American Airlines Federal Credit Union, headquartered in Fort Worth, Texas. I am also the Vice-Chair of the Consumer Protection Subcommittee of the Credit Union National Association (CUNA),[1] on whose behalf I am testifying today.

American Airlines Federal Credit Union proudly serves over 274,000 members - offering a variety of consumer, mortgage, vehicle, small dollar, credit card, and business loans, as well as a variety of savings and deposit accounts. We began as a single sponsor credit union for American Airlines (AA) over 80 years ago, when only AA employees and their families could become members. Following 9/11, we became an Air Transportation Industry charter. Therefore, while still serving the employees of AA and their families, our members now include those consumers who work directly in the administration, regulation, or security of airlines, airports, or air transportation; work at other airlines or airports; and those whose work is related to the airline/airport industry, such as Transportation Security Administration and Federal Aviation Administration employees.

[1] Credit Union National Association represents America's credit unions and their 110 million members.

By asset size ($6.5 billion), loans outstanding ($3.9 billion), and member deposits ($5.8 billion), we may be considered relatively "large" for a credit union but are still quite small compared to national or regional banks. Like all credit unions, we are a not-for-profit institution owned by the very members we serve and established for the sole purpose to promote thrift and provide access to credit to members for provident purposes. This member-owner structure is what makes credit unions unique financial institutions in our economic environment. My credit union, as all others, pledges itself to the preservation, protection, and prosperity of the system of cooperative credit.

American Airlines Federal Credit Union is dedicated, first and foremost, to providing excellent products and services to our member-owners. Their financial health and well-being is the most critical element to keeping our credit union operations successful. As such, my credit union takes compliance and financial security seriously, and applies whatever resources necessary to ensure our operations are solid and our members are protected. The good news is that credit unions are, and have always been, strong and stable financial services providers in our communities.

I wish there were no challenges to credit union operations in today's regulatory regime, but that is not the current reality. While credit unions support laws and regulations that prevent terrorists and criminals from using their institutions to launder money or otherwise engage in illegal activity, the compliance burden of the current regulatory environment often unnecessarily takes away from our ability to serve our members. Since the 2008 economic crisis and the resulting regulations that followed, credit unions have been required to devote more resources for regulatory and legal compliance particularly for mortgage loans and other consumer products, services, and protections. Given these new requirements, it has become difficult for credit unions to absorb their current total compliance burden. The new regulatory regime makes Bank

Secrecy Act (BSA)[2] and Anti-Money Laundering (AML) regulatory compliance even more daunting.[3]

We support efforts to track money laundering and terrorist financing, but also believe it is important to strike the right balance between the costs to financial institutions, like credit unions, and the benefits to the federal government from the BSA, AML, and Office of Foreign Assets Control (OFAC) regulations. As such, we support legislative and regulatory changes to address the redundancies, unnecessary burdens, and opportunities for efficiencies within the BSA/AML statutory framework. In particular, we support changes to (1) minimize the duplication of the same or similar information; (2) provide additional flexibility based on the reporting institution type or level of transactions; (3) curtail the continually enhanced customer due diligence requirements; (4) increase the currency transaction reporting (CTR) threshold; (5) reduce and simplify the reporting requirements of Suspicious Activity Reports (SARs) that have limited usefulness to law enforcement; and (6) allow for greater regulatory and examination consistency among regulators, including the National Credit Union Administration (NCUA) and state credit union regulators, in order to help with interpretations of BSA requirements and guidance and to minimize regulatory overlap.

My testimony provides details on specific issues that credit unions have been facing regarding BSA/AML compliance. It also outlines how commonsense changes would help responsible financial institutions, like credit unions, continue to serve their members and communities while protecting them from crime. There are opportunities to reduce financial institution burden while at the same time ensuring that our country and our citizens are protected from financial wrongdoing. Credit unions are deeply committed to the fight against crime, but it is important to recognize we are not law enforcement

---

[2] The Currency and Foreign Transactions Reporting Act of 1970 (commonly referred to as the "Bank Secrecy Act" or "BSA") requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. The act specifically requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. The BSA is often referred to as an "anti-money laundering" law ("AML") or jointly as "BSA/AML."

[3] The Department of Treasury's Financial Crimes Enforcement Network (FinCEN) implements the regulations for recordkeeping and reporting requirements of the Bank Secrecy Act codified at 31 C.F.C. § 103.

agents and we have certain fundamental limitations. I hope my testimony will help this Subcommittee find the proper middle ground between protection and undue burden.

Providing Credit Unions with the Compliance Tools for Success

My primary goal as Senior Vice President and General Counsel of American Airlines Federal Credit Union is to provide legal and compliance guidance to my credit union so it can operate successfully and provide products and services for its members. This job has become exponentially more difficult in recent years. While credit unions acclimate and adapt to the complex array of payment options today, they are also operating under sophisticated compliance regimes for new technologies. As noted, the burden credit unions face on BSA/AML compliance is further compounded due to complex new regulations that have been promulgated in response to actions of bad actors during the financial crisis, despite the fact credit unions did not cause or contribute to the crisis.

It is important to note that since the economic crisis of 2008, credit unions have been subject to more than 200 regulatory changes from over a dozen federal agencies. These new rules total nearly 8,000 *Federal Register* pages, and counting. The constant stream of new regulations has led to credit union resources being diverted from serving members to making the tough choices to limit or eliminate certain products and services. Furthermore, the disparity in the cost impact of regulation has accelerated the consolidation of the credit union system. While the number of credit unions has been declining since 1970, the attrition rate has accelerated since 2010, after the recession and the creation of the regulations that did not exempt credit unions. In fact, 2014 and 2015 were among the top five years in terms of attrition rates since 1970, at 4.2% and 4.1% respectively. Attrition rates at smaller credit unions have been especially high. In both 2014 and 2015, the attrition rate at credit unions with less than $25 million in assets (half of all credit unions are of this size) exceeded 6%. There is an indisputable connection between both the dramatically higher regulatory costs and their higher attrition rates. It is for this reason that credit unions speak regularly about the cost of regulatory burden and are looking for solutions to streamline and tailor important requirements, including BSA/AML requirements.

BSA regulations, administered by FinCEN, are the foundation of all efforts by our government to stop criminal money laundering and terrorist financing. These have been strengthened through AML laws, which include part of the USA PATRIOT Act. These laws require financial institutions such as banks, credit unions, and non-depository financial institutions to keep records of events that could signal money laundering and terrorist financing. BSA/AML regulations require financial institutions to maintain records on cash sales of negotiable instruments of $3,000 - $10,000 and records of wire transfers of $3,000 or more, and to report cash transactions over $10,000 and any suspicious activity that might show money laundering, tax evasion, or another type of crime. The forms used by credit unions to report transactions are the Currency Transaction Report (CTR)[4] and the Suspicious Activity Report (SAR).[5] In addition, BSA requires the verification of member identity and response to the 314a information request lists provided by FinCEN. When financial institutions fail to comply with these laws and regulations, they can receive significant civil money penalties and risk damage to their reputation.

My credit union has a team of experts to ensure we comply fully with these laws and regulations. We conduct detailed record keeping and spend thousands of hours and dollars on due diligence. In fact, due to increasing BSA requirements, we have split our BSA department into two separate sections – one section to work on the investigative side and one section to work on the risk side. This adjustment was made so my credit union could efficiently keep up with the many filing and record keeping requirements. Of all the requirements on BSA/AML, the most burdensome and time consuming are working on open SAR investigative cases, monitoring the members' account and transaction activity for unusual or suspicious activity, conducting the exhaustive research

[4] Financial institutions must file a Currency Transaction Report on any transaction in currency of more than $10,000.

[5] *See* "Anti-Money Laundering Compliance Frequently Asked Questions and Answers (FAQs)," *available at* https://www.ncua.gov/Resources/Documents/LCU2005-09Encl1.pdf ("In general, federally-insured credit unions must file a SAR when there is a known or suspected violation of a federal law, a pattern of criminal violations, or a suspicious activity committed or attempted against the credit union or involving a transaction or transactions through the credit union meeting the following criteria: insider abuse involving any amount; violations aggregating $5,000 or more where a suspect can be identified; violations aggregating $25,000 or more regardless of a potential suspect; and transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.").

on an average of 600 potential suspicious activity scenarios per month, and filing the SARs and CTRs. Overall, it takes my credit union three to five days to process an average SAR for one case from beginning to end, and we have 30 - 45 SAR filings per month.

In addition, quality control is costly and time-consuming. Preparing for our federal regulatory agency examination on BSA/AML compliance requires the work of three full-time professional staff members and takes about two full months. This time is dedicated to ensuring reports are filed accurately, the risk assessments are completed, and there have been no mistakes made to the process and filings. Furthermore, my credit union is required to conduct BSA/AML training every year for all our 600 employees, and this training must be customized to the individual roles of the employees. Many credit unions will perform quarterly or monthly training. Federal regulatory agencies also require institutions to conduct regular training on OFAC.[6]

American Airlines Federal Credit Union was previously able to conduct online training for our employees spread over 13 states and the District of Columbia, but now we must supplement the online training with additional one-on-one training. We also train our Board of Directors annually on BSA/AML compliance, because we are being examined on our credit union's "culture of compliance" and examiners expect director accountability and a strong top-down approach to understanding and overseeing compliance programs.

Indeed, my credit union dedicates a great amount of time, staff resources, and money to BSA/AML requirements and we are not a large national bank. The reality is the cost of technology for monitoring and ensuring compliance with BSA/AML laws and regulations is disproportionately burdensome on smaller and less complex institutions, such as credit unions. Often, credit unions choose not to serve certain markets because of the complexities of compliance. Money Service Businesses are a prime example of where many credit unions have difficulty providing needed services because of the BSA and AML ongoing due diligence requirements associated with serving these businesses.

---

[6] *See id.*

Nevertheless, our government can ease the compliance burden for smaller or less complex financial institutions, such as credit unions, while maintaining the protections needed. The following technical changes would make a major difference in the compliance burden facing credit unions on these requirements.

SAR and CTR Forms Should Be Combined

It would be helpful to the industry if the SAR and CTR forms – the two forms used for reporting – were combined into one form and submitted to the same place. This form should be streamlined and consolidated so the same information can be populated for either form, or the form can simultaneously be used for either SAR or CTR (for example, with a check box on the form to specify for which report, CTR or SAR, the information is being provided). This relatively minor change in paperwork would greatly ease compliance burden and ensure mistakes are not made during reporting, without compromising efforts to prevent criminal activity.

Reporting Thresholds and Deadline to File Should Be Increased to Reflect Today's Environment

The threshold for a CTR has not been adjusted in many years for inflation. Credit unions support an adjustment to this $10,000 threshold to account for inflation and economic change over the past several years. This current amount was established in 1972, and would be over $58,400 if adjusted for inflation in today's world.[7] Furthermore, the current relatively low limit is now capturing routine cash transactions that are not necessary to report since such transactions will be reported via the SAR if there is suspicious activity. Credit unions support increasing the CTR threshold to a minimum $20,000 amount and at least doubling other key thresholds, such as the $5,000 threshold for filing a SAR.

Additionally, the deadline to file a SAR should be extended from 30 days to 40 days for the more complex cases. The more complex the case, the longer it takes to

[7] *See* Bureau of Labor Statistics Consumer Price Index Inflation Calculator, *available at* https://data.bls.gov/cgi-bin/cpicalc.pl?cost1=100%2C00.00&year1=197907&year2=201705.

research the facts, which places substantial pressure on the credit union to timely file a SAR.

"Beneficial Owner" and Beneficiaries Requirements

FinCEN finalized its beneficial ownership rule, which would extend Customer Due Diligence (CDD) requirements under BSA rules to the natural persons behind a legal entity, and require financial institutions to have risk-based procedures for conducting ongoing customer due diligence. The final rule creates a new § 1010.230 in Title 31 C.F.R. to require covered financial institutions to identify and verify the identity of beneficial owners of legal entity customers when a new account is opened, and conduct risk profiles and monitoring of customers. The requirements for identifying the true beneficial owner of various entities, which is effective on May 11, 2018, places an enormous burden on credit unions.

In addition, checking payable-on-death (POD) account beneficiaries against the OFAC list should only be required to occur if payout to the beneficiary is necessary. Payable-on-death beneficiaries do not have access to or control of the account in question, and may never have access, so there is no need to continually check them until they receive this access and control. Information on the beneficiaries is often not available for accurate checks because usually only the name of a beneficiary is collected, making this work difficult and time consuming to conduct. The OFAC checks are a substantial compliance burden and would be easier for institutions to conduct when ownership of the funds occurs. Again, this change would in no way limit our efforts to prevent criminal activity.

Monetary Instrument Purchases

Under 31 C.F.R. § 1010.415, banks and credit unions are required to verify the identity of persons purchasing monetary instruments for currency in amounts between $3,000.00 and $10,000.00, and maintain documentation of such transactions. The requirement to maintain a separate documentation for these transactions is antiquated given today's systems that track every transaction that occurs in a financial institution. A

credit union can trace any transaction on its core system if it is needed by law enforcement. Therefore, the separate documentation requirement should be eliminated.

Working with Financial Institutions, Not Against Them

Credit unions work diligently to ensure they are complying with all applicable rules and regulations. While American Airlines Federal Credit Union has a larger staff, as recently noted by the NCUA, the median size of a credit union is less than $30 million in assets and the median staff size is eight employees. Accordingly, the NCUA noted that credit unions can "struggle to stay abreast of complex and evolving compliance requirements without the retention of often cost prohibitive counsel, accountants, financial advisors, and other professionals."[8]

At American Airlines Federal Credit Union, we, like other credit unions, take compliance seriously and dedicate significant resources to it. However, when credit unions are spending their limited resources disproportionately on compliance, this means they are spending fewer resources on innovating and providing safe and affordable products and services. We recognize that regulatory agencies –whether it be the NCUA, the Consumer Financial Protection Bureau (CFPB), or bank regulators – have a renewed focus on BSA/AML compliance, particularly on issues such as cybersecurity and mobile payments. However, we encourage a regulatory regime that will recognize the time and effort that goes into good faith compliance with laws, and does not unduly punish financial institutions for unintentional technical or minor errors. The seemingly never-ending stream of regulatory expectations for credit unions, often with small and stretched staffs, must be considered in agency examinations and when laws and requirements are enacted.

Furthermore, the ever-increasing technology and payment systems make it difficult for a smaller institution to keep up with what is necessary for BSA/AML purposes. For example, shared branch servicing, new bill-pay systems, and Bitcoin all hit

[8] National Credit Union Administration Letter to CFPB Concerning Compliance with CFPB Rules, *available at* https://www.cuna.org/uploadedFiles/CUNA/Legislative_And_Regulatory_Advocacy/Removing_Barriers_Blog/Removing_Barriers_Blog/Cordray%20CU%20Compliance%20with%20CFPB%20Rules%20Letter.pdf (May 24, 2017).

a credit union's core system differently, and it could be difficult to know what one is looking at to determine if an activity is suspicious or not. It is in these cases that regulatory agencies can be a resource to financial institutions and work with them to ensure that proper compliance takes place. Below are recommendations for a commonsense approach to working with credit unions on BSA/AML compliance.

Zero Tolerance for Unintentional Non-Compliance Should Be Reconsidered

The zero tolerance for non-compliance should be loosened so unintentional errors on SARs or CTRs, which can be complex and confusing to complete depending on the situation, do not result in an unfair penalty or violation in a supervisory examination. Intentional noncompliance or a pattern of negligence with the essential and substantive requirements should be subject to zero tolerance, but the occasional clerical error, such as failing to check a box on a complex form, should be afforded more leniency.

In the current regulatory environment, even a substantially minor error, such as recording a P.O. Box as an address instead of a street address, can lead to a Document of Resolution (DOR) for the institution for non-compliance. If there is more than one error, for one or more consumers, the DOR by the financial regulator could be for a "systemic" violation, which would garner increased attention and be considered a greater violation. In today's complex regulatory environment, federal and state examiners are particularly conservative and will report institutions for a systemic violation even if only two similar errors were made. This reality increases the compliance burden for credit unions to conduct more checks than likely necessary and spend more resources on quality control. Furthermore, because the safe harbor for compliance only applies when a SAR is filed, institutions like my credit union tend to err on the side of caution and file a SAR even though law enforcement officials tell us not to file unless necessary.

Finally, another reason why the burden is high for BSA/AML compliance is because now BSA officers can be held personally liable and be required to pay high civil money penalties out of their own pocket if they do not have a solid BSA/AML Program, as seen in some recent court cases. The penalties can be harsh and daunting, and can prevent individuals from becoming BSA officers or make these officers too expensive to hire.

Credit unions are on the front-line defense against financial crime, and we are on the side of the good guys. Please allow us to do our jobs as efficiently as possible without fear of a regulatory death sentence for a minor or unintentional oversight when completing complex paperwork.

Greater Transparency Helps Us Do Our Jobs Better

It would be helpful if financial institutions received detailed information about relevant law enforcement cases and results due to reporting. It would allow credit unions to more effectively implement BSA/AML compliance programs if they better understood how their reports are helpful to law enforcement and how they have prevented any criminal activity. Greater transparency and communication between the regulatory agencies, law enforcement, and the industry will ensure all stakeholders have consistent goals and improve the value of the information collected and reported. Furthermore, greater communication can educate regulatory agencies as to what requirements and guidance are helpful or not to law enforcement, so that any unnecessary or useless requirements can be amended.

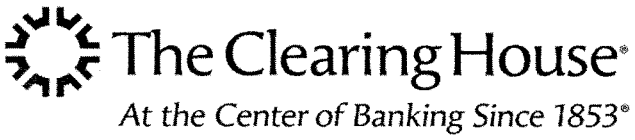
Ensuring All Stakeholders Have a Meeting of the Minds

It is critical that all federal regulators and agencies are consistent in the examination and supervision of these laws and requirements. Credit unions encourage FinCEN to work toward greater regulatory and examination consistency among regulators, including the NCUA and state credit union regulators, to help with interpretations of BSA requirements and guidance and to minimize regulatory overlap.

Conclusion

Thank you again for the opportunity to testify and be a part of this process. I take my role in the credit union movement, and as part of the financial services industry, seriously. I believe we have an obligation to protect our members and the financial community from fraud and crime, and there can always be more that should be done. However, credit unions are first and foremost in the financial services business, and do not have the infrastructure for law enforcement. This is the reality we struggle with every day.

The tough question that lawmakers must grapple with is how to balance the need for protection with the burden placed on financial institutions and consumers who ultimately pay the cost. The credit union industry is open to working with the government to protect against crime, and we look forward to being a resource as you develop processes and requirements that are streamlined and more manageable. On behalf of America's credit unions and their 110 million members, thank you for consideration of our views.



Testimony of Greg Baer
President
The Clearing House Association

"Examining the BSA/AML Regulatory Compliance Regime"

House Financial Services Subcommittee on
Financial Institutions and Consumer Credit

June 28, 2017

Chairman Luetkemeyer, Ranking Member Clay, and members of the Subcommittee, my name is Greg Baer and I am the President of the Clearing House Association and General Counsel of the Clearing House Payments Company. Established in 1853, we are the oldest banking payments company in the United States. Our Association is a nonpartisan advocacy organization dedicated to contributing quality research, analysis and data to the public policy debate. Over the past year, we have devoted substantial resources to the topic we are discussing today, including working with members of the Committee on beneficial ownership legislation.

Introduction

Our current anti-money laundering/counter-terrorist financing (AML/CFT) system is broken. It is extraordinarily inefficient and outdated, and driven by perverse incentives. Fundamental change is required to make that system an effective law enforcement and national security tool, and reduce the collateral damage it is doing to global development, financial inclusion, and other U.S. policy interests. As I'll describe further, we believe the Department of the Treasury must take the lead here, and fortunately it has already begun that process with a public request for input on how it can regulate better, both in this area and others.

For a better appreciation of how the current system malfunctions, I will begin with an analogy. Imagine an army where officers are not evaluated based on how they or their units behave in battle, or how well they lead their troops. Rather, the officers are considered for promotion based on audits of the accuracy and punctuality of their expense reports. The auditors also track unit casualties, with repeated casualties resulting in demerit, demotion or court martial for the responsible officers. The auditors do not have sufficient seniority or clearance to be briefed on the battles that have occurred, or read any after-action reports. Thus, their audits reflect only the losses suffered by the unit itself, not the casualties it inflicted upon the enemy.

What sort of an army would this system produce? Certainly, one hesitant to take risk. While a patriotic desire to defeat the enemy would remain strong, officers would know that outside-the-box thinking or risky advances could result in casualties and audit lapses, and eventually end their careers. Promotion would come for those who entrenched their positions, adhered to the rules, and excelled at paperwork. This army inevitably would end up being led by a George McClellan (whom Lincoln famously described as "having a terminal case of the slows"), not an Eisenhower or Patton. Morale among the troops would plunge.

The U.S. AML/CFT regulatory regime, circa 2017, is not dissimilar. It is a system in which banks have been deputized to act as quasi law-enforcement agencies and where the largest firms collectively spend billions of dollars each year, amounting to an annual budget somewhere between that of the ATF and the FBI.[1] However, in talking to senior executives at banks large and small, I have never heard a single one of them complain about how much money they *spend*. Rather, they complain about how much money they *waste*. And that waste derives from a series of perverse incentives that are embedded in our current system.

---

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

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

Unfortunately, our AML/CFT regulatory system is focused elsewhere. Large banks have been pushed away from risk-based approaches, because their performance is not examined and graded by law enforcement or national security officials, but rather by bank examiners, who are not permitted to know of their successes.[2] Instead, those examiners focus on what they know and control: policies, procedures, and quantifiable metrics – for example, the number of computer alerts generated, the number of suspicious activity reports (SARs) filed, the number of compliance employees hired.

Specific Problems with the Status Quo

A key obligation of banks under the current AML regime – and the key area of focus by bank examiners – is the filing of SARs. The comprehensive SAR reporting regime originated in 1992 as a way for banks to centrally provide leads to law enforcement. The process typically begins with an alert generated by a bank's monitoring system, with a SAR filed in the event the activity looks to be suspicious. For example, negative media reports on an existing bank customer trigger an alert, prompt an investigation by a bank compliance department, and can result in a SAR filing.

In the current regulatory and enforcement climate, bank compliance officers have powerful incentives to trigger as many alerts and file as many SARs as possible, because those "defensive" SAR filings protect them (and their examiners) in the event that the bank is used by the companies or individuals ultimately found to have committed a crime. What gets measured gets done, and providing valuable intelligence to law enforcement or national security agencies does *not* get measured; writing policies and procedures and filing SARs does get measured. So, almost two million SARs are filed per year.[3]

Worse yet, SAR filing rules and metrics fail to consider the relative severity of the offense. SAR dollar thresholds have not been raised in 21 years, and there is no dollar threshold for so-called insider abuse (say, a teller stealing a small amount of money).[4] No federal law

---

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

[3] *See* "SAR Stats," *available at*: https://www.fincen.gov/fcn/Reports/SARStats. The total number of SARs filed in 2016 was 1,975,644. Accessed June 27, 2017.

[4] *See* 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System) (Federal Reserve); 12 CFR 353 (Federal Deposit Insurance Corporation)(FDIC); 12 CFR 748 (National Credit Union Administration)(NCUA); 12 CFR 21.11 and 12 CFR 163.180 (Office of the Comptroller of the Currency)(OCC); and 31 CFR 1020.320 (FinCEN) for federal SAR regulations. The SAR requirement became effective April 1, 1996 and dollar thresholds have not been raised since.

enforcement agency would ever prosecute the large and growing majority of offenses that are reported in SAR filings, but the filings continue apace.

(One sometimes hears the argument that even a minor offense could be the "last piece in the puzzle" for a law enforcement agency trying to make a larger case, and there are undoubtedly cases where that is true. In the same way, someone arrested for jaywalking could turn out to be a wanted fugitive. The important question, though, is what the opportunity cost for that puzzle piece is – whether resources allocated elsewhere couldn't produce large and fully formed puzzles of their own.)

To be clear, this is not a criticism of the examiners, but rather of the role the current system forces them to play. From a political and personal risk perspective, they are in a no-win situation. On the one hand, they are excluded when the bank they examine is pursuing real cases with law enforcement, national security or intelligence community officials, and therefore receive no credit when those cases are successful. But if something goes wrong – if a corrupt official or organization turns out to be a client of the bank they examine – the examiner faces blame. Thus, from an examiner and banking agency perspective, the only possible safe harbor is to demand more policies and procedures, ensure that a lot of SARs are filed, encourage the bank to jettison any client that presents significant risk, and take swift and long-lasting enforcement action whenever something goes wrong. While all other aspects of banking – for example, credit risk management – have risk tolerances, for AML/CFT, there is none. And because reward and risk tend to go together, the system suffers.

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

The Great Opportunity Being Lost

This lack of focus on the goals of the system is especially disheartening in an age in which emerging technology has the potential to make the AML/CFT regime dramatically more effective and efficient. Artificial intelligence (AI) and machine learning could revolutionize this area, and banks continue to discuss various concepts for greater sharing of information. Unfortunately, SAR filers receive almost no meaningful feedback on whether a given SAR has proven useful to law enforcement. In the 1970s, when relatively few reports were filed, each SAR was read by someone in law enforcement. Now, with banks and other financial institutions employing tens of thousands of people and using computer monitoring to

flag potentially suspicious activity, almost two million SARs are filed per year.[5] Law enforcement generally reads SARs only if they are specifically flagged by the institution, or if a word search identifies it as relevant to an existing investigation.

Thus, the role of a SAR in law enforcement has changed completely, which is not necessarily a bad development. Because so much more data is available, there is extraordinary potential for the use of AI and machine learning to improve the system. But those strategies require feedback loops, which do not exist in the current system. Worse yet, several AML executives have reported that efforts to construct novel approaches to detecting illegal behavior have resulted in examiner criticism because such innovative approaches were deemed to lack sufficient documentation, and therefore were not auditable by bank examiners. Banks will be reluctant to invest in systems unless someone in the government can tell them that such systems will meet the banking examiners' expectations. Thus, we have a database created for one purpose and being used for another. Innovation awaits regulatory reorganization and leadership.

The Example of De-Risking

Nowhere is this set of perverse incentives more clear than in the push for banks to eliminate clients in countries or industries that could end up creating political risk to examining agencies.

The causes of de-risking are not difficult to discern. For example, in June 2014, the Office of the Comptroller of the Currency (OCC) published an enforcement action against Merchants Bank of California that contained broad statements indicating that the bank needed to treat all of its money services business (MSB) clients as high risk and take extraordinary measures when dealing with them.[6] When the bank, which was servicing Somali remitters, later left the MSB business entirely, the Somali community in the U.S. was left without a reliable channel controlled by ethnic Somalis for sending remittances home. Of course, the OCC has subsequently denied imposing any pressure on banks to de-risk, and issued a statement asserting that it does not characterize all money services businesses as "uniformly" high risk.[7] For banks, though, (enforcement) actions speak far louder than words.[8] And of course public statements by regulators are not necessarily consistent with examiner queries to bank compliance officers to provide assurances that high risk businesses or countries have received heightened due diligence and will never present a problem – with strong suggestions that any future problems inconsistent with such assurances could result in personal ruin for those providing them.

Thus, faced with unlimited potential liability (both institutional and personal) if something goes wrong in a jurisdiction or line of business identified by regulators as high risk,

---

[5] SAR Stats, *supra* note 3.

[6] *See* OCC Consent Order 2014-084; *available at*: https://www.occ.gov/static/enforcement-actions/ea2014-084.pdf.

[7] *See* OCC "Statement on Risk Management," released November 19, 2014, *available at*: https://www.occ.gov/news-issuances/bulletins/2014/bulletin-2014-58.html.

[8] For a broader discussion of this trend, see article by Clay Lowery and Vijaya Ramachandran, "Unintended Consequences of AML Policies," in TCH Q3 2016 *Banking Perspectives* issue; *available at*: https://www.theclearinghouse.org/research/banking-perspectives/2016/2016-q3-banking-perspectives/aml-unintended-consequences.

the rational response for a financial institution is to "de-risk" – that is, fire its customers in that business or country.

Of course, there are major costs of de-risking: business loss suffered by the bank from de-risking, certainly, but more broadly and importantly a blinding of the intelligence community to overseas jurisdictions as illicit finance moves to shadow markets or foreign banks; a loss of political influence for the nation's diplomats; a loss of allies for national defense; and human suffering in countries cut off from correspondent banking, remittances, and other access points to the global financial system. An IMF report recently noted, "[p]ressure on correspondent banking relationships could disrupt financial services and cross-border flows, including trade finance and remittances, potentially undermining financial stability, inclusion, growth and development goals."[9] A survey carried out by the World Bank in 2015 found that 75% of large global banks are withdrawing from correspondent banking relationships, with U.S. banks being the most active.[10]

Similarly, domestically, banks of all sizes report that customer due diligence requirements have dramatically increased the cost of opening new accounts, and now represent a majority of those costs. Of course, this makes low-dollar accounts for low- to moderate-income people much more difficult to offer and price. While the connection is not immediately apparent, AML/CFT expense now is clearly an obstacle to banking the unbanked, and a reason that check cashers and other forms of high-cost, unregulated finance continue to prosper.

The problem, of course, is that bank examiners and federal prosecutors seeking record fines do not internalize those costs. And those in the government who do internalize those costs play no role in examining the performance of financial institutions.

The Beginning of a Solution

Fortunately, a remarkable number of stakeholders, including foreign policy, development and technology experts, have been focusing on all these issues. Their goal is not to save banks money or embarrassment. Their goal is to do what is best for our country. We convened a group of these experts at two symposia in 2016, and the result is the report attached to my testimony, along with a list of some of the key participants.

You will see numerous recommendations in that report. The most important one, though, is for the Department of the Treasury to accept – or, better yet, claim – responsibility for the system. That includes convening on a regular basis the end users of SAR data – law enforcement, national security and others affected by the AML/CFT regime including the State Department – and setting goals and priorities for the system. We also believe it means the Treasury Department, through FinCEN, should assume supervisory authority for certain banks.

---

[9] *See* IMF Staff Discussion Note by Michaela Erbenová, Yan Liu, Nadim Kyriakos-Saad, et al, "The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action, " IMF 2016; *available at:* http://www.imf.org/~/media/websites/imf/imported-full-text-pdf/external/pubs/ft/sdn/2016/_sdn1606.ashx.

[10] *See* "Withdraw from Correspondent Banking: Where, Why, and What to do About It," World Bank Group 2015; *available at:* http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2015/11/24/090224b083395501/3_0/Rendered/PDF/Withdraw0from000what0to0do0about0it.pdf.

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

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

Remarkably, this arrangement is exactly what Congress intended and authorized. In the Bank Secrecy Act, Congress granted FinCEN, *not* the banking agencies, authority to examine for compliance. However, over 20 years ago, FinCEN delegated its supervisory authority to the federal banking agencies, while retaining enforcement authority. At the time the delegation was made, FinCEN's decision was logical, even inevitable. The agency had few resources, and insufficient knowledge of the banking system. Furthermore, the nation had over 10,000 banks, and those banks were more alike than different.[11] Restrictions on interstate banking meant that there were no truly national banks, and U.S. banks generally were not internationally active. As a result, there was no real basis by which FinCEN could have distinguished among banks. Given the choice between supervising 10,000 banks or none, it logically chose none, effectively sub-contracting its statutory duties in this area to the banking agencies.[12]

Whether for those few financial institutions, or the thousands that would continue to be examined by financial regulators, we believe the result of FinCEN assuming some supervisory authority would be a massive *cultural* change, as the focus shifted to the real-world effectiveness of each institution's AML/CFT program, rather than the number of SARs filed or number of

---

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

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

policies written. That change would start with those banks under direct FinCEN supervision, but would eventually spread to all institutions.

Empowered and informed leaders also could weigh these important factors and tackle some very difficult questions that are not currently addressed in a balkanized system. While a general goal of the BSA/AML system is to deny access to the financial system to potentially bad actors, are there cases where it benefits national security to have them in the system, where they can be monitored by regulated banks with sophisticated techniques, potentially leading to more useful information for law enforcement? Or is it better to push illicit actors out to overseas banks or non-banks, where law enforcement has little line of sight and a much harder time tracking illicit funds? Is any law enforcement or counter-terrorism gain worth exacerbating poverty in countries that harbor terrorists by using the blunt force of pressuring U.S. banks to "de-risk" those countries by ending correspondent relationships? Are the vast quasi-law enforcement resources of the banks better deployed marching in lock step, under rigid policies and procedures set by regulators, or by developing innovative techniques for detecting money laundering? Should banks be filing more SARs under a low standard for what constitutes suspicious activity, or instead be filing fewer SARs under a higher standard focused on plausible evidence of serious wrongdoing? A strong AML/CFT regulatory system would thoughtfully consider these questions after receiving input from all the relevant stakeholders, and clearly communicate answers to the financial institutions that implement it.

Finally, as I noted at the outset, one important change to the current system that requires new legislation is ending the use of shell companies with anonymous ownership. Here, the United States trails the rest of the world, and has been criticized by the Financial Action Task Force for being a shelter for criminals or cryptocrats seeking to launder money by adopting the corporate form and cloaking their ownership.[13] There may be valid reasons why corporate owners would want to keep their ownership secret from the broader public; however, it is difficult to imagine a valid reason why corporate owners would want to keep their ownership secret from the state incorporating them, law enforcement, and a financial institution that is legally obligated to determine that ownership in the exercise of its BSA/AML obligations. The Clearing House strongly urges Congress to adopt such legislation promptly, and is pleased to see bicameral, bipartisan support for it.

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

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

Attachments

The Clearing House®
At the Center of Banking Since 1853®

For Immediate Release:
Date: February 16, 2017
Contact: Sean Oblack, 202.649.4629
sean.oblack@theclearinghouse.org

The Clearing House Publishes New Anti-Money Laundering Report

Leading experts and practitioners recommend reforms to improve AML/CFT effectiveness

Washington, D.C. – Today, the Clearing House released a report entitled *A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement*. The paper analyzes the current effectiveness of the AML/CFT regime, identifies fundamental problems with that regime, and proposes a series of reforms to remedy them.

The report reflects conclusions reached in two closed-door symposia, in April and October 2016, that convened approximately 60 leading experts in this field. The group included senior former and current officials from law enforcement, national security, bank regulation and domestic policy; leaders of prominent think tanks in the areas of economic policy, development, and national security; consultants and lawyers practicing in the field; FinTech CEOs; and the heads of AML/CFT at multiple major financial institutions. The first meeting focused on problems with the current regime; the second focused on a review of potential solutions. The conclusions on both are set forth in the report.

Said Greg Baer, President of the Clearing House Association, "Today's report reflects a remarkable consensus on how to substantially increase the effectiveness of the AML/CFT regime. Those participating in the effort come from a wide range of disciplines and reflect a variety of interests, but have reached a common diagnosis of the problems with the current regime and in their prescription for reform."

Among those participating in the symposia and supporting the report are the following individuals, acting in their personal, non-institutional, capacity:

- *H. Rodgin Cohen*, senior chairman of Sullivan & Cromwell;
- *David D. DiBari*, managing partner of Clifford Chance, Washington office;
- *James H. Freis, Jr*, former Director of FinCEN; chief compliance officer, Deutsche Börse Group;
- *Aaron Klein*, policy director, Center on Regulation and Markets, Brookings Institution;
- *Sharon Cohen Levin*, former Chief, Money Laundering and Asset Forfeiture Unit, U.S. Attorney's Office, Southern District of New York; partner, WilmerHale;
- *Joseph Myers*, former Director, International Financial Affairs in the Office of Combating Terrorism, National Security Council; vice president, Western Union;

- *Chip Poncy*, former senior Treasury official; President, Financial Integrity Network; Senior Adviser, Center on Sanctions and Illicit Finance;
- *Vijaya Ramachandran*, senior fellow, Center for Global Development;
- *Elizabeth Rosenberg*, senior fellow, Center for a New American Security;
- *Gary Shiffman*, CEO, Giant Oak; and
- *Juan C. Zarate*, former senior Treasury official; former Deputy National Security Adviser; Chairman, Financial Integrity Network; Chairman, Center on Sanctions and Illicit Finance.

In addition, the Center on Sanctions and Illicit Finance (CSIF) at the Foundation for Defense of Democracies has also endorsed the report.

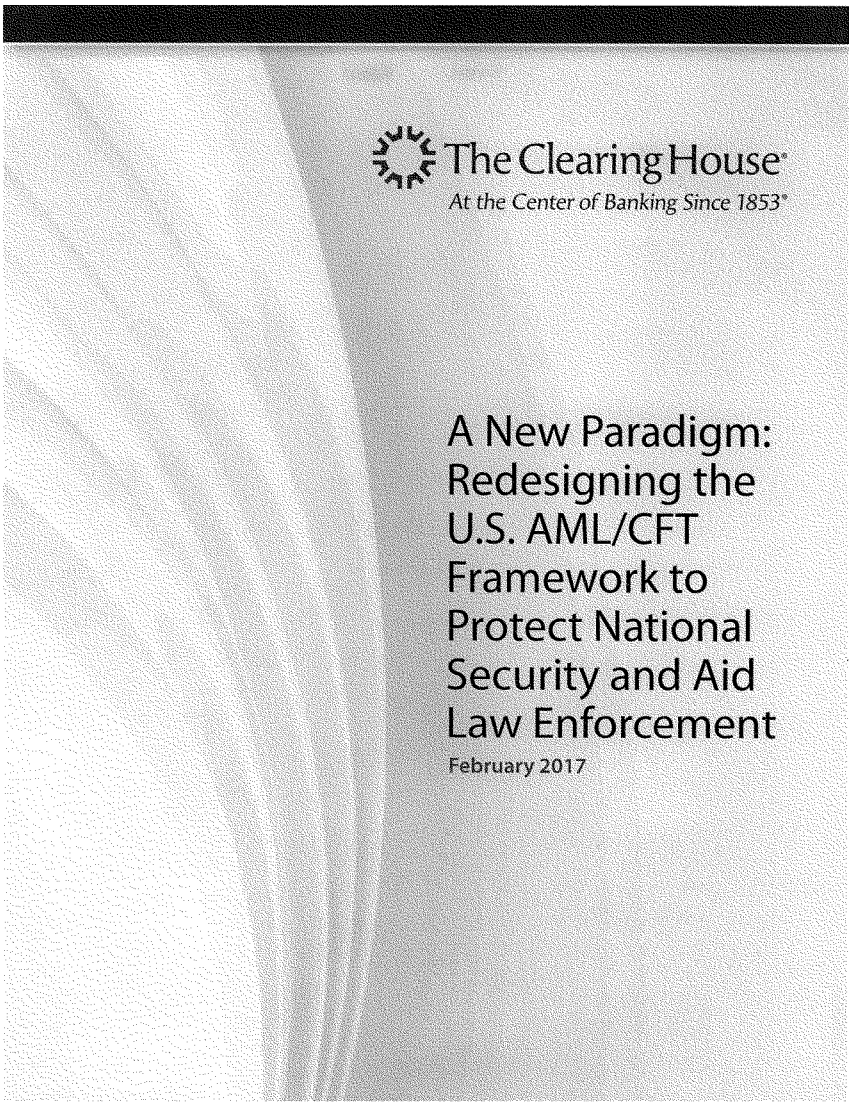
The report identifies eight reforms for immediate action:

- The Department of Treasury, through its Office of Terrorism and Financial Intelligence (TFI), should take a more prominent role in coordinating AML/CFT policy across the government;
- FinCEN should reclaim sole supervisory responsibility for large, multinational financial institutions that present complex supervisory issues;
- Treasury/TFI/FinCEN should establish a robust and inclusive annual process to establish AML/CFT priorities;
- Congress should enact legislation, already pending in various forms, that requires the reporting of beneficial owner information at the time of incorporation, preventing the establishment of anonymous companies;
- Treasury TFI should strongly encourage innovation, and FinCEN should propose a safe harbor rule allowing financial institutions to innovate in an FIU "sandbox" without fear of examiner sanction;
- Policymakers should incentivize banks to work on investigations and reporting of activity of high law enforcement or national security consequence;
- Policymakers should further facilitate the flow of raw data from financial institutions to law enforcement to assist with the modernization of the current AML/CFT technological paradigm;
- Regulatory or statutory changes should be made to the safe harbor provision in the USA PATRIOT Act (Section 314(b)) to further encourage information sharing among financial institutions, and the potential use of utilities to allow for more robust analysis of data; and
- Policymakers should enhance the legal certainty regarding the use and disclosure of SARs.

-30-

About The Clearing House. The Clearing House is a banking association and payments company that is owned by 25 of the largest commercial banks and dates back to 1853. The Clearing House Payments Company L.L.C. owns and operates core payments system

infrastructure in the United States and is currently working to modernize that infrastructure by building a new, ubiquitous, real-time payment system. The Payments Company is the only private-sector ACH and wire operator in the United States, clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume. Its affiliate, The Clearing House Association L.L.C., is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system.


The Clearing House
At the Center of Banking Since 1853
A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement
February 2017

A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement

February 2017

Table Of Contents

Introduction

In April and October 2016, a group of approximately 60 experts came together to discuss how to improve the U.S. framework for anti-money laundering/countering the financing of terrorism (AML/CFT) as it applies to financial institutions. The group included senior former and current law enforcement, national security, bank regulatory and domestic policy officials; leaders of prominent think tanks in the areas of economic policy, development, and national security; consultants and lawyers practicing in the field; FinTech CEOs; and the heads of AML/CFT at multiple major financial institutions. The first meeting focused on problems with the current regime; the second focused on a review of potential solutions. The consensus on both is set forth in this paper. It was prepared with the assistance of The Clearing House's special counsel, Wilmer Cutler Pickering Hale and Dorr LLP.

The stakes here are high. The United States leads the world in shaping and enforcing international standards of financial integrity and accountability and has demonstrated the importance of the AML/CFT regime to combating and preventing financial crime and protecting international security. Nevertheless, substantial challenges to the systemic effectiveness and sustainability of the current regime have emerged and require urgent attention.

Under the current AML/CFT regime, the nation's financial firms are effectively deputized to prevent, identify, investigate, and report criminal activity, including terrorist financing, money laundering and tax evasion. The largest firms collectively spend billions of dollars each year, amounting to a budget somewhere between the size of the ATF and the FBI.[1] Yet the conclusion of the vast majority of participants in the process is that many if not most of the resources devoted to AML/CFT by the financial sector have limited law enforcement or national security benefit, and in some cases cause collateral damage to other vital U.S. interests – everything from U.S. strategic influence in developing markets to financial inclusion. Thus, a redeployment of those resources has the potential to substantially increase the national security of the country and the efficacy of its law enforcement and intelligence communities, and enhance the ability of the country to assist and influence developing nations.

Executive Summary

The current AML/CFT statutory and regulatory framework is outdated and thus ill-suited for apprehending criminals and countering terrorism in the 21st century. In particular, the following are core problems with the current AML/CFT regime that must be resolved:

STRATEGIC PROBLEMS

» **ABSENCE OF PRIORITIZATION.** Law enforcement, national security and development officials have little to no input into how financial institutions allocate their AML/CFT resources. Rather, compliance is assessed primarily by bank examiners, essentially functioning as auditors, who are focused on preventing the institutions they supervise from suffering financial loss or reputational embarrassment, and ensuring that there is rigorous adherence to all written policies and procedures. Thus, for example, while financial intelligence units within the banks are of great benefit to law enforcement and national security officials, and focus on real risks, the examination process tends to result in banks prioritizing other, more readily auditable processes.

» **ABSENCE OF OVERARCHING PURPOSE.** For approximately the past 15 years, regulators described "preserving the integrity of the financial system" as the primary goal of the AML/CFT regime, but the notion has no statutory basis or clear definition. It implies an overarching goal of keeping money out of the financial system, but another goal should be and sometimes is the tracking of money once it is in the financial system and providing financial services to developing nations and underserved U.S. communities. Thus, the current examination and enforcement regimes have encouraged financial institutions to exclude (or "de-risk") accounts from a customer, industry or country that is perceived to have heightened risk of engaging in criminal activity; meanwhile, those concerned with international development and diplomacy, and financial inclusion, have little voice in the examination process.

» **OUTDATED SAR REGIME.** The original purpose of the suspicious activity report (SAR) regime was for financial institutions to provide leads to law enforcement agencies, but government agencies now could develop the technical resources and sophistication to mine financial data, significantly reducing the need for SARs as they are currently constructed. Yet the SAR remains the focus of the system.

OPERATIONAL PROBLEMS

» **COUNTERPRODUCTIVE EXAMINATION STANDARDS AND PROCESSES.** National security, law enforcement, and intelligence agencies—the end users of AML/CFT information—focus on the quality of information they receive from financial institutions, while those who grade the financial institutions focus on auditable processes. Thus, there are disincentives for financial institutions to develop innovative methods

for identifying criminal behavior. Firms receive little or no credit for proactive, aggressive cooperation with law enforcement – focusing on real risk – because examiners generally are unaware of such actions and in any event have no method for weighing such behavior against any policy or operational shortcomings within the confines of the examination framework.

» **SIGNIFICANT BARRIERS TO INFORMATION SHARING.** Existing rules prevent efficient and effective sharing of information among financial institutions and between financial institutions and law enforcement.

» **INEFFICIENCIES.** Financial institutions devote vast resources to activities that could easily be performed centrally by government or some other party or not at all – for example, constant monitoring of media for adverse stories about customers, or multiple firms engaging in customer due diligence on the same customers. With these tasks de-prioritized or executed collectively, resources could be deployed to more sophisticated and productive approaches designed to detect real risks.

Set forth below are clear and actionable responses to these problems, divided into two groups: areas for immediate reform and areas for further study.

Areas for Immediate Reform

- The Department of Treasury, through its Office of Terrorism and Financial Intelligence (TFI), should take a more prominent role in coordinating AML/CFT policy across the government;
- The Financial Crimes Enforcement Network (FinCEN) should reclaim sole supervisory responsibility for large, multinational financial institutions that present complex supervisory issues;
- Treasury/TFI/FinCEN should establish a robust and inclusive annual process to establish AML/CFT priorities;
- Congress should enact legislation, which was proposed in various forms during the 114th Congress and is expected to be re-introduced in the 115th Congress, that requires the reporting of beneficial owner information at the time of incorporation;
- Treasury TFI should strongly encourage innovation, and FinCEN should propose a safe harbor rule allowing financial institutions to innovate in a Financial Intelligence Unit (FIU) "sandbox" without fear of examiner sanction;
- Policymakers should de-prioritize the investigation and reporting of activity of low law enforcement or national security consequence;
- Policymakers should further facilitate the flow of raw data from financial institutions to law enforcement to assist with the modernization of the current AML/CFT technological paradigm;
- Regulatory or statutory changes should be made to the safe harbor provision in

the USA PATRIOT Act (Section 314(b)) to further encourage information sharing among financial institutions; and

- Policymakers should enhance the legal certainty regarding the use and disclosure of SARs.

Areas of Reform Requiring Further Study:

- Enhancing information sharing through the establishment of AML/sanctions utilities.
- Establishing better protections from discovery for SAR information;
- Clarifying and balancing responsibility for AML/CFT between the public and private sector;
- Establishing a no action letter-like system within the regime to assist with AML/CFT compliance;
- Providing financial institutions with clearer AML/CFT standards;
- Allowing for better coordination of AML/CFT and sanctions policy goals, supervision and enforcement; and
- Modernizing the SAR regime.

Assessment of the Existing Regime

BACKGROUND

The current AML/CFT regulatory framework is an amalgamation of statutes and regulations that generally derive from the Bank Secrecy Act, which was passed by Congress in 1970 with iterative changes since, and added to (but not reformed by) the USA PATRIOT Act, which was passed in 2001. This 45-plus year regime has not seen substantial changes since its inception and is generally built on individual, bilateral reporting mechanisms (i.e. currency transaction reports and suspicious activity reports), grounded in the analog technology of the 1980s, rather than the more interconnected and technologically advanced world of the 21st century.

In particular, the Bank Secrecy Act imposes requirements that can be in tension with each other and need to be considered in tandem as part of a risk-based system. Financial institutions are required to (i) report on suspicious activity and (ii) keep out customers that could generate suspicious activity. These conflicting requirements are further magnified by the wide-reaching and complex network of state and federal government actors who are responsible for implementing, enforcing and utilizing the information produced by the regime.[2] Generally, each entity has different missions and incentives, which has led to the development of competing and sometimes conflicting standards for institutions to follow.

Outlined below are what was determined by the group as fundamental problems with the current regime as well as recommendations for reform and items for further study.

FUNDAMENTAL PROBLEMS

Participants in the first symposium identified several fundamental problems with the current AML/CFT regime:

ABSENCE OF PRIORITIZATION. In law enforcement, it is routine for the Justice Department and other agencies to establish priority enforcement areas, set qualitative and dollar thresholds for the cases they are willing to bring, and generally manage the process of law enforcement. Aware of their limited budgets, these agencies choose which crimes to prosecute and which ones to let pass. However, financial institutions operating AML/CFT compliance programs receive little guidance on these matters, and are not able to exercise sufficient discretion within the current regulatory framework to themselves identify priorities. Thus, although the government may want financial institutions to prioritize cases involving, for example, terrorist financing, nuclear proliferation and human trafficking, in practice, there is little to no policy guidance to the financial sector on these priorities.[3] The reason is simple: the representatives of government that face financial institutions and have the ability to set the AML/CFT priorities for these institutions (most frequently, bank examiners) are not engaged with the law enforcement or intelligence communities, and thus lack the knowledge and authority to set such priorities on their behalf. Rather, they are focused on preventing the institutions they supervise from suffering financial loss or reputational embarrassment, establishing auditable policies and procedures, and ensuring rigorous adherence to those policies and procedures. This focus, plus a near-zero tolerance for error, necessarily focuses financial institutions on recordkeeping rather than developing imaginative and innovative approaches to identifying important threats to our country.

OUTDATED NATURE OF THE SAR REGIME. When it was first established in the 1990s, the goal of the SAR regime was for financial institutions to provide leads to law enforcement agencies; those agencies had little insight into the financial system, and no technical ability to mine data. Today, government agencies could develop resources to mine financial data, and rely less on financial institutions to provide robust, individual reports on suspicious activities or transactions. Also, as financial institutions have been incentivized by regulatory enforcement actions to file increasing numbers of suspicious activity reports (SARs), a declining percentage provide value to law enforcement.[4] Yet those regulators examining banks for AML compliance continue to emphasize the importance of financial institutions developing carefully crafted, highly-detailed SARs, with little to no feedback provided on such submissions, either from themselves or those government authorities who utilize the data.

COUNTERPRODUCTIVE EXAMINATION STANDARDS. Although financial institutions have been developing innovative methods for identifying criminal behavior, they face regulatory criticism for taking unconventional or innovative actions that seemingly deviate from policy and may not be readily auditable. The job of examiners is to check compliance against current standards, and they tend to disfavor imaginative deviation from those standards – particularly as they are cut off from information about the benefits of such deviations, given that law enforcement and national security officials

do not include them in investigations. As a result, financial institutions have begun to innovate less. Law enforcement and national security officials most value the work done by FIUs at financial institutions, which are laboratories dedicated to developing new and frequently outside-the-box methods of detecting illegal or dangerous conduct. Yet, several institutions reported shifting resources away from FIUs towards compliance staff, because of explicit or implicit examiner insistence that resources be devoted to demonstrating compliance with existing policies and procedures and ensuring the auditability of those mechanisms. Compliance officers, in turn, have received increasing pressure to ensure 100% compliance, and are increasingly at risk of personal liability or dismissal in the event of deviation from regulatory expectations; they thus have greater incentives to "work to the rule" rather than encourage innovation.

In sum, under the current regime, national security, law enforcement, and intelligence agencies—the end users of AML/CFT information—focus on outcomes, while those who grade the financial institutions for compliance focus on auditable processes.

BROADER CONFLICTING POLICY INTERESTS. The examination and enforcement regimes for the Bank Secrecy Act have incentivized financial institutions to exclude (or "de-risk") accounts from any customer, industry, or country that has relatively higher potential to engage in criminal activity: for example, to de-risk money service businesses or correspondent banks in developing or high-risk countries where public corruption, narcotics, or terrorist activity is prevalent. On the other hand, policymakers concerned with income inequality want banks to serve poor and underserved populations; development experts want multinational U.S. banks to serve developing countries; intelligence officials and law enforcement want multinational U.S. banks to stay engaged abroad in order to establish leads on nefarious activity; and national security and diplomatic officials want multinational U.S. banks to remain engaged abroad, rather than ceding those markets to other, less transparent, actors. Because a bank's AML/CFT regime is evaluated solely by bank examiners, these other policy interests generally are not considered. When they have been considered – for example, in recent OCC guidance – the response has been to require banks to develop policies and procedures for documenting their decision to de-risk rather than to encourage them to manage the risk more effectively.

BARRIERS TO INFORMATION SHARING. Significant barriers to information sharing are embedded in the system – for example, rules or interpretations limiting the ability of financial institutions to share within their own corporate structure, and with other financial institutions. These barriers block the flow of relevant information among financial institutions and between financial institutions and law enforcement. Some of these barriers serve legitimate privacy concerns that must be balanced against any potential benefits from greater sharing, but in many instances the barriers are simply the result of basic policy errors that have not been remedied over time.

INEFFICIENCIES. Financial institutions devote vast resources to activities that could easily be performed centrally by government or some other party. One example is the lack of an established reporting requirement for

beneficial owners of corporations, forcing financial institutions to research such information when it should be readily available upon incorporation. Another is filing SARs on activity that existing prosecution handbooks make clear will never be prosecuted – for example, low-dollar crimes committed against banks. A third is the tracking of politically exposed persons (PEPs), the definition of which is subject to multiple and changing standards across agencies and jurisdictions.

ALTERNATIVE APPROACH TO INFORMATION SHARING

The group also reviewed an alternative approach to information sharing that offered real promise: the UK's Joint Money Laundering and Intelligence Task Force (JMLIT).[5] JMLIT brings together financial institutions, law enforcement, and trade associations to discuss current AML/CFT risks and is underpinned by legislation that enables the UK National Crime Agency (NCA) to act as the gatekeeper for the information provided, and facilitate the exchange of information between the public and private sectors. Following completion of a one-year pilot program, an independent review determined that JMLIT had met its core objective to prevent, detect, and disrupt money laundering.

The JMLIT process has attributes that could help to resolve several problems identified with the current U.S. regime. The current SAR regime fails to provide feedback from law enforcement to the private sector about SAR efficacy, while JMLIT allows banks to follow-up on SAR activity. In addition, the JMLIT structure provides the dialogue about prioritization that U.S. financial institutions currently do not receive. Furthermore, JMLIT uses an operational priority structure which focuses on "(i) understanding and disrupting the funding flows linked to bribery and corruption; (ii) understanding and disrupting trade based money laundering; (iii) understanding and disrupting the funding flows linked to organized immigration crime and human trafficking; and (iv) understanding key terrorist financing methodologies." While U.S. policymakers might choose different priorities, and those priorities might change over time, they currently do not communicate any priorities with this degree of clarity.

POTENTIAL REFORMS

Set forth below are reforms that would: (i) make the AML/CFT regime more effective as a tool for law enforcement and national security; and (ii) reduce the collateral damage imposed by the current AML/CFT regime—generally, needlessly—on other important national priorities such as the projection of U.S. influence globally, the alleviation of poverty in less developed countries, and the availability of banking services in underserved communities in the United States. Possible reforms can be divided into two groups:

AREAS FOR IMMEDIATE REFORM: These reforms are clearly warranted and are of high priority. On these reforms, there was clear consensus of symposium participants on both the immediate need for the reforms and their wisdom.

AREAS OF REFORM REQUIRING FURTHER STUDY: These reforms warrant further consideration, because potential solutions may involve difficult tradeoffs or would benefit from the input of other stakeholders.

Areas for Immediate Reform

I. RATIONALIZE THE SUPERVISION OF MULTINATIONAL, COMPLEX FINANCIAL INSTITUTIONS

A. FinCEN should reclaim sole supervisory authority for large, multinational financial institutions that present complex supervisory issues.

BACKGROUND. FinCEN was granted authority to examine for compliance with the Bank Secrecy Act. However, over 20 years ago, it delegated its supervisory authority to the federal banking agencies, while retaining enforcement authority. In addition, in 1986, Congress granted the federal banking agencies authority to prescribe regulations requiring banks to comply with the Bank Secrecy Act, and examine for such compliance.[6]

At the time the delegation was made, FinCEN's decision was logical, even inevitable. The agency had few resources, and insufficient knowledge of the banking system. Furthermore, the nation had over 10,000 banks,[7] and those banks were more alike than different. Restrictions on interstate banking meant that there were no truly national banks, and U.S. banks generally were not internationally active. As a result, there was no real basis by which FinCEN could distinguish among banks. Given the choice between supervising 10,000 banks or none, it logically chose none.

RECOMMENDATION.

(1) FinCEN should revoke its delegation of examination authority for large, internationally active financial institutions[8] and any others it designates as presenting important and significant issues with respect to national security, law enforcement, and global development priorities. This would include not only banks but also large money service businesses and other significant non-bank financial institutions. As discussed below, FinCEN should assemble sufficient staff to conduct rigorous Bank Secrecy Act examinations of such institutions.[9]

(2) FinCEN, in coordination with relevant Treasury Department offices (i.e. TFI, Domestic Finance, and International Affairs), should create a multi-agency advisory group to: (i) establish priorities for each financial institution on an annual basis; (ii) review progress with the institutions on a quarterly basis; and (iii) oversee any examination of the institutions.

(3) The advisory group should include senior officials representing the FBI, DHS (Secret Service and other relevant personnel), OFAC, State Department, Defense Department, the intelligence community, and select financial regulators.

BENEFITS. The advantages of centralizing supervision and examination of AML/CFT compliance for complex institutions would be numerous:

» It would allow for the creation of a core, centralized examination team that could

work cooperatively with law enforcement, national security, and diplomatic officials, receiving the necessary security clearances (which bank examiners currently lack) and establishing the necessary trust, to understand the full picture.

» Such an examination team would reward rather than hinder innovation, emphasizing results rather than process. Financial institutions would be instructed to shift resources away from box checking and reporting petty offenses toward law enforcement, national security and global development priorities. As one participant in the symposium noted, "what gets measured gets done."

» Performance evaluations for a FinCEN examination team would be driven by the quality of the information identified and reported by its supervised institutions, and the strength of their analyses, rather than the auditability of its processes, or the number of alerts generated or SARs filed by the institutions. These evaluations would include feedback given by senior national security and law enforcement officials who are now absent from that process.

» The examination team should be well trained in technological innovations, including big data, and work across the financial services industry to leverage those concepts to detect illegal or threatening activity. Such a team could draw on resources at the Defense Advanced Research Projects Agency and elsewhere in the U.S. government.

» The examination team should be fully engaged in the whole range of AML/CFT activities at the institutions it supervises, including working with other agencies to support the institutions' investigations. It would also be knowledgeable about international financial services and money laundering typologies.

» Finally, a centralized supervision and examination function for large, internationally active institutions would contribute to the tailoring of the AML/CFT regulatory regime to participating institutions' risk profiles.

ISSUES. A centralized examination team would require resources. One alternative would be appropriated funds, which would be money well spent. Another would involve FinCEN assessing financial institutions for examination costs in the same way as banking regulators; existing statutory authority appears to allow for such an assessment.[10] Affected institutions would see a corresponding reduction in the assessment they currently pay to prudential regulators for supervision of this function. A third alternative would be to establish a centralized team funded *pro rata* by each of the affected agencies but reporting directly and solely to the Director of FinCEN.

Alternatively, but not ideally, each regulatory agency could designate personnel to serve as members of a joint team to conduct a review of Bank Secrecy Act compliance on its behalf.[11] This approach could leverage the existing cooperation model of the Federal Financial Institutions Examination Council (FFIEC) to create a joint national exam team for AML/

CFT and sanctions issues. The team would still report to FinCEN and would otherwise function as described above. There would also necessarily be some coordination among the exam team and the other regulators, who would remain responsible for safety and soundness examination.

B. FinCEN should institute a process to establish AML/CFT priorities for all covered institutions.

The multi-agency advisory group described above, and led by Treasury and FinCEN, should also establish priorities for the many institutions, including non-banks, that are not subject to centralized exams. FinCEN should communicate that guidance to those regulators that continue to exercise delegated authority for their use in establishing examination standards for the coming year. In addition, FinCEN should meet regularly with the regulators to review progress on priorities.

II. ENACT BENEFICIAL OWNERSHIP LEGISLATION

Federal regulations require financial institutions to know their customers and conduct ongoing monitoring of account information. FinCEN's new customer due diligence rule will soon require financial institutions to collect beneficial ownership information from certain legal entity customers. Yet there is currently no requirement that states record the beneficial ownership of the legal entities they incorporate. This makes it easier for money launderers and terrorist financiers to obscure their identities from both law enforcement and the financial institutions with which they deal. Indeed, the Financial Action Task Force ("FATF") recently criticized the gaps in the legal framework in the United States that prevent access to accurate beneficial ownership information in a timely manner and recommended that the United States take "steps to ensure that adequate, accurate and current [beneficial ownership] information of U.S. legal persons is available to competent authorities in a timely manner, by requiring that such information is obtained at the Federal level."[12] Due to the lack of easily accessible beneficial ownership information, financial institutions allocate significant resources to investigating the ownership of their customers.

Congress should enact legislation—forms of which were pending in both the House and Senate during the 114th Congress and are expected to be re-introduced in the 115th Congress—that would require the collection of beneficial ownership information at the time of incorporation and whenever such information changes, and ensure that such information is provided to relevant stakeholders including FinCEN and law enforcement. In addition, any legislation should clarify that financial institutions performing customer due diligence can obtain access to reported beneficial ownership information upon account opening and on an ongoing basis, and can rely on that information in complying with any obligation to know their customers. Under the current regime, many if not most of the resources devoted to identifying money laundering and terrorist financing are provided by financial institutions; denying them access to this important information would significantly undermine the goals of any bill.

III. ESTABLISH A CLEAR MANDATE IN SUPPORT OF INNOVATION

BACKGROUND. Financial institutions are motivated to assist the government in understanding and identifying financial crime and are constantly developing new methods to thwart money laundering and terrorist financing. One significant example is the establishment of FIUs within large financial institutions. FIUs are often staffed by former law enforcement personnel with significant expertise and strong motivations to help their former colleagues in the government. They generally have broad mandates to evaluate client relationships and the risks they may pose to the institution and the financial system itself. FIUs are most effective when they can be agile and adapt in real-time to threats as they develop. FIUs should be given latitude by regulators to operate outside the compliance regime, giving them the agility needed to aid law enforcement.

RECOMMENDATION. To this end, FinCEN should propose a rule stating that financial institutions are encouraged to innovate in an FIU "sandbox," and that FIUs may operate outside the strictures of regular policies and procedures.

BENEFITS. This proposal may be superfluous for financial institutions designated for FinCEN supervision, as the establishment of priorities and direct communications with the end users of SAR data would naturally cause such institutions to shift resources to priority areas like FIUs. But for any firms not so designated, the current need for prioritization would continue.

IV. DE-PRIORITIZE THE INVESTIGATION AND REPORTING OF ACTIVITY OF LIMITED LAW ENFORCEMENT OR NATIONAL SECURITY CONSEQUENCE

BACKGROUND. The goal of the SAR regime is to provide useful information about money laundering and terrorist financing to law enforcement. The ideal SAR is a well-researched, carefully-written summary of suspicious activity, which is likely to require significant time and energy on behalf of a financial institution's staff. Unfortunately, the current regime promotes the filing of SARs that may never be read, much less followed up on as part of an investigation.[13] Any diversion of resources from creating quality SARs does not truly serve the interest of law enforcement. The SAR regime should produce SAR filings that actually advance law enforcement and other national security goals.

There are two embedded issues: the first is the type of conduct that merits a SAR filing; the second is the level of suspicion or evidence of that conduct that should trigger a filing. We make recommendations with regard to the former here because there was consensus on the reforms needed. The latter is a more complicated question, and is discussed in the next section as an area in need of further review.

Presently, financial institutions are required to file a SAR on two broad categories of conduct. The first encompasses criminal violations that: (i) involve insider abuse; (ii) total at least $5,000 in which a suspect can be identified; or (iii) total at least $25,000, regardless of whether a suspect can be identified. The second encompasses transactions totaling at least $5,000 if the financial institution knows, suspects, or has

reason to suspect that the transaction: (i) may involve money laundering or other illegal activity; (ii) is designed to evade the Bank Secrecy Act or its implementing regulations (e.g. structuring); or (iii) has no business or apparent lawful purpose or is not of the type in which the customer would be expected to engage (and, after examining the available facts, the financial institution knows of no reasonable explanation for the transaction).

RECOMMENDATION:

» The SAR dollar thresholds, which were set in 1996, should be raised.

» The standards for insider abuse should be eliminated. Financial institutions are the victims of these crimes, and therefore have an incentive to report any serious misconduct. Under the current standard, however, they allocate significant resources to investigating employee misconduct leading to termination and establishing a paper trail to justify a decision not to file a SAR, or an investigative record in support of a SAR. As no federal prosecutor will ever follow up on such a SAR, these resources are misallocated.[14]

» FinCEN should review all existing SAR guidance to ensure it establishes appropriate priorities. For example, FinCEN should reconsider its just-issued guidance requiring SAR filings for cyber attacks. Large financial institutions experiencing cyber attacks are already in regular, and frequently real-time communication with law enforcement and other government organizations. They are members of the Financial Services Information Sharing and Analysis Center, which is designed to facilitate cyber and physical threat intelligence analysis and sharing between stakeholders. The relevant governmental organizations will derive few incremental benefits from the filing of a post-hoc SAR; other governmental organizations will make no use of it. But financial institutions will now be taking resources away from responding to cyber attacks to documenting them in regulatory filings that may never be read.

V. PROVIDE MORE RAW DATA TO FINCEN AND FEEDBACK TO FINANCIAL INSTITUTIONS

BACKGROUND. FinCEN's e-filing system provides a common format for suspicious activity reporting, but additional data that could be useful to law enforcement are not provided in a consistent format or in real time. Furthermore, in choosing which information to include in a SAR, financial institutions necessarily bias the data available to law enforcement. For example, since each bank uses different procedures for filing SARs, the combined data set has massive amounts of noise and little information of use to law enforcement. To date, the database is used for federated searches only, and a different approach could identify strategic trends of value to law enforcement and national security personnel.

Furthermore, financial institutions generally provide underlying raw data only at law enforcement request following a SAR filing, but a better approach would facilitate real-time information flow and analysis using modern data capabilities, while adhering to privacy and civil liberty concerns as well as

managing for other risks. The provision of raw data has been considered before – though in a limited capacity. In 2006, FinCEN published a Congressional report on the *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act* in compliance with Section 6302 of the Intelligence Reform and Terrorism Prevention Act of 2004. At the time, the report found that simply implementing a cross-border funds transfer reporting requirement would require significant investment from both the public and private sectors. In particular, it was estimated that FinCEN would need approximately $32.6 million and three and a half years to make sure its system was capable of receiving such information. However, in 2015, FinCEN completed an IT Modernization Project that has likely impacted that original estimate.[15]

The ideal outcome is not each bank analyzing bulk data for a given customer and using resources to draft an elaborate and heavily audited SAR narrative. Rather, a middle ground would be a utility that allows banks to share bulk data and have it analyzed. But the best outcome would be to have bulk data deposited at FinCEN and analyzed by law enforcement and intelligence community professionals, with a mechanism for regular feedback to be provided to institutions to enable them to target their internal monitoring and tracking mechanisms to better serve the goals of law enforcement and intelligence officials.

RECOMMENDATION. Facilitate the flow of raw data from financial institutions to law enforcement, and between financial institutions, under safe harbor protections. FinCEN should require a financial institution to provide a broader set of raw data once the institution has determined that the underlying activity is suspicious. For instance, raw data about the parties to a transaction, including transaction history and such information on their other counterparties, could be shared to form clearer pictures of complex relationships, and the attributes of the parties to the transaction. Any such proposal would need to be crafted with privacy issues in mind: any potential solution would require scrubbing the data of personal identifying information, and inserting a generic identifier in its place. Current technology allows for the sharing of encrypted or hashed unique identifiers, allowing analytical integrity to be preserved while protecting personally identifiable information.

BENEFITS. Providing such data in bulk, directly to FinCEN upon the filing of a SAR, would modernize the SAR regime from one built for the 20th century, where financial institutions were comparatively better equipped to filter data, to one appropriate for the 21st century, where big data analytics could enable law enforcement to effectively sift through large quantities of data without requiring as much assistance from financial institutions in investigating illicit activity. Financial institutions could then reallocate associated resources to FIUs or other higher value activities.

VI. CLARIFY AND EXPAND THE SCOPE OF INFORMATION SHARING UNDER SECTION 314(B)

BACKGROUND. Section 314(b) of the USA PATRIOT Act provides an avenue for financial institutions to share with each other information relevant to potential money laundering or

terrorist financing investigations. In 2009, FinCEN issued guidance explaining that financial institutions are covered by the provisions of Section 314(b) when they participate in a program that "share[s] information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities ('SUAs')" as long as the purpose of the information sharing is to identify and report activities that may involve terrorist activity or money laundering.[16] In a 2012 administrative ruling, FinCEN elaborated on this guidance and distinguished between information sharing that satisfies the purpose requirement and other sharing arrangements that are not covered by Section 314(b).[17] However, the current standard requiring that information shared pursuant to 314(b) must relate to potential money laundering or terrorist financing is vague and limited given the current illicit finance risks facing financial institutions and would benefit from additional clarification.

RECOMMENDATION. Regulatory or statutory changes should encourage additional use of the 314(b) safe harbor.

- FinCEN should clarify that financial institutions can share information about clients as part of their attempt to identify suspicious activity. Such sharing should be permissible even before there is already-formed, formal suspicion of money laundering or terrorist financing. This would not be a wholesale license for financial institutions to broadly share information, but rather would be useful in situations in which one financial institution has incomplete information about a customer's AML/CFT risk and another can provide additional information that produces a fuller picture of the situation – for example, with respect to client on-boarding.

- Congress should expand the 314(b) safe harbor to cover the sharing of information related to illicit finance activities beyond money laundering or terrorist financing. For example, the safe harbor could be revised to permit sharing also for the purpose of identifying and reporting a specified unlawful activity (as defined in 18 U.S.C. 1956(c)(7)). As the Federal crimes listed in 18 U.S.C. 1956(c)(7) include crimes related to computer fraud and abuse, such a revision would protect sharing regarding cybercrimes and identity theft without requiring that financial institutions first determine whether the crime also involves money laundering or terrorist financing.

- Congress should also expand the safe harbor to cover technology companies and other nondepository institutions, to provide greater freedom to experiment with information-sharing platforms.

VII. ENHANCE LEGAL CERTAINTY REGARDING THE USE AND DISCLOSURE OF SARS

To facilitate better information flow on suspicious activity among public and private institutions, financial institutions must be confident in the current confidentiality regime for SAR-related data, including at the enterprise-wide level and across borders.

BACKGROUND. FinCEN regulations generally prohibit the disclosure of SARs and information

that would reveal the existence of a SAR ("SAR information"), with an exception for sharing "within the bank's corporate organizational structure for purposes consistent with Title II of the Bank Secrecy Act as determined by regulation or guidance."[18] In 2006, FinCEN and the federal banking agencies issued guidance providing that a U.S. depository institution may share SAR information with its controlling company (whether foreign or domestic), and that a U.S. branch or agency of a foreign bank may share SAR information with its foreign head office.[19] FinCEN reaffirmed portions of this guidance in 2010 when it issued new guidance permitting U.S. depository institutions to share SAR information with affiliates subject to U.S. SAR regulations (i.e., U.S.-based affiliates).

FinCEN regulations explicitly provide that depository institutions are not prohibited from disclosing the underlying facts, transactions, and documents upon which a SAR is based within the bank's corporate organizational structure.[20] Thus, on its face, the regulations would appear to permit depository institutions to share such information with foreign branches and foreign affiliates. Such sharing should be allowed, particularly where the foreign affiliates are subject to confidentiality agreements or located in FATF-member countries. However, FinCEN guidance does not permit U.S. depository institutions to share SAR information with foreign branches, and, in light of commentary by FinCEN on this topic, the scope of the exception for disclosing underlying information is not entirely clear. For example, in a 2010 final rule, FinCEN indicated that "[d]ocuments that may identify suspicious activity but that do not reveal whether a SAR exists (e.g., a document memorializing a customer transaction, such as an account statement indicating a cash deposit or a record of a funds transfer), should be treated as falling within the underlying facts, transactions, and documents upon which a SAR may be based, and should not be afforded confidentiality."[21] Yet, other language in the Supplementary Information might be read as limiting the exception to information produced in the ordinary course of business.[22] Thus, there is confusion about the extent to which the exception covers facts, descriptions of transactions, and documents that both: (i) underlie a SAR; and (ii) are recited or referenced in, or attached to, a SAR, including with respect to sharing such underlying facts, transactions, and documents with foreign branches and foreign affiliates.[23]

The issue here is not limited to lack of clarity in the U.S. regime, and negotiation with foreign regulators would be important to rationalizing the process.

RECOMMENDATION. FinCEN should:

» By regulation, clearly authorize U.S. depository institutions to share SARs with a foreign branch or affiliate if the branch or affiliate is located in a country that is a member of the FATF.

» For non-FATF countries, establish a clear standard (or list of approved or disapproved countries) that would allow institutions to share SARs within such a country if the U.S. depository institution enters into a written confidentiality agreement with the branch or affiliate that is consistent with the 2006 interagency guidance for SAR

sharing with controlling companies and head offices.[24] While there may be countries of sufficient concern that any information shared could be interdicted and misused, the general presumption should be towards information sharing within an institution.

» By regulation, clearly authorize U.S. depository institutions to share the underlying facts, transactions, and documents upon which a SAR is based with foreign branches and foreign affiliates.

» Encourage other FATF-jurisdictions to adopt policies that apply a substantially consistent standard. [25]

BENEFITS. A less restricted flow of AML information within a banking enterprise would result in:

- better transaction monitoring;
- higher quality SARs;
- better information for law enforcement investigations;
- better knowledge of international money laundering and terrorist financing trends;
- easier implementation of a risk-based, enterprise-wide approach to AML, including mitigating the risk of illicit actors abusing different entities within multinational institutions; and
- efficiencies in the process of preparing SARs, greater uniformity in SARs filed by a banking enterprise, and minimization of duplicative SAR filings.

ISSUES. The major concerns motivating SAR-sharing restrictions relate to the importance of protecting the confidentiality of SARs, which is a legitimate policy goal. However, globally active banking organizations are able and required to employ increasingly sophisticated controls to protect the confidentiality of sensitive information, and those controls have proven effective. Thus, the benefits of allowing institutions to share SARs within their organizations and information that would reveal the existence of a SAR clearly outweigh the risks of such information being inappropriately released.

Areas of Reform Requiring Further Study

The following are reforms that would bring substantial benefits, but warrant further study and the input of a wide array of stakeholders. In some cases—for example, the standard for SAR filings—the issue is extremely complex; in others—for example, the use of utilities—concerns with privacy and data security would need to be resolved.

I. ENHANCE INFORMATION SHARING

BACKGROUND. The theory behind the SAR regime is that financial institutions have vast amounts of information about their customers and are thus best positioned to identify and report suspicious activity. However, the current system encourages stove-piping of information that inhibits the dynamic flow of information among authorities and institutions and limits the ability of any one institution to see the bigger picture. Visibility into information from authorities and peer institutions would provide helpful context to financial institutions and law enforcement.

RECOMMENDATION. Establish AML/Sanctions utilities for information sharing beyond 314(b) sharing. A utility-like database of AML and/or sanctions information gathered from multiple public and private sources has the potential to make the sharing of information among financial institutions and law enforcement more efficient and effective. An AML/sanctions utility would facilitate the bulk screening of transactions against sanctioned and suspect parties and the detection of patterns of potentially suspicious transactions on a real-time basis across multiple financial institutions. This model could have a government agency, such as FinCEN, at the center, or it could rely on a private-sector actor or consortium acting as a clearinghouse. To support such a utility and other outcomes, consideration should be given to the creation of industry forums through which banks and other stakeholders may share resources and collaborate to: (i) address new risks and regulations in a consistent, cost effective manner; (ii) engage in efforts to benchmark with each other, share ideas, and harmonize standards; and (iii) incubate and test collaboration and utility ideas. Such forums could also serve as the vehicle for public/private cooperation on the development of industry utilities.

BENEFITS. Both public and private sector participants have suggested that AML or sanctions utilities have the potential to: (i) better detect illicit or prohibited activity by looking at a wider set of data, including, for example, by examining both sides of a transaction or comparing transactions across multiple financial institutions; (ii) allow the industry to shift resources to more productive uses; and (iii) improve efficiency and enable more consistent compliance approaches across financial institutions of all sizes. A KYC utility could, for instance, be responsible for running adverse media searches on clients, rather than imposing such a duty on every financial institution at which the relevant party holds an account; such an approach would be more efficient, cost-effective, and allow for resources to be allocated to more fruitful investigations.

ISSUES. While there has already been some success in implementing utilities such as Clarient and SWIFT's KYC Registry, efforts to establish utilities have been hampered by regulatory concerns, implementation and operational challenges, and liability concerns as well as the need for further regulatory support and oversight.

- **REGULATORY CONCERNS.** One regulatory concern is reliance. In order to be effective, financial institutions must be able to rely on the information and functions provided by a utility. Time and resources required

to re-validate information or re-perform functions coming from a utility will reduce efficiency, which is a key benefit of utilities. Another is potential regulatory criticism. Financial institutions should be afforded an opportunity to experiment with processes and controls that leverage collaboration and utility models. Without some regulatory flexibility and protection of experimentation, the long-term gain that could be achieved by a utility may be stifled by short-term regulatory risk. Potential solutions to this problem include placing the KYC utility within FinCEN's jurisdiction or making it a government entity.

» **IMPLEMENTATION AND OPERATIONAL CHALLENGES.** The purpose and functionality of a utility must be clearly defined to ensure the utility will be more efficient than individual, in-house systems. Financial institutions must resolve differences in standards, definitions, and processes, and align on technology and data in order for utilities to operate efficiently.

» **LIABILITY CONCERNS.** One possible issue with either a public or private database is potential liability associated with inaccurate information, including in the context of negative news. The impact of such inaccurate information may be multiplied by the tacit endorsement it would receive from its inclusion in the utility or the reports generated by the utility. A safe harbor could be of help here.

» **REGULATORY SUPPORT AND OVERSIGHT.** Utilities will not be effective unless regulators provide meaningful assurance that financial institutions can rely on the information provided by utilities for the fulfillment of certain of their compliance obligations. Regulatory encouragement of and oversight over utilities would provide confidence to the financial services industry and facilitate reliance on such a system. The FFIEC's Multi-Regional Data Processing Servicer program could serve as a model for regulatory oversight of an AML/sanctions utility.

II. PROVIDE BETTER PROTECTION FROM DISCOVERY FOR SAR INFORMATION

BACKGROUND. As the agencies have stated in the FFIEC BSA/AML Examination Manual, under the current regime, the provision of suspicious activity information by financial institutions "is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. . . . [and] the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system."[26] The effectiveness of this monitoring and reporting system depends in large part on the confidentiality restrictions and protections afforded SARs and related materials.[27] Banks take seriously their obligation to help law enforcement, but to perform their job under the current regulatory framework, they need to prepare investigatory materials for the purpose of identifying suspicious activity and determining whether to file a SAR ("SAR Investigatory Materials"). SAR Investigatory Materials include, but are not limited to:

- documents representing drafts of SARs;

- documents memorializing communications that are a part of the investigation of unusual or potentially suspicious activity;
- reports of or internal communications related to unusual or potentially suspicious activity on which SAR reporting may be required (whether generated automatically or manually);
- documents and forms generated by a bank as part of its internal process of determining whether to file a SAR;
- documents relating to a bank's monitoring and investigations to detect unusual or potentially suspicious activity, including descriptions of SAR filing procedures and descriptions of suspicious activity monitoring and investigation policies, procedures, methods and models;
- information about technology and about system alerts used by a bank for suspicious activity monitoring;
- any documents created for the purpose of informing, assessing or reporting (internally) on the bank's SAR investigatory process; and
- pre- and post-SAR communications with law enforcement, including hold harmless letters, law enforcement requests for back-up documentation, and grand jury subpoenas.

Several courts have interpreted "information that would reveal the existence of a SAR" to mean more than documents that indicate whether a SAR has been filed, but others continue to misinterpret this standard on the mistaken belief that documentation produced in the ordinary course of business is not entitled to confidentiality protection even if the business at hand is investigating suspicious activity or potential SAR filings.[28] Therefore, banks are increasingly wary that information about their efforts to identify criminal behavior will be revealed, including through litigation or arbitration. Further, these decisions are likely to ultimately: (i) inhibit the robust investigative processes that banks undertake today in an effort to make their SARs as useful as possible to law enforcement; and (ii) undermine the industry's ability to effectively detect and report suspicious activity by revealing the techniques and processes they use.

RECOMMENDATION. Congress should enact legislation making clear that SAR Investigatory Materials are to be treated as confidential, particularly in private litigation.[29] An alternative approach could be the issuance of guidance to this end by FinCEN jointly with the federal financial regulators.

BENEFITS. The disclosure of SAR information in private litigation could undermine the ability of financial institutions to effectively combat financial crimes by compromising ongoing investigations, chilling financial institutions' willingness to file detailed SARs, and revealing the financial institution's process for analyzing and reporting such data. Thus, this legislation could help both to allow financial institutions to continue filing the most helpful SARs possible, and protect bad actors from discovering their methods for doing so.

ISSUES. Some believe that litigants and others have a right to information potentially contained in SAR Investigatory Materials for a variety of reasons, some of which could be considered in the proposed legislation.[30]

III. CLARIFY AND BALANCE THE RESPONSIBILITY OF THE PUBLIC AND PRIVATE SECTOR TO DETECT AND PREVENT FINANCIAL CRIME

BACKGROUND. The current AML/CFT statutory and regulatory regime does not clearly allocate responsibility for detecting and preventing financial crime between the public and private sectors. The current system creates incentives for financial institutions to de-risk, thereby withdrawing financial services to already underserved populations and pushing transactions out of the traditional financial services sector into shadow banking channels that are not monitored for suspicious activity. The result of this de-risking is to deprive law enforcement of valuable intelligence. De-risking may also perpetuate political and economic instability in already unstable regions, potentially giving rise to terrorism and criminal activity in the absence of legitimate economic opportunities.

Government intervention is needed to reverse the de-risking trend and better allocate money laundering and terrorist financing risk. For instance, in recent months, Treasury and the federal banking agencies have issued a joint fact sheet on foreign correspondent banking and AML/CFT and sanctions supervision and enforcement.[31] The OCC followed with a Bulletin on *Risk Management Guidance on Periodic Risk Reevaluation of Foreign Correspondent Banking*.[32] These statements indicate a recognition of the problems caused by de-risking, but do not provide a workable solution. Rather than providing assurances that an enforcement action will not result from maintaining accounts for customers based in countries considered high risk, these proposals could be read as imposing, without a basis in law, a new legal obligation, and potential liability: not to de-risk.

As noted above, the most effective way to reduce inappropriate de-risking is to change the way internationally active banks are supervised, giving voice to the numerous government agencies that would prefer that U.S. banks remain engaged abroad – whether in correspondent banking, facilitating payments through money-service businesses, or supporting NGOs. We believe that step is necessary and may even be sufficient. However, the below initiatives could also better align responsibility and encourage innovation in the financial sector.

IV. ESTABLISH A PROCEDURE AND RESOURCES FOR NO-ACTION LETTERS

BACKGROUND. There is no established mechanism by which financial institutions can query FinCEN about certain actions and receive, if warranted, confirmation that no enforcement would be initiated if they are undertaken. The SEC has established such a procedure, the no-action letter, to ensure that the financial institutions it regulates have access to the government's perspective on complicated issues.[33]

RECOMMENDATION. FinCEN should provide a no-action letter mechanism for financial institutions to pose compliance questions in a format designed to promote efficiency. Regulators would be empowered to grant a prospective shield from liability on a question posed, provided that the facts represented are substantially accurate and any conditions set are followed. In considering the response, regulators and law enforcement would discuss the merits of particular inquiries.

BENEFITS. While rulemaking and the issuance of guidance are cumbersome processes that do not always promote innovation or dialogue with the industry, a no-action letter process could be more effective. It would (i) allow individual financial institutions to ask particular questions about actions they plan to take, thereby spurring innovation; (ii) provide quick answers, thereby promoting dynamism; and (iii) increase the flow of information from industry to FinCEN about new technologies and procedures, thereby improving information for FinCEN's rulemaking and enforcement purposes.

ISSUES. Although such a proposal would protect against the risk of enforcement by FinCEN, OFAC, and the federal examiners for potential violations of the Bank Secrecy Act or OFAC sanctions, it would not necessarily eliminate liability from state or foreign regulatory authorities. However, coordination through bilateral negotiations or forums such as the FATF might encourage global cooperation that would provide real assurance to financial institutions willing to certify their AML compliance programs. In addition, FinCEN would likely need to be provided with additional resources to implement such a mechanism – though such a change would ultimately achieve efficiency gains for the broader regime. Consideration should also be given to whether there are areas where state law should be preempted.

V. PROVIDE CLEAR STANDARDS TO FINANCIAL INSTITUTIONS

BACKGROUND. Financial institutions currently operate under a strict liability, post-hoc regulatory standard that is both opaque and constantly changing. As a result, they have been forced, in many cases, to deemphasize innovation and the pursuit of real AML/CFT risk, and instead focus on adherence to examiner-approved policies and procedures. They "work to the rule" in the worst sense, because this is the best way to insulate themselves from liability. The AML/CFT regime should be geared toward law enforcement outcomes, not only compliance processes.[34]

In addition to the above proposed reforms to the supervision of financial institutions, other steps could be taken.

RECOMMENDATION.

1. FinCEN should establish by regulation a clearer definition of what constitutes a reasonable AML/CFT program, including what conduct will result in an enforcement action or prosecution. If a financial institution engages in compliance conduct that a regulator deems acceptable ex ante and illicit financial activity still occurs, the issue can be addressed through discussions between financial institutions and their regulators, with no enforcement action taken.

2. FinCEN could also provide clear assurances that any sanction imposed will come only after a holistic review of the financial institutions' overall performance, and in no case be based on the failure to file a single SAR, unless the failure to file was found to be willful. Rather, any significant sanction should be based on a pattern or practice of noncompliance.

Additional, detailed guidance from FinCEN is necessary with respect to the following topics:

- **DUE DILIGENCE ON CUSTOMERS OF CUSTOMERS.** Although FinCEN's recent customer due diligence rule explains the circumstances in which financial institutions must identify beneficial owners of legal entity customers, there is still considerable confusion about the extent of due diligence financial institutions must conduct on the customers of their customers in order to conduct what examiners consider a reasonable AML compliance program.

- **RELIANCE.** Similarly, FinCEN could clarify the extent to which a financial institution can reasonably rely on work done by another financial institution, or by a utility or collection of institutions; absent a clear safe harbor, the examination process is likely to nullify any efficiency gains by requiring that work be duplicated.

- **MONITORING FOR CONTINUING SUSPICIOUS ACTIVITY.** FinCEN has issued guidance on when financial institutions should file SARs on suspicious activity of a continuing nature, but the financial industry would benefit from additional, more detailed guidance about FinCEN's expectations for ongoing monitoring for the purpose of detecting and reporting continuing suspicious activity. In other words, what specific monitoring, if any, should financial institutions do, above and beyond their regular transaction monitoring once they have filed a SAR on a given customer or account, in order to determine whether the activity reported in the initial SAR is of a continuing nature.

- **WHEN DOES A FINANCIAL INSTITUTION HAVE REASON TO SUSPECT A TRANSACTION IS SUSPICIOUS?** Financial institutions are required to file SARs when they "know, suspect, or have reason to suspect" that a transaction is suspicious. But if a financial institution does not actually know or suspect that a transaction is suspicious, under what circumstances can a regulator infer that the financial institution had reason to suspect a transaction was suspicious? FinCEN should provide guidance on this important issue.

BENEFITS. Unclear standards result in financial institutions devoting compliance and legal resources to divining regulators' meaning, instead of focusing on investigating and reporting suspicious activity. Such unclear standards lead any rational actor to err on the side of caution, resulting in the defensive filing of SARs at the expense of higher value compliance activities and law enforcement outcomes. These concerns are sharpened in the current enforcement environment, which increasingly focuses on holding individuals liable for alleged programmatic issues.

VI. BETTER COORDINATE AML/CFT AND SANCTIONS POLICY GOALS, SUPERVISION AND ENFORCEMENT

BACKGROUND: The AML and sanctions compliance regimes are increasingly interdependent, even if their aims are not always consistent. Regulators treat AML and OFAC compliance as related, as demonstrated by the FFIEC BSA/AML Examination Manual, which contains a section on OFAC compliance and examination procedures. A recent regulation issued by the New York State Department of Financial Services addresses both AML transaction monitoring programs and OFAC filtering programs.[35] Examiners and auditors often test both AML and sanctions compliance programs together, and enforcement actions frequently allege violations of both the Bank Secrecy Act and OFAC sanctions.

This has led many large financial institutions to treat AML and OFAC compliance as related disciplines that, along with anti-bribery and corruption, fall within the realm of financial crimes compliance. They employ similar tools to deal with both AML and OFAC compliance. For example, customer due diligence procedures must address screening customers against sanctions watch lists and for indicia of money laundering or terrorist financing risk.

At the U.S. Treasury, both FinCEN and OFAC are housed within TFI, reporting to its undersecretary. Prior to 2002, when Section 361 of the USA PATRIOT Act made FinCEN a separate bureau of the Treasury, both FinCEN and OFAC were sister offices within Main Treasury. Today, FinCEN is a bureau, while OFAC is still a Main Treasury office. The Office of Terrorist Financing and Financial Crimes (TFFC)—also a component of TFI within Main Treasury—is responsible for coordinating policy with respect to the full spectrum of illicit finance threats. Over time, some of the prior synergies between FinCEN and OFAC may have been lost as FinCEN has become increasingly independent.

Additionally, the aims of the sanctions and AML/CFT regimes can, at times, also work at cross-purposes, excluding from the financial system the very bad actors most likely to conduct suspicious activity that is ultimately reported to law enforcement.

RECOMMENDATION: Better coordination would help reconcile competing U.S. government priorities and align their effect on financial institutions, while creating efficiencies.

For example, Treasury could speak with one voice regarding regulatory expectations with respect to illicit finance, helping to better address the competing policy goals of excluding certain bad actors from the financial system while also providing valuable financial intelligence to law enforcement.

As noted above, one way to accomplish these aims would be to strengthen TFI, particularly with respect to its oversight of FinCEN and OFAC. Empowering TFI to truly coordinate policy and enforcement across both FinCEN and OFAC would ensure that Treasury policy goals all move in one direction with little drag. TFI could also be given a more visible role in industry outreach.

VII. MODERNIZE THE SAR REGIME

BACKGROUND. As described in an earlier recommendation, standards for SAR filings have incentivized filing SARs on activity that prosecutors are unlikely to pursue. We recommend changing the type of activity that merits a SAR filing. An equally important, but more complicated question, is the level of suspicion of that activity that should merit a filing. Obviously, that could vary from merest suspicion to absolute certainty, and it is a difficult but important task to determine where on that spectrum the standard should be set.

RECOMMENDATION. Another approach would be for FinCEN to further elaborate on the reporting criterion for what is deemed "suspicious" – whether it be illicit activity, criminal activity, or activity that is clear evidence of one of these categories. Furthermore, it would be helpful if the aforementioned guidance also provided contours for SARs that should not be filed. Further elaboration of the SAR-filing standard would relieve financial institutions of the need to file SARs on activity that is merely suspicious without an indication that such activity is illicit. Whether a financial institution perceives an activity as "suspicious" is inherently subjective, and a bright-line approach would take the subjective guesswork out of SAR filing. However, there are some significant drawbacks, requiring SAR filings only in cases of a more objective standard—such as illicit or criminal activity—requires legal analysis that is not currently required and may actually prove to be more burdensome than the current regime.

Changing the SAR filing thresholds would also require modifying multiple statutes, including the Bank Secrecy Act and the Federal Deposit Insurance Act, and implementing regulations thereunder.

Conclusion

As decribed above, the stakes are high. Under the current AML/CFT statutory and regulatory regime, the nation's financial firms play an integral role in preventing, identifying, investigating, and reporting criminal activity, including terrorist financing, money laundering and tax evasion. Yet, today, most of the resources devoted to AML/CFT compliance by the financial sector have limited law enforcement or national security benefit, and in some cases cause collateral damage to other vital U.S. interests. A redeployment of these resources could substantially increase the national security of the country and the efficacy of its law enforcement and intelligence communities, and enhance the ability of the country to assist and influence developing nations.

Endnotes

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

2 See The Center for Global Development's report entitled "Unintended Consequences of Anti-Money Laundering Policies for Poor Countries," Table 1, found on Page 8, for a sampling of some of the federal government entities involved in AML/CFT. In addition, many state government entities are imposing standards.

3 While various documents are released by governmental and multinational entities providing guidance on AML/CFT issues or further elaborating on the current state of AML/CFT risks, like the U.S. Treasury's *2015 National Money Laundering Risk Assessment*, diffuse FinCEN guidance and FATF typologies, none provides a clear set of priorities for U.S. financial institutions as they seek to assist law enforcement in their AML/CFT efforts.

4 Multiple participants reported that examiners have developed expected ratios of alerts to SARs, though such ratios have never been published for notice and comment.

5 See National Crime Agency, Joint Money Laundering Intelligence Taskforce, **http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit**. While in the United States, the Treasury Department has a Bank Secrecy Act Advisory Group (BSAAG), it has not taken on an operational role.

6 See 31 C.F.R. § 1010.810. "Overall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter, is delegated to the Director, FinCEN." *Id.* § 1010.810(a). See also 12 U.S.C. § 1818(s).

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

8 While FinCEN would be free to adopt its own definition and decision, existing banking law already provides ways of making such a determination; in other words, this is not a novel concept.

9 It should be noted that even if FinCEN were to revoke its delegated exam authority, the federal banking agencies would have additional statutory authorities under which they would likely still be required to conduct exams for AML/CFT compliance. However, in order to further streamline and centralize the examination of large multinational institutions, there appears to be no reason why they would not be able to delegate such authorities to FinCEN.

10 The Independent Offices Appropriation Act provides general authority for a government agency to assess user fees or charges by administrative regulation, based on the value of the service to the recipient. See 31 U.S.C. § 9701. OMB Circular No A-25 provides further guidance regarding "user fees" ("A user charge . . . will be assessed against each identifiable recipient for special benefits derived from Federal activities beyond those received by the general public."). See OMB Circular No. A-25 Revised.

11 See, e.g., 12 U.S.C. §§ 1786(q), 1818(s)(2).

12 See FATF Anti-money laundering and counter-terrorist financing measures, Mutual Evaluation of the United States, December 2016, pg. 11; *available at:* **http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf**. FATF also noted that "deficiencies in [customer due diligence] requirements (in particular [beneficial ownership] requirements) can undermine the usefulness of SARs," FATF 2016 Mutual Evaluation of the United States, pg. 58.

13 As noted in note 12, FATF found that "deficiencies in [customer due diligence] requirements (in particular [beneficial ownership] requirements) can undermine the usefulness of SARs" in the United States. FATF 2016 Mutual Evaluation of the United States, pg. 58.

14 An alternative mechanism for reporting insider abuse to the banking regulators could be established, as necessary.

15 In a speech in October 2015, former FinCEN Director Jennifer Shasky Clavery stated that through the IT modernization program "(1) we assumed responsibility for maintaining our own data in a FinCEN system of record; (2) we supported a significant shift from the paper filing of BSA reports to the electronic filing of BSA data; (3) we developed a new IT system for our many law enforcement and regulatory partners to search, slice, and dice BSA data; and (4) we provided advanced analytics tools to FinCEN's analysts to enhance their capabilities to make sense of the data. *Available at:* **https://www.fincen.gov/news/speeches/jennifer-shasky-calvery-director-financial-crimes-enforcement-network-4**."

16 FinCEN, *Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act*, FIN-2009-G002 (June 16, 2009).

17 FinCEN, *Administrative Ruling Regarding the Participation of Associations of Financial Institutions in the 314(b) Program*, FIN-2012-R006 (July 25, 2012) ("[I]nformation shared for the purposes of identifying fraud or other specified unlawful activity that is not related to a transaction involving the possibility of money laundering and/or terrorist financing is not covered by the statutory safe harbor.").

18 31 C.F.R. § 1020.320(e)(1)(ii)(B).

19 Interagency Guidance, Sharing Suspicious Activity Reports with Head Offices and Controlling Companies (Jan. 20, 2006).

20 31 C.F.R. § 1020.320(e)(1)(ii)(A)(2).

21 75 Fed. Reg. 75593, 75595 (Dec. 3, 2010).

22 *Id.* at n. 13 ("As one commenter correctly suggested, information produced in the ordinary course of business may contain sufficient information that a reasonable and prudent person familiar with SAR filing requirements could use to conclude that an institution likely filed a SAR (e.g., a copy of a fraudulent check, or a cash transaction log showing a clear pattern of structured deposits). Such information, alone, does not constitute information that would reveal the existence of a SAR.")

23 For avoidance of doubt, please note that this group is not requesting guidance with respect to the confidentiality of SARs themselves, or even draft SARs, or documents produced in the course of a depository institution's transaction surveillance procedures or investigation of whether to file a SAR – all of which are confidential under 31 C.F.R. § 1020.320(e)(1)(i).

24 Interagency Guidance, Sharing Suspicious Activity Reports with Head Offices and Controlling Companies (January 20, 2006).

25 FATF has advised the U.N. Security Council that the need for enhanced information sharing globally is critical in order to enhance the ability to combat terrorism and, in particular, to defeat ISIL. *See* **http://www.fatf-gafi.org/publications/fatfgeneral/documents/importance-urgent-action-to-implement-fatf-standards-counter-terrorist-financing.html**

26 FFIEC BSA/AML Examination Manual (2014), 60.

27 *See* 31 U.S.C. § 5318(g)(2) and 31 C.F.R. § 1020.320(e); 12 C.F.R. § 21.11(k).

28 *See* 31 C.F.R. § 1020.320(e); 12 C.F.R. § 21.11(k). FFIEC BSA/AML Examination Manual (2014), 73 ("A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill Bank Secrecy Act obligations and responsibilities. For example, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR"). *See also Cotton v. PrivateBank & Trust Co.*, 235 F. Supp. 2d 809, 814-15 (N.D. Ill. 2002) (holding that documents representing drafts of SARs or other work product or privileged communications that relate to the SAR itself are confidential); *Whitney National Bank v. Karam*, 306 F. Supp. 2d 678, 683 (S.D. Tex. 2004) (holding that SAR confidentiality protects "discussions leading up to . . . the preparation of filing of a SAR or other form of report of suspected or possible violations."); *but see First Am. Title Ins. Co. v. Western Bank, No. 12-CV-1210*, 2014 U.S. Dist. LEXIS 121063 at *5 (E.D. Wis. August 29, 2014) (allowing production of fraud alerts, including information automatically generated by fraud monitoring software, because "[n]ot all means or methods a bank may use to detect fraud or other financial irregularity are privileged simply because they might culminate in a SAR."); *Freedman & Gersten, LLP v. Bank of America, N.A.*, 09-cv-5351, 2010 U.S. Dist. LEXIS 130167 at *10 (D.N.J. Dec. 8, 2010)(holding that "general policies and procedures concerning the handling of suspicious activity," and "any memoranda or documents drafted in response to the suspicious activity" are not entitled to protection because they merely reflect the bank's "standard business practice" for investigating suspicious activity).

29 The term "bank" as used in this section has the meaning given to it in 31 C.F.R. § 1010.100(d).

30 *See* , e.g., Wultz v. Bank of China, 56 F. Supp. 3d 598, 602-603 (S.D.N.Y. 2014) (case brought by Wultz family against Bank of China for terrorist-related death of family member, alleging that a customer of BOC, Said al-Shurafa ("Shurafa"), was a senior operative of the terrorist group responsible for the bombing and that BOC assisted Shurafa by executing dozens of wire transfers on his behalf totaling several million dollars).

31 *See* "Joint Fact Sheet on Foreign Correspondent Banking," August 30, 2016. *Available at:* **https://www.treasury.gov/press-center/press-releases/Documents/Foreign%20Correspondent%20Banking%20Fact%20Sheet.pdf.**

32 See OCC Bulletin 2016-32, "Risk Management Guidance on Foreign Correspondent Banking," October 5, 2016. *Available at:* **https://www.occ.gov/news-issuances/bulletins/2016/bulletin-2016-32.html.**

33 FinCEN has established a process for issuing "administrating rulings." FinCEN has explained that "[i]n conformance with the procedures outlined at 31 CFR § 1010.710-717, we will issue administrative rulings interpreting regulations contained in Chapter X either unilaterally or in response to specific requests made and submitted to us consistent with the procedures outlined at 31 CFR § 1010.711. Administrative letter rulings . . . are issued pursuant to our authority as the administrator of the Bank Secrecy Act, if the facts and circumstances, issues, and analyses that appear in an administrative letter ruling are of general interest to financial institutions then the letter ruling is published on our website. Published letter rulings often express an opinion about a new issue, apply an established theory or analysis to a set of facts that differs materially from facts or circumstances that have been previously considered, or provide a new interpretation of Title 31 of the United States Code, or any other statute granting FinCEN authority. *See* **https://www.fincen.gov/sites/default/files/shared/regrelease.pdf** . By contrast, the SEC has explained that "[a]n individual or entity who is not certain whether a particular product, service, or action would constitute a violation of the federal securities law may request a "no-action" letter from the SEC staff. Most no-action letters describe the request, analyze the particular facts and circumstances involved, discuss applicable laws and rules, and, if the staff grants the request for no action, concludes that the SEC staff would not recommend that the Commission take enforcement action against the requester based on the facts and representations described in the individual's or entity's request." *See* **https://www.sec.gov/answers/noaction.htm**

34 In its Mutual Evaluation of the United States, FATF concluded that "there is a need for more and ongoing guidance from supervisors to industry on their regulatory expectations." FATF 2016 Mutual Evaluation of the United States, pg. 135.

35 *See* New York State Register Notice, *Regulating Transaction Monitoring and Filtering Systems Maintained by Banks, Check Cashers and Money Transmitters*, New York Department of Financial Services, July 20, 2016.

ABOUT THE CLEARING HOUSE

The Clearing House is a banking association and payments company that is owned by the largest commercial banks and dates back to 1853. The Clearing House Association L.L.C. is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system. Its affiliate, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States and is currently working to modernize that infrastructure by building a new, ubiquitous, real-time payment system. The Payments Company is the only private-sector ACH and wire operator in the United States, clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume.

The Clearing House®
At the Center of Banking Since 1853®

Executive Profile

GREG BAER
President of the Association
Executive Vice President and General Counsel of the Payments Company
Office: 212.613.0138
greg.baer@theclearinghouse.org

Greg Baer is President of The Clearing House Association and Executive Vice President and General Counsel of The Clearing House Payments Company, the oldest and largest private sector payments operator in the United States. The Clearing House Association represents the interests of The Clearing House's commercial bank ownership on a diverse range of regulatory and legislative matters through position papers, academic research, comment letters, and *amicus curiae* briefs. Mr. Baer oversees the legal, compliance, and litigation functions for the organization's payments business and leads the strategic agenda and operations of the Association.

Prior to joining The Clearing House, Mr. Baer was Managing Director and Head of Regulatory Policy at JPMorgan Chase, working to analyze the impact of regulatory developments, formulate and present positions to regulatory authorities globally, and engage in capital policy and planning. He previously served as General Counsel for Corporate and Regulatory Law at JPMorgan Chase, supervising the company's legal work with respect to financial reporting, global regulatory affairs, intellectual property, private equity and corporate M&A, and data protection and privacy.

Mr. Baer previously served as Deputy General Counsel for Corporate Law at Bank of America, and as a partner at Wilmer, Cutler, Pickering, Hale & Dorr. From 1999 to 2001, Mr. Baer served as Assistant Secretary for Financial Institutions at the U.S. Department of the Treasury, after serving as Deputy Assistant Secretary. Prior to working for the Treasury Department, Mr. Baer was managing senior counsel at the Board of Governors of the Federal Reserve System.

Mr. Baer received his J.D. cum laude from Harvard Law School in 1987, and served as managing editor of the *Harvard Law Review*. He received his A.B. with honors from the University of North Carolina at Chapel Hill in 1984. He is the author of two books: *The Great Mutual Fund Trap* (Random House, 2002) and *Life: The Odds (And How to Improve Them)* (Penguin-Putnam, 2003).

June 28, 2017

Testimony of

Lloyd DeVaux

On behalf of the

Florida Bankers Association

before the

House Financial Services Committee

Subcommittee on Financial Institutions and Consumer Credit

United States House of Representatives

Testimony of Lloyd DeVaux

On behalf of the

Florida Bankers Association

before the

House Financial Services Committee

Subcommittee on Financial Institutions and Consumer Credit

United States House of Representatives

June 28, 2017

Chairman Luetkemeyer, Ranking Member Clay and members of the subcommittee, my name is Lloyd DeVaux. I am President & CEO of Sunstate Bank, which is a community bank founded in 1999 based in South Florida. My bank has $200 million in assets with three locations in Miami-Dade County.

I appreciate the opportunity to be here today to present the views of the Florida Bankers Association regarding the challenges and burdens the industry faces in complying with the demands of the Bank Secrecy Act (BSA).

Sunstate Bank has 45 employees and focuses on the needs of small businesses, consumers, real estate investors, and non-resident aliens in the communities we serve. We have approximately 3,000 business and retail deposit accounts, including demand, money market, savings and certificates of deposits, and approximately 300 loans. We also offer safekeeping services to foreigners.

As a community bank, we have seen an influx of *new* regulations over the past few years as well as *additional* requirements under *old* regulations such as the Bank Secrecy Act. Clearly, BSA compliance is an important building block for our national security, but it is founded on principles that were developed nearly 50 years ago. The world has drastically changed since the BSA was adopted in 1970; criminals keep evolving and staying one step ahead of banks and law enforcement. As the United States takes steps to combat terrorism and financial crime, now would be a good time to update the compliance requirements to develop a system suited to the twenty-first century.

In late 2013, to ensure that the bank had a robust BSA/Anti-Money Laundering (AML) compliance program, the board of Sunstate Bank made the decision to seek new management and I was hired in July, 2014. Over the next 18 months, we strengthened our BSA/AML program in all phases, including system enhancements, new policies and procedures, additional staffing, and extensive training. At the beginning of the process, to ensure that the bank was proceeding in the right direction, a significant portion of the bank's efforts involved hiring outside consultants—at annualized rates of $110,000 to $185,000 per year per consultant.

The resources devoted to compliance, especially BSA compliance, are significant for a bank of our size. Sunstate Bank employs seven people to manage its compliance program, including six full-time employees in BSA/AML and one in consumer compliance. This represents 15.5% of total staffing of 45 people, and the BSA/AML staff includes both a BSA/AML Officer and deputy BSA/AML officer. This represents a 100% increase in staffing over 2012 levels, even though the Bank has not changed significantly in size and number of customers. However, it underscores the fact that BSA compliance efforts represent a significant use of bank resources, in time, money and human capital.

Our experience is not unique. In 2007, 86% of Florida banks had five or less BSA/AML employees. Now only 62% have five or less. BSA/AML staffing has increased for many banks. While some of this is due to acquisitions, much has been driven by regulatory pressure to add more resources to BSA/AML and the regulatory risk and concern over enforcement actions.

The added costs of BSA/AML compliance—on top of the significant costs from Dodd Frank—has been significant and has led to the disappearance of many smaller institutions in Florida. Small banks have found it difficult to survive on their own due to the current regulatory environment. Many have decided to sell or merge with a larger bank. This has impacted our communities because small banks do the highest percentage of lending to small businesses.

For example, since 2007, 173 banks have disappeared. More telling, is 111 of those disappeared after Dodd Frank was enacted—a consolidation of more than 50% of all Florida banks in just the last 7 years.

What is more important about the impact that the cost of compliance is having isn't in direct costs but rather how it affects our customers and our communities. In an informal survey

conducted by the Florida Bankers Association, 91% of the banks that responded said that BSA/AML regulation has caused them to avoid certain industries, decrease business development, and lower customer retention. Many industries that are legal businesses are labeled "high risk" by regulators. This means banks must collect more customer data, conduct more analysis, provide more oversight and monitoring, and engage in more site visits—all of which translates into higher costs for the bank and for the customer. The best option, in many cases, is to not bank certain industries and certain customers, and to ask existing customers to close their account(s). From the bank's perspective, it is a simple matter of cost/benefit analysis: the economics of compliance make it unprofitable to maintain certain accounts.

Most importantly, the costs and risks associated with compliance are driving some customers outside the banking industry. This creates opportunities for an underground economy or shadow banking system to serve their needs. That has serious drawbacks which must be considered by policy-makers. First, it makes no sense to create a system that drives legitimate customers outside the formal banking system to less regulated or even unregulated providers. Second, it creates a system and series of financial transactions that may not be reported or available to law enforcement. And third, it can create a shadow financial system that is readily available for criminals and terrorists.

Overview of the BSA Program

All BSA/AML Programs must adhere to four pillars. These pillars are: (1) a strong monitoring program, (2) a periodic third-party independent review, (3) a BSA Officer responsible for overseeing the program, and (4) an effective training program across the organization that is appropriately geared to the responsibilities of each individual. And, a new fifth pillar that imposes new expectations for Customer Due Diligence is now being enforced. Failure to comply with any of these pillars is a violation of law, and whether it is by error, neglect or malfeasance, a misstep can result in a Consent Order, monetary fines, and even arrest in some cases. Should that happen, it can cause damage to the reputation and financial strength of the organization, and possibly lead to the loss of the bank's charter.

Additionally, personal legal fees and fines incurred by officers and directors to defend a BSA/AML legal action against them cannot be paid by the institution or by the institution's insurance. With a renewed focus on personal liability, *even for actions outside a compliance officer's personal control*, the reluctance by individuals to take on compliance responsibilities is increasing. Already, the personnel costs for hiring a trained and competent compliance professional have been increasing, and more banks are reporting that it is difficult to find qualified individuals to serve that role.

As mentioned above, Sunstate Bank has six people just in BSA/AML—***the largest department in the bank***. We only have ***four*** full-time lenders. That means that we have fewer staff devoted to serving customers and making loans that benefit the community than we have devoted to compliance. This is not a recipe for success. BSA/AML expenses were more than 10% of total expenses for our bank in 2016. The more we spend on compliance and regulations, the less we have to spend on service for our communities. Every $100,000 spent on compliance translates to $1,000,000 less we can lend.

To understand how this impacts the bank, it would help if I describe BSA/AML compliance, starting with the opening of a new customer account. There are a number of major activities related to BSA/AML compliance for on-boarding and monitoring a customer. The easiest way to visualize this is by following the path of a customer through the process.

New Customer scenario

BSA/AML compliance starts the minute a new customer walks through the door. Once the bank has established the type and purpose of the account the customer wants to open, it is required to properly identify the customer. The Customer Identification Program (CIP) rule requires the bank to obtain the name, date of birth, address, and an identification number of the customer and then independently verify the customer's identity. In the current environment, we must go beyond using picture IDs such as passports and driver's license. To meet the expectations of bank examiners, CIP rules encourage "banks to review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity." Other forms of identification that may be used to supplement the picture ID, are Social Security card, birth certificate, utility bills, or mortgage statements.

Once the bank has properly identified the customer and verified the customer's identity, it is expected to determine the anticipated monthly activity in the account; where deposits will come from, and where the money will go. This includes the number of transactions, and the aggregate dollar amount, by each type of transaction (checks, wires, debit card usage, ACH, internal transfers, cash, etc.). According to the banking agencies, all this information is needed to set up the customer's expected risk profile in the monitoring system. Deviations from this profile will generate alerts on a daily, weekly, and monthly basis.

Based on a number of determinants such as country of residence or countries where business is conducted, type of business, dollar and transaction volumes, expected cash activity, etc., the customer is rated as high, medium or low risk. If a customer is determined to be high risk, the bank conducts a High Risk Review (HRR) every year. For customers that have very active accounts, when the dollar volume passing through an account exceeds $3.5 million annually, the customer must be visited at their office, in the country where the business is located, by the bank every 24 months; plus the customer has to provide updated financial statements. In 2016, the Bank had to perform 157 HRRs and 50 visitations. This effort is needed solely to comply with BSA expectations.

Another requirement when the bank opens a new account is to check the OFAC (Office of Financial Asset Control) database to ensure the customer is not on the OFAC sanctions list. It is important to understand that the list of individual and entities on the OFAC lists can change almost daily. For example, in 2016, my bank received updated OFAC database lists 73 times. In order to ensure the Bank remains in compliance with OFAC requirements, the bank runs all customers and accounts, including beneficial owners, through the OFAC database every evening during the nightly batch update. Additionally, an OFAC check is done anytime a customer sends or receives a wire or ACH; purchases a monetary instrument or visits the teller. ***Despite all of this matching activity, the bank did not have a single positive OFAC match in 2016.*** However, because there are penalties for conducting a transaction with someone on the OFAC list, it is important that the bank perform this constant check.

Once an account has been established, it is then monitored daily, weekly, and monthly to ensure that the activity matches the risk profile that was created for the customer at account opening. If the activity doesn't match the profile, the monitoring system generates alerts to be

reviewed and cleared by the BSA/AML department. These alerts have to be reviewed manually by a bank employee to determine if they are in line with the profile and the nature of the business. If there is a question about whether the activity is appropriate or within the expectations for that individual's profile, a case will be opened and a full investigation conducted. Most of the time, this investigation will require research by the bank and possibly additional supporting information from the customer. If the investigation is not able to clear the transaction, the case will then be flagged for further review to determine if a suspicious activity report (SAR) should be filed to alert law enforcement. Sunstate Bank processed 7,109 alerts in 2016; which resulted in only 15 SARs being filed.

Cash and monetary instrument activities are watched closely. All aggregate cash transactions on a customer's account, in and out of the bank, on a daily basis in excess of $10,000 are reported on a Currency Transaction Report (CTR). Repetitive cash activity between $3,000 and $10,000 that triggers an alert will be investigated for structuring (purposely trying to avoid the CTR filing limit). Finally, all cash for the purpose of purchasing a monetary instrument, such as official checks, money orders, and gift cards, are logged. All BSA records, including these logs, must be kept for five years after the account is closed.

While the concept of filing a CTR seems straightforward, it can be challenging. The Financial Crimes Enforcement Network (FinCEN) requires detailed information about the customer holding the account where the funds were deposited or withdrawn. In addition, since the person who conducted the transaction may not be the account-holder, the bank also is required to collect information, including occupation or profession, about that individual as well. Finally, the bank must also identify the person(s) on whose behalf the transaction is conducted. And, compounding the challenge facing the bank is that we are expected to aggregate transactions over the course of the day to identify instances where a customer might have made multiple deposits at different locations or through different channels.

The question is whether all this effort to report large cash transactions is particularly helpful. The past FinCEN Director, Jennifer Shasky Calvery, commented that law enforcement made use of approximately 65% of CTRs on file to identify additional suspects, accounts or assets during an investigation. That means that the efforts undertaken by banks to file that information is used for supplemental purposes, not to start an investigation. Second, it means that

nearly one-third of all the CTRs filed are never used. And yet, there have never been any efforts made to identify whether there is a common trend or basis associated with these unnecessary CTRs that would let banks stop filing useless CTRs.

In the Money Laundering Suppression Act of 1994, Congress directed the Secretary of the Treasury to reduce CTR filings by 30%. Despite efforts by FinCEN, that goal has never been achieved. There have been other unsuccessful attempts to eliminate needless reports. In 2006, Congress considered the Seasoned Customer CTR Exemption Act to let banks exempt customers when the cash transaction information was identified as having little or no value to law enforcement. And, even though similar bills have been introduced since then, that format for exempting customers has never been adopted. Meanwhile, the number of CTR filings continues to rise.

Even when the process is automated, it takes time to verify that the filing is correct and complete. Knowing that fully one-third of that effort is useless for law enforcement is frustrating to us as bankers. The CTR form was the original effort for tracking money and identifying possible criminal activity but since then, use of the Suspicious Activity Reporting regime has taken center stage. Despite other, more efficient efforts to detect criminal activity, the CTR format is still in place. For example, law enforcement has access to regular checks with banks through an information sharing mechanism under the USA PATRIOT Act, section 314(a). And finally, despite these new sources of information for law enforcement, the CTR filing threshold of $10,000 which is still being used in 2017 was set in 1970; today, that same amount adjusted for inflation would be more than $64,000 in today's dollars. And so even the threshold for CTR filings is outdated. The question is whether all the time, effort and resources used to file a CTR could be better allocated to identifying and reporting truly suspicious activities.

According to the banking agencies, "Suspicious activity reporting forms the cornerstone of the BSA reporting system." Investigations and SARs can be triggered for a number of reasons, such as alerts due to deviations from expected activity, cash activities, HRRs, negative news, subpoenas, OFAC, or 314a matches, and so forth. In 2016, the Bank filed a total of 29 SARs. A decision to file a SAR is taken very seriously, and is only done after a full investigation that leads to either a conclusive finding, the inability to understand the nature of the activity, or a lack

of cooperation from the customer. A decision of whether or not to close the account is also made anytime a SAR is filed.

What's important to understand is that it takes time, effort and resources to file a SAR – or to determine not to file one when our systems create an alert. Treasury and FinCEN recognized that it takes time to put together all this information to provide the detail that's required. As a result, the filing deadline for reporting suspicious activity is 30 days after a determination has been made that suspicious activity did occur. When no suspect can be identified, that timeline increases to 60 days. And, where there is ongoing activity that was reported in a previous SAR, the bank has up to 120 days to file a follow-up SAR. The industry definitely needs that amount of time to conduct the investigation and research to submit a package for law enforcement. However, it may be that the system developed nearly 25 years ago is inappropriate in today's world.

When the United States was evaluated by the Financial Action Task Force (FATF) last year, it pointed out that the time and thresholds for filing SARs were inappropriate and should be reconsidered. A bank can determine that an activity is inappropriate or inconsistent with a customer's usual pattern of activities, but law enforcement is far better equipped to conduct the analysis and research to determine whether an activity reported as suspicious is criminal or terrorism. It would be far more efficient if a bank were allowed to file a short SAR to report a transaction that made no sense or that couldn't be explained. Although this idea needs to be explored more carefully, instead of requiring a bank to do a full-blown investigation and analysis of the activity, requiring time, effort and resources that are outside a bank's activity as a bank, it would be more appropriate to file a brief alert with as much information as available to notify law enforcement that something suspicious has occurred. This would quickly call the suspicious transaction to the attention of law enforcement and then let law enforcement agents do exactly what they are trained and qualified to do. Bankers should not be serving as un-deputized law enforcement agents.

Another element of the current BSA compliance regime was added by the USA PATRIOT Act in 2001. Section 314 is designed to encourage information to be shared from banks to law enforcement, from law enforcement to banks, and from banks to other financial institutions. Unfortunately, only one element of the information sharing mechanism Congress

anticipated is operating as intended, and that's the request from law enforcement for possible matches of a named individual and a bank customer. The Bank receives a 314a list from FinCEN bi-weekly, plus special lists when FinCEN feels it is appropriate. This list includes people and entities of interest to FinCEN in relation to an investigation involving money laundering or terrorist financing. The Bank has to check their customer and wire transaction database against this list, and inform FinCEN of any matches. The Bank received 26 bi-weekly lists and 32 special lists in 2016, and did not have a single positive match.

The feedback from law enforcement, which has been explored, has never really attained the level of usefulness that it could. At one time, FinCEN published a regular *SAR Activity Review* that identified ways that law enforcement made use of BSA data in investigations and prosecutions, but even that minimal feedback has been discontinued. Periodically, FinCEN does offer guidance in the form of advisories that identify possible red flags which indicate suspicious activity in areas such as elder financial abuse, human trafficking or other criminal enterprises. However, there is far more potential for communication from law enforcement that would help banks focus efforts and resources in ways that would be more useful to law enforcement. The partnership between law enforcement and the private sector needs to be a two-way street to succeed.

Similarly, there is a provision in that same section that encourages banks to share information with each other, but the restrictions and red tape surrounding its use make it impractical. For more than 15 years, the industry has suggested ways to encourage information sharing about possible criminal activity between banks, such as creating a directory of contacts at other financial institutions. Sadly, these have never been fully explored.

Apart from the information sharing process, there is another BSA requirement that banks must follow which has affected foreign correspondent relationships. From time-to-time, the Bank receives a notice of any foreign jurisdiction, foreign financial institution or financial entity that has been added to or removed from another list called Special Measures under 311. These are entities or jurisdictions that have been identified as not compliant with FinCEN BSA/AML guidelines and which are therefore of primary money laundering concern. The bank is required to do a historical look- back and investigate any transactions to or from any entity or foreign jurisdiction on this list. As the requirements to meet expectations have increased in recent years,

it has had a noticeable impact on foreign correspondent relationships and more and more banks have been decreasing the number of foreign correspondent accounts they maintain, in some instances simply because the costs associated with maintaining and monitoring these accounts have steadily increased. As a result, it can be increasingly difficult to wire funds internationally.

We all recognize the need and importance to stop criminals and terrorists from abusing the United States financial system. The point, though, is that the current compliance regime is out of balance. It needs to be updated and brought into the twenty-first century.

In theory, a bank's approach to BSA/AML compliance is based on risk and the unique risk profile of the bank. That overall risk profile takes into account the bank's customer base, the products and services it offers, its market area, and its strategic plan. There is a lot of agreement that regulations should be applied based on risk, but it seems that is getting increasingly lost in the application of BSA/AML expectations. Community banks are less complex and therefore less risky and should be regulated as such.

We recognize that certain elements of a BSA/AML program do not vary from bank-to-bank. For example, CTRs, structuring, and monetary instrument rules are the same for all banks and that makes sense. If a $10,000 cash transaction is potential money laundering at a $2 trillion bank, it should be considered money laundering at a $200 million bank. However, the disparities arise when it comes to risk ratings as they are applied to an individual bank and its customers. As applied by examiners, something that is considered highly risky in a small institution would be irrelevant for a larger bank. For example, if a $200 million bank is monitoring the 10% of their customers that are deemed to be that bank's highest risk customers, those same customers would not even be on the radar of a $2 trillion bank that is monitoring its 10% highest risk customers. Their 10% highest risk customers are much larger than our 10% highest risk customers. This is frustrating community banks because we are chasing $5,000 transactions and large banks are chasing $500,000 transactions. We have customers complain all the time that small banks are asking questions that larger banks never ask. The problem is that the application of the risk assessment process needs to focus on the actual risk and not graded on some arbitrary bell-curve. We need to focus on real risks, not arbitrary risks depending on where someone opens an account.

Conclusion

No banker would ever suggest that fighting money laundering and terrorist financing are not important or that we don't need regulation. We are only asking that the regulation be practical and sensible. Gilbert and Sullivan once said, "Let the punishment fit the crime." In the BSA context, we need to apply resources wisely and efficiently to combat the crime.

Dodd Frank has caused harm to communities and customers because the rules are not applied based on risk. The USA Patriot Act has also put a big burden on banks; however, it is difficult for banks to even know what should be changed. Banks produce a lot of information for the regulators, but seldom get any feedback about how the information is used, what is effective or not effective, and who is arrested and or convicted. The users of the information should be the ones to assess the value of the information provided, and suggest changes that make sense. BSA is a little like looking for a needle in a haystack. If we can decrease the size of the haystack by doing less 'low-value' activities, and focus our resources on the things that produce the more meaningful results, we will be more effective at finding the bad guys; and at a lower cost. We urge this committee to help reduce the size of the BSA haystack by working with the banking industry and the regulators to address our concerns and to update the Bank Secrecy Act to relieve unnecessary burden from financial institutions and to make the process efficient, effective and up-to-date.

GLOBAL FINANCIAL INTEGRITY

Testimony of Heather A. Lowe
Legal Counsel and Director of Government Affairs, Global Financial Integrity
before the
House Financial Services Subcommittee on Financial Institutions and Consumer Credit
June 28, 2017
on
Examining the BSA/AML Regulatory Compliance Regime

Thank you for the opportunity to testify before you today on the subject of Examining the BSA/AML Regulatory Compliance Regime. I hope that my contributions to today's hearing will help you take measured and informed decisions that are in the public's interest with respect to the U.S.'s anti-money laundering (AML) regime as set forth in the Bank Secrecy Act (BSA).

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

The topic of this hearing is BSA compliance challenges facing financial institutions, including compliance trends, the effectiveness of the suspicious activity report (SAR)/currency transaction report (CTR) reporting regime, and how the compliance regimes might be improved.

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

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

1. Money laundering and the technology that can help us combat it are both evolving and, in light of this, it is appropriate to consider whether changes to our regulatory structure should be made. Equally, however, it is critical that Congress consider and carefully weigh the potential benefits against potential negative ramifications before making decisions in this area. Regulation and enforcement are primarily dissuasive measures because they carry potential liability, and we should be very careful when we look to decrease those dissuasive measures.

1100 17th Street, NW, Suite 505 | Washington, DC | 20036 | USA
Tel. +1 (202) 293-0740 | Fax. +1 (202) 293-1720 | www.gfintegrity.org

2. AML compliance and reporting is undertaken by a wide range of entities and persons, going far beyond the banking sector. Any proposed changes should consider the implications for all of these types of entities and persons.

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

4. Congress should request from the various regulators data regarding formal and informal enforcement actions pertaining to AML/BSA violations and deficiencies so that they are able to independently asses the appropriateness of the enforcement regime currently in place.

5. Both small banks and large banks have been the subject of major money laundering cases.

6. Enforcement against money laundering is primarily through identification of regulatory infractions as opposed to through criminal charges of actually laundering money. This may be because it is much easier to find evidence of regulatory infractions, the burden of proof is lower, the cost of doing so is far less than pursuing a criminal money laundering charge, and the dissuasive effect is just as great. However, when one looks at the cases where enforcement was merely through identification of deficiencies of AML systems and filing requirements, the hallmarks of serious criminal money laundering are there in the cases. As a result, decreasing the ability to enforce using the regulatory approach may have serious, negative repercussions on compliance and, ultimately, criminal access to the U.S. banking system.

7. Suspicious Activity Reports are meant to be just that, reports of "suspicious" activity. Requiring bank employees to determine if activity is in fact illegal before filing a SAR would be counterproductive for a number of reasons, including increasing the burden on bankers who would consequently have to make a new, legal determination.

8. The Clearing House recommends greater information sharing among banks and with the government in a number of ways. While we generally support greater sharing of information in the AML area, it must be done with appropriate privacy safeguards. Where it may result in a person being denied banking services at all, there must be a system for redress for people to be able to restore that access if they can demonstrate that they are involved in legitimate activity.

9. It is critical that information about the natural person(s) who own or control companies (the beneficial owners) is finally collected by either the state or federal government and is made available to law enforcement and to financial institutions. Companies with unknown or hidden ownership are the number one problem in the AML world and the U.S. cannot continue to allow our failure to act to put the U.S. and global financial system at risk.

10. I would strongly caution against transferring responsibility for setting AML priorities for individual banks from those banks to FinCEN. Banks are best placed to understand their business and their systems and the money laundering risks inherent therein, and create the systems that work best in their business models to combat money laundering. FinCEN and/or other regulators should review those assessments but cannot be responsible for carrying them out.

11. Transferring raw baking data from banks to FinCEN to analyze (with appropriate privacy safeguards) is not a bad idea. However, not absolving banks of the responsibility to carry out their own analysis as well, which they have the ability to review within the context of the additional client information that they have, is essential because they are the gatekeepers to the financial system. The federal government cannot do this alone.

12. Money laundering and sanctions violation cases over the past few years relate to willful, knowing, and egregious violations of U.S. laws and regulations that have resulted in U.S. and foreign banks granting access to hundreds of millions of dollars in funds supporting genocide and funds supporting major, violent South American drug cartels into our system, to name a few examples. The fines that have resulted from these cases have been seen by the banking industry as heavy and so banks have begun to take AML regulations that have been in place for many years more seriously as the possibility and repercussions of enforcement have increased. I would therefore remind Members of Congress that the regulatory "burden" has not actually been increasing, the threat of being found out is what has actually increased.

Preface: Who Has AML Compliance Responsibilities?

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

---

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

There are also a few persons that ought to have U.S. AML obligations but currently do not. Although banks serve as an immediate gateway into the U.S. financial system and must therefore bear significant responsibility for preventing criminals and other wrongdoers from finding safe haven here, they shouldn't bear that responsibility alone. Other actors that handle large sums of money, such as persons involved in real estate transactions, escrow agents, investment advisors, lawyers, corporate service providers, and accountants must also take responsibility for knowing with whom they are doing business and guard against their services being used to launder dirty money. Excluding these non-bank sectors renders the U.S. financial system vulnerable to serious, ongoing money laundering threats as shown by multiple media reports about how, for example, anonymous ownership of high-value real estate facilitates money laundering[2], a 60 Minutes segment showing how lawyers facilitate money laundering by corrupt foreign government officials[3], and of course the Panama Papers which disclosed how corporate formation agents and lawyers help wrongdoers hide and launder criminal proceeds.

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

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

I. Trends in Compliance

A. Understanding Regulatory Enforcement Data

As you know, the money laundering realm is governed by statutes which both criminalize the act of laundering money[4] and impose civil and criminal penalties for the failure of a financial institution to have an effective AML program.[5] Under federal law, the type, nature, and scope of a financial institution's AML systems and controls depend upon the institution's risk profile, which differs significantly for banks that, for example, serve a local, rural community versus a global institution that operates in high-risk foreign environments. A financial institution's risk profile depends upon its

---

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

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

[4] 18 U.S.C. §§1956-1957.

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

assessment of the types of risks it faces, which are a function of where it operates, what products and services it offers, and what clients it takes on, among other variables.

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

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

- One of our primary observations was that, apart from the rather small number of publicly available deferred prosecution agreements (DPAs) and non-prosecution agreements (NPAs) that financial institutions have entered into with respect to AML-related activity, it is extremely difficult to determine the number and nature of the formal and informal enforcement actions taken by regulators in response to BSA/AML deficiencies.

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

---

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

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

The bottom line is that it is unclear how much policymakers really know about enforcement related to BSA/AML. The regulatory agencies can take both formal and informal enforcement actions against FIs. While formal enforcement actions are typically public, informal actions may result in a non-public memorandum of understanding (MOU), which requires a bank to take remedial actions to resolve AML deficiencies.

The amount of information available from each agency about their informal enforcement action varies. When we examined annual reports for the regulators as part of our research in 2015, the FDIC was the most transparent agency with respect to statistical reporting, reporting both formal and informal actions and further disaggregating these figures for BSA/AML actions specifically.[8] The U.S. Federal Reserve Board[9] and the U.S. Office of the Comptroller of the Currency[10], report some information about the number of MOUs undertaken, but the nature of the conduct giving rise to the agreements was not available. The National Credit Union Administration and FinCEN did not report any comprehensive figures on their enforcement actions.

The nonpublic nature of most informal enforcement actions plus the lack of useful statistical data about them leaves policymakers in the dark about the number, nature, and impact of current informal AML enforcement actions, a problem that could be remedied in part if this Committee were to request and analyze the related documents.

Another problem is that, while formal enforcement actions were publicly available, the summary information that was searchable and sortable did not include any reference to the type of infraction that gave rise to the action (AML, sanctions, mortgage related, consumer lending, etc.), nor did it reference the laws or regulations that were violated. We constructed a database of public agency enforcement data that spanned from 2001 to early March 2017 and were able to locate approximately 7400 enforcement records. Without being able to sort these actions into infraction categories it is not practicable to conduct a thorough analysis of the BSA/AML violations that may be found in these records. The only alternative is to open and review each of these records to determine the nature of the enforcement action. The exception is the actions by FinCEN, which must all be AML/BSA related, as discussed below.

A final, counter-intuitive problem is that a formal enforcement action does not always indicate misconduct, and where it does address misconduct, the misconduct exists on a spectrum. Depending on

---

[8] *See e.g.*, FDIC, 2014 Annual Report, at 25, Mar. 2015 (reporting 41 consent orders and 180 MOUs, of which 20 consent orders and 23 MOUs addressed at least some BSA/AML violations), https://www.fdic.gov/about/strategic/report/2014annualreport/2014AR_Final.pdf.

[9] *See e.g.*, Board of Governors of the Federal Board System, 100th Annual Report: 2013, at 51, May 2014 (reporting 50 formal enforcement actions and 161 informal enforcement actions), *available at* http://www.federalreserve.gov/publications/annual-report/files/2013-annual-report.pdf.

[10] *See e.g.*, OCC, Annual Report Fiscal Year 2013, at 39 (reporting 97 formal enforcement actions and 46 informal enforcement actions, including 7 MOUs), *available at* http://www.occ.gov/publications/publications-by-type/annual-reports/2013-OCC-Annual-Report-Final.pdf.

the agency, these enforcement actions can range from something routine and not indicative of actual wrongdoing, for example the FDIC terminating deposit insurance for a banking unit whose deposits were transferred to another bank within the group,[11] to the exceptional, like the willful and systematic violation of sanctions laws. As a result, one cannot even equate the number of enforcement actions against FIs with actual wrongdoing.

An additional feature of this multiple-regulator system is that banks within the same banking group may be subject to supervision by different regulators, so that frequently there will be more than one enforcement action against the same banking group for the same violations (perhaps one against the bank actually engaged in the misconduct and another against its holding company or parent). Therefore, the presence of numerous records related to one bank does not necessarily indicate a higher degree of misconduct, as each record shown on agency websites is not necessarily a separate case. In addition, there may be more than one record (or document) issued by the same agency on the very same matter.

In other words, out of 7,400 actions there may be only 5,500 different cases, 1,000 of those notices may have been simply notice of a routine change in supervision, and perhaps 2,500 of the remaining 4,500 actions were AML related. 2,500 AML related enforcement actions over 14 years is about 180 action notices per year. These are simply guestimates and the numbers may be substantially different, but this should be part of Congress' analysis.

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

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

FinCEN Enforcement Actions

The first body of materials we reviewed were the FinCEN enforcement actions. Unlike bank regulatory agencies that tend to be more concerned with ensuring the general health and stability of our financial system, FinCEN's specific mission is to "safeguard the financial system from illicit use and combat money

---

[11] *See e.g.*, FDIC, *In the Matter of Wells Fargo Bank Michigan, National Association*, Order of Approval of Termination of Insurance, No. FDIC-04-185q, Sept. 4, 2004 ("Wells Fargo Bank, National Association, San Francisco, California ("Wells Fargo"), has provided to the FDIC on August 16, 2004, satisfactory evidence that it has assumed the liabilities for deposits of Wells Fargo Bank Michigan, National Association, Marquette, Michigan ("Insured Institution"), as of February 20, 2004, as required by section 307.1 of the FDIC's Rules and Regulations, 12 C.F.R. §307.1, and that Wells Fargo has notified the Insured Institution's depositors of its assumption of their deposits..."), *available at* https://www5.fdic.gov/EDOBlob/Mediator.aspx?UniqueID=f7299e5f-a4be-4c57-8a09-813447369778.

laundering and promote national security."[12] As a result, FinCEN's enforcement actions relate solely to issues involving money laundering and illicit finance.

Given the available data, GFI analyzed 61 separate actions[13] against 52 different banks.[14] There were 26 American banks subject to FinCEN actions, and 26 foreign banks and U.S. branches and offices of foreign banks that were subject to FinCEN actions. Each case involved multiple failings over a period of years, making categorization of the violations challenging.

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

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

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

> For example, from April 1999 through August 2002, one customer who operated a sportswear business purchased approximately $674,390 in cashier's checks, all individually purchased below the $3,000 Bank Secrecy Act recordkeeping threshold for monetary instrument transactions. Concurrently, from April 1999 through August 2002, the same customer engaged

---

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

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

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

> in a pattern of structured transactions involving over $6,199,616 in cash deposits in amounts under $10,000 per deposit. Ultimately, in December 2002, the Bank discovered that this customer had conducted nearly $10 million in cash transactions between April 1999 and November 2002.
>
> Another Foster customer routinely made cash deposits in the amounts of $9,900 up to four times daily. The Bank retained no documentation in its file to support a legitimate business reason for these deposits.
>
> Other customers engaged in large aggregate cash transactions, totaling an average of $300,000 to $600,000 per month, at least some of which appeared to be designed to avoid currency transaction reporting. Foster did not have documentation supporting the legitimacy of the customers' banking activities and failed to file timely suspicious activity reports for these customers.[15]

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

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

For example, North Dade Community Development Federal Credit Union was a non-profit community development bank based in North Dade County, Florida, with $4.1 million in assets. As a community development bank, its clients were supposed to be limited to people who live, work or worship in the

---

[15] FinCEN, Assessment of Civil Money Penalty against The Foster Bank, Case No. 2006-8, at 5, http://www.fincen.gov/news_room/ea/files/foster.pdf.

North Dade County area. North Dade had only one branch and only five employees. Despite its small, local focus, North Dade was servicing multiple money service businesses that were located outside of its geographic field of membership and that were engaging in high-risk activities. For example, records showed "(1) deposits in excess of $14 million in U.S. cash that was physically imported into the United States on behalf of nearly 40 Mexican currency exchangers, and (2) hundreds of millions of dollars in wire transfers to foreign bank accounts of MSBs located in Mexico and Israel."[16] It is difficult to believe that the bank's five staff members were unaware of the likelihood that the bank was being used to launder money via their MSB clients, and it is wholly possible that the bank was either illegally established for that purpose or was overtaken by criminal clientele.

DPAs and NPAs

The second body of material we reviewed with respect to BSA/AML violations were DPAs and NPAs, which we drew from the University of Virginia School of Law's *Federal Organizational Prosecution Agreements* collection.[17] As you know, NPAs and DPAs represent a step beyond agency enforcement actions. They represent settlements of criminal and civil cases brought by the government against corporations where the corporation generally admits to certain facts, agrees to take certain remedial measures, and often pays a fine in exchange for the government deferring or discharging the prosecution. In the case of NPAs, the matter is settled once the government has signed the agreement. In the case of DPAs, the government has the option of renewing the prosecution if the company does not implement the required remedial measures or continues to otherwise act unlawfully.

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

Several of the money laundering cases involved funds being moved from developing or middle income countries into the U.S. via money service businesses or correspondent banking activities. The majority of the countries involved were South or Central American (mainly focusing on the Black Market Peso Exchange) or Middle Eastern. One case involved a bank in Nigeria and one case involved Russian banks.

---

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

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

The countries that arise in these cases are not surprising in light of the American political priorities of fighting drug crime and terrorist financing.

C. Conclusion of Analysis and Recommendation

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

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

II. Suspicious Activity Reports (SARs)

The Subcommittee also asked GFI to discuss issues related to Suspicious Activity Reports (SARs). It is important for the Subcommittee to understand that SARs were intended to be just that, reports of *suspicion* of criminal activity. They are not called *illegal activity reports,* because FI employees are not required to determine if the activity they are seeing is actually illegal. Instead, FI employees are supposed to file reports where they see something out of the ordinary and simply have a suspicion that there is a problem. Requiring bank employees to go further and make a determination that an activity is actually illegal would be an unrealistic and unwarranted expectation. There is no "bright line" test for when a SAR should be filed because that is contrary to the intended nature of a SAR.

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

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

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

It seems that there may need to be a better balancing of expectations in this area. It is possible that there may be new technological approaches that can also be brought to bear and the government should find ways of encouraging new approaches, including through the creation of a technological "sandbox", as has been proposed by The Clearing House and has been implemented in the UK. The UK structure appears to have some specific safeguards to protect consumers, however, which they consider to be an integral part of their system. I have not had an in-depth look at the UK program, regulators presented it at a recent FATF industry consultation meeting I attended, but they stressed the importance of ensuring that consumers were protected at all times as innovative approaches were being tested, and the U.S. should do the same.

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

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

However, knowledge of the beneficial owner(s) of a company holding an account is a critical question in KYC. Therefore, one Clearing House proposal that GFI wholeheartedly supports is its proposal that information about the beneficial owners of U.S. companies—the actual individuals who own or control those companies—should be collected at the time that companies are incorporated in the U.S. and that

this information should be made available to law enforcement and financial institutions. This is an issue that has been gaining visibility and urgency on a global level. This is because anonymous companies, or companies with hidden owners, are the most frequently used vehicle for money laundering. That's why identifying who owns or controls a company is a fundamental step necessary to combat the problem.

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

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

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

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

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

The suggestion that FinCEN be given access to bulk data transfers from FIs to enable it to analyze AML trends and patterns across institutions is another potentially useful idea. But questions about the

effectiveness and cost of this proposal include whether FinCEN currently has the technological capability and personnel needed to perform that type of data analysis or whether it would need to be built, which could be a significant expense. Privacy issues are another concern. In addition, charging FinCEN with industry-wide data collection and analysis should not be seen as a way for banks to absolve themselves of their AML obligations. The banks would retain their function as the primary gateway into the U.S. financial system, so the first level of responsibility to safeguard the system against money laundering abuses must remain with the individual banks who open their accounts to individuals and entities around the world.

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

Overall, it is critical that the Subcommittee understand that changes of the magnitude suggested by The Clearing House would require a huge appropriation from the federal budget to pay for, among other things, a very large staff increase and procedural and technological improvements at FinCEN. In addition, many new regulations would have to be drafted to give effect to these changes. The result would be a much bigger government agency and a bigger FinCEN impact on AML activities. Careful analysis is needed to determine whether the benefits of each of these changes would outweigh the costs.

Finally, I am in favor of exploring the ways in which today's (and tomorrow's) technology can be used to innovate in the AML compliance sphere and believe that the government should be supporting such innovation (usually referred to as "FinTech"). Northern Europe seems to be leading in this space, and it would be helpful to create a better environment for such innovation in the U.S.

V. Conclusion

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

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

misconduct, our survey reveals that attitudes toward corruption within the industry have not changed for the better."[18]

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

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

---

[18] *The Street, the Bull and the Crisis* is available at https://www.secwhistleblowerадvocate.com/pdf/Labaton-2015-Survey-report_12.pdf.

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

(2) "financial institution" means—

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

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

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

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

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

AMERICAN GAMING ASSOCIATION

799 9th Street NW, Suite 700
Washington, D.C. 20001
MAIN LINE 202.552.2675
FAX 202.552.2676
www.americangaming.org

June 28, 2017

The Honorable Blaine Luetkemeyer
Chairman
House Financial Services Subcommittee on
Financial Institutions and Consumer Credit
Rayburn House Office Building, 2129
Washington, D.C. 20515

The Honorable Wm. Lacy Clay
Ranking Member
House Financial Services Subcommittee on
Financial Institutions and Consumer Credit
Rayburn House Office Building, 2129
Washington, D.C. 20515

Dear Chairman Luetkemeyer and Ranking Member Clay:

Ahead of today's House Financial Services Subcommittee on Financial Institutions and Consumer Credit hearing, "Examining the Bank Secrecy Act/Anti-Money Laundering Regulatory Compliance Regime," I write to express our appreciation for your continued work on our shared goal of protecting the U.S. financial system.

The American Gaming Association (AGA), a national trade association which represents licensed commercial and Tribal casino operators and gaming suppliers supporting 1.7 million U.S. jobs across 40 states, values the exchange of information and would welcome the opportunity to engage with the subcommittee as we all work towards maintaining the most robust and effective anti-money laundering (AML) programs.

Currently, the AGA holds a close working relationship with the Treasury's Financial Crimes Enforcement Network ("FinCEN") -- serving on the Bank Secrecy Act Advisory Group (BSAAG) and strongly supporting FinCEN's efforts to enhance compliance with the Bank Secrecy Act (BSA). In addition, the gaming industry has created a set of Best Practices for AML Compliance[1] and was recently recognized by the Financial Action Task Force (FATF) for demonstrating "a good understanding of risks and obligations" and "putting in place mitigating measures above the requirements [of the Bank Secrecy Act] and showing an increased focus on raising awareness and improving compliance."[2]

Every day, AGA members are making significant investments to foster a strong culture of compliance within their organizations and ensuring compliance with the BSA and all applicable laws and regulations. Industry-wide, AML compliance continues to take an increasingly prominent role in all corporate structures. For that reason, we thank the subcommittee in advance for your attention to these important matters and look forward to future engagement opportunities.

Sincerely,

Geoff Freeman
President and CEO

cc: The Honorable Jeb Hensarling, Chairman, House Financial Services Committee
The Honorable Maxine Waters, Ranking Member, House Financial Services Committee

[1] American Gaming Association, 'Best Practices for Anti-Money Laundering Compliance' (January 2017), https://www.americangaming.org/sites/default/files/Best%20Practice%202017.pdf.
[2] *Fourth Mutual Evaluation Report on Anti-Money Laundering and Counter-Terrorist Financing Measures, Financial Action Task Force, December 2016*

June 28, 2017

The Honorable Blaine Luetkemeyer
Chairman
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
U.S. House of Representatives
Washington, DC 20515

The Honorable Wm. Lacy Clay
Ranking Member
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
U.S. House of Representatives
Washington, DC 20515

RE: Statement for the Record

Dear Chairman Luetkemeyer and Ranking Member Clay:

The American Land Title Association[1] appreciates the opportunity to submit this statement for the record for this hearing entitled "Examining the BSA/AML Regulatory Compliance Regime."

The purchase and sale of a home should be an exciting time for Americans. Unfortunately, for too many families today, that excitement is dampened because of the loss of their life savings due to sophisticated fraud schemes. The proceeds from these crimes now comprise a major source of money laundered through the US financial system.

Business email compromise or other attempts by criminals to defraud homebuyers and divert their earnest money deposits or other closing funds are on the rise. In May, the FBI reported a 480% increase in reports of these frauds. Overall, these scams have cost American's $5.3 billion.

In a typical scheme, the criminal monitors real estate transaction information. In many instances, they obtain access to unsecured public domain email accounts, including those used by real estate professionals who are trusted by the consumer. This access is obtained either through

[1] The American Land Title Association, founded in 1907, is a national trade association and voice of the real estate settlement services, abstract and title insurance industry. ALTA represents more than 6,200 member companies. ALTA members operate in every county in the United States to search, review and insure land titles to protect home buyers and mortgage lenders who invest in real estate. ALTA members include title insurance companies, title agents, independent abstracters, title searchers and attorneys, ranging from small, one-county operations to large national title insurers.

1828 L Street, N.W. ■ Suite 705 ■ Washington, DC 20036 ■ (202)296-3671 ■ 202-296-3671 ■ 800-787-ALTA
E-mail: service@alta.org ■ Web: www.alta.org ■ Fax: 888-FAX-ALTA ■ Local Fax: (202)223-5843

a common social engineering technique called phishing or by purchasing email login credentials online.

Once the criminals gain access to an email account, they will monitor messages to find someone in the process of buying a home. They then use the stolen information to email fraudulent wire transfer instructions disguised to appear as if they came from a professional to the buyer, seller, real estate agent or title company. These emails look legitimate and often come from nearly identical domains as the supposed sender and use an actual party's logo.

When this occurs, it is not uncommon for the fraud to be discovered weeks later when the buyer shows up to settlement with insufficient funds. This delay in detection also makes it nearly impossible to recover the stolen funds.

These criminals typically use witting and unwitting money mules to move and aggregate funds in the United States before sending it overseas. This puts financial institutions at risk of becoming unwitting participants in the laundering of money.

We believe policy makers should focus on two key areas when trying to prevent these crimes and the use of our financial system by these criminals.

First, we need to increase public awareness of these schemes. In an advisory last year, the Financial Crimes Enforcement Network (FinCEN) stated that due to the irrevocable nature of these transfers, the best first line of defense is to prevent American's from falling victim to these scams.

At ALTA, we educate our members about these schemes and the need to make consumers and real estate agents aware of these risks early in the transaction. We have also developed a set of five tips that people can use to protect against wire fraud:

1. **Call, don't email:** Confirm all wiring instructions by phone before transferring funds. Use the phone number from the title company's website or a business card.
2. **Be suspicious:** It's not common for title companies to change wiring instructions and payment info
3. **Confirm it all:** Ask your bank to confirm not just the account number but also the name on the account before sending a wire.
4. **Verify immediately:** You should call the title company or real estate agent to validate that the funds were received. Detecting that you sent the money to the wrong account within 24 hours gives you the best chance of recovering your money.
5. **Forward, don't reply:** When responding to an email, hit forward instead of reply and then start typing in the person's email address. Criminals use email address that are very

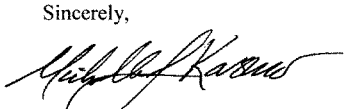
similar to the real one for a company. By typing in email addresses you will make it easier to discover if a fraudster is after you.

Second, a simple change in practices can be the single biggest deterrent to wire fraud. We encourage financial institutions to match not only the account number of the beneficiary but also the payee's name. Oftentimes the fraudulent instructions will say the transfer is to be sent to the title company's trust account but instead it goes to a money mule's personal account. Just matching the account number on the request with an account number at the beneficiary bank will not catch this.

Lastly, policymakers should consider ways to better use both suspicious activity reports and IC3 data to better detect accounts used by these criminals and their mules. We need to provide financial institutions with as much information as possible to uncover potential money laundering. Even if more information does not lead to prosecutions of these criminals it can help banks decide to place holds on the account preventing the criminal or the mule from withdrawing funds while they conduct a more thorough investigation.

ALTA appreciates the opportunity to provide this statement for the record. Should you have any questions about this statement, please do not hesitate to contact Justin Ailes, Vice President of Government Affairs at 202.261.2937.

Sincerely,



Michelle L. Korsmo
Chief Executive Officer

INDEPENDENT COMMUNITY
BANKERS *of* AMERICA®

June 28, 2017

BSA Modernization Can Strengthen Law Enforcement and Ease Compliance

On behalf of the more than 5,800 community banks represented by ICBA, we thank Chairman Luetkemeyer, Ranking Member Clay, and members of the Financial Institutions and Consumer Credit Subcommittee for convening today's hearing on "Examining the BSA/AML Regulatory Compliance Regime." We appreciate you raising the profile of this important issue, and we are pleased to offer this statement for the record.

Community bankers are committed to supporting balanced, effective measures that will prevent terrorists from using the financial system to fund their operations and prevent money launderers from hiding the proceeds of criminal activities. We believe there are opportunities to modernize and reform the Bank Secrecy Act (BSA) so that it produces more useful information for law enforcement while alleviating community banks' compliance burden. Community bankers have consistently cited BSA as one of the most significant sources of compliance burden. Below are our recommendations for BSA modernization.

Update Currency Transaction Report Threshold

As the government combats money laundering and terrorist financing, ICBA strongly recommends an emphasis on quality over quantity for all BSA reporting. In this regard, the currency transaction report (CTR) threshold should be raised from $10,000 to $30,000 with future increases linked to inflation. The current threshold, set in 1970, is significantly outdated and captures far more transactions than originally intended. A higher threshold would produce more targeted, useful information for law enforcement.

Improve Flexibility and Ease of Compliance

ICBA supports FinCEN's efforts to simplify certain BSA forms and encourages the government to continue streamlining other reporting requirements. The federal government should continue working with the banking industry to provide additional guidance—such as best practices, questions and answers, or commentary—that is understandable, workable and easily applied by community banks. ICBA encourages FinCEN to continue its investigation and adaptation of technology to assist banks with their BSA compliance requirements. ICBA also encourages the Office of Foreign Asset Control to streamline and simplify its lists for ease of reference and application by bankers.

To ensure a consistent and balanced effort to combat money laundering and terrorist financing, the federal government should have consistent regulations across all financial services providers including nonbank entities. Additionally, the government should require reporting of only truly suspect transactions—and strive to balance those requirements against the need to respect customer privacy.

Compensation for Anti-Money Laundering and Anti-Terrorist Financing Efforts

As the Financial Crimes Enforcement Network (FinCEN) identifies additional high risk transactions and accounts, it increases banks' requirements in these new areas. For community banks, BSA compliance represents a significant expense in terms of both direct and indirect costs. BSA compliance, whatever the benefit to society at large, is a governmental, law enforcement function. As such, the costs should be borne by the government. ICBA supports the creation of a tax credit to offset the cost of BSA compliance.

Beneficial Ownership

Beneficial ownership information should be collected and verified at the time a legal entity is formed. Collecting and verifying the identity of all natural person owners of each entity by either the Internal Revenue Service or other appropriate federal agency and/or state in which the entity is formed would provide uniformity and consistency across the United States. Making the formation of an entity contingent on receiving beneficial owner information would create a strong incentive for equity owners and investors to provide such information. Additionally, periodic renewal of an entity's state registration would provide an efficient and effective vehicle for updating beneficial ownership information. If such information is housed at a government entity, community banks should have access to it.

Closing

Thank you again for convening today's hearing. ICBA looks forward to working with this Committee to modernize the Bank Secrecy Act in a way that will strengthen critical law enforcement while rationalizing community bank compliance with this important law.