PROMOTING CORPORATE TRANSPARENCY: EXAMINING LEGISLATIVE PROPOSALS TO DETECT AND DETER FINANCIAL CRIME

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL DEVELOPMENT AND MONETARY POLICY

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MARCH 13, 2019

Printed for the use of the Committee on Financial Services

Serial No. 116–9

U.S. GOVERNMENT PUBLISHING OFFICE
36–559 PDF WASHINGTON : 2019

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
WM. LACY CLAY, Missouri
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
BILL FOSTER, Illinois
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
RASHIDA TLAIB, Michigan
KATIE PORTER, California
CINDY AXNE, Iowa
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
BEN MCADAMS, Utah
ALEXANDRIA OCASIO-CORTEZ, New York
JENNIFER WEXTON, Virginia
STEPHEN F. LYNCH, Massachusetts
TULSI GABBARD, Hawaii
ALMA ADAMS, North Carolina
MADELEINE DEAN, Pennsylvania
JESÚS "CHUY" GARCIA, Illinois
SYLVIA GARCIA, Texas
DEAN PHILLIPS, Minnesota

PATRICK MCHENRY, North Carolina, *Ranking Member*
PETER T. KING, New York
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
ANN WAGNER, Missouri
ANDY BARR, Kentucky
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
TREY HOLLINGSWORTH, Indiana
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
BRYAN STEIL, Wisconsin
LANCE GOODEN, Texas
DENVER RIGGLEMAN, Virginia

CHARLA OUERTATANI, *Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL DEVELOPMENT AND MONETARY POLICY

EMANUEL CLEAVER, Missouri, *Chairman*

ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
DENNY HECK, Washington
BRAD SHERMAN, California
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
MICHAEL SAN NICOLAS, Guam
BEN MCADAMS, Utah
JENNIFER WEXTON, Virginia
STEPHEN F. LYNCH, Massachusetts
TULSI GABBARD, Hawaii
JESÚS "CHUY" GARCIA, Illinois

STEVE STIVERS, Ohio, *Ranking Member*
PETER T. KING, New York
FRANK D. LUCAS, Oklahoma
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
DENVER RIGGLEMAN, Virginia, *Vice Ranking Member*

CONTENTS

PROMOTING CORPORATE TRANSPARENCY: EXAMINING LEGISLATIVE PROPOSALS TO DETECT AND DETER FINANCIAL CRIME

Wednesday, March 13, 2019

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY,
INTERNATIONAL DEVELOPMENT
AND MONETARY POLICY,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:09 p.m., in room 2128, Rayburn House Office Building, Hon. Emanuel Cleaver [chairman of the subcommittee] presiding.

Members present: Representatives Cleaver, Perlmutter, Heck, Sherman, Vargas, Gottheimer, Wexton, Lynch, Garcia; Stivers, Williams, Hill, Gonzalez, Rose, and Riggleman.

Ex officio present: Representatives Waters and McHenry.

Also present: Representatives Maloney and Luetkemeyer.

Chairman CLEAVER. The Subcommittee on National Security, International Development and Monetary Policy will come to order.

Without objection, the Chair is authorized to declare a recess of the subcommittee at any time. Also, without objection, members of the full Financial Services Committee who are not members of this subcommittee are authorized to participate in today's hearing.

Today's hearing is entitled, "Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crime."

I now recognize myself for 3 minutes to give an opening statement.

I would like to thank Chairwoman Waters for creating this new Subcommittee on National Security, International Development and Monetary Policy. These are some of the most pressing issues facing our country and the world, and I am excited for the opportunity this Congress presents to confront them head on. Many of the matters that are likely to come before this subcommittee have historically enjoyed bipartisan support. They go to the very heart of our most profound responsibilities as Members of Congress: preserving America's national security, and the United States' global position as an international leader in free and fair markets.

I am convinced that there is no better issue to start our subcommittee's work than a discussion of policies to detect and deter these financial crimes.

Since the last major anti-money laundering reforms in 2001, the national security threats that face our country have evolved profoundly. Cyber and technological attacks have risen to the very top of our most recent worldwide threat assessment as a paramount national security risk. Underground online trafficking now allows for simplified avenues to transport illicit materials across the nation and around the globe.

While the bill that we are dealing with today will close a number of loopholes that have allowed for financial crimes to be committed, it will also pull us into the 21st Century by positioning the U.S. to face tomorrow's challenges. An innovation council will be created from this bill, represented by directors from each innovation lab, who will coordinate on active Bank Secrecy Act compliance. It is imperative that we modernize our efforts to combat financial crimes because our adversaries will continue to modernize theirs. And this proposal is an important step, even though it is our first step.

With that, I will also be sending a letter to the Treasury's Financial Crimes Enforcement Network (FinCEN) this week to discuss how Fintech is being deployed to confront illicit finance. I am also happy to see that the committee will be considering Congresswoman Maloney's bill, which I know she and her team have worked very long and hard on. The straightforward bill provides needed transparency by requiring companies in the United States to disclose the financial beneficiary in order to prevent criminals and wrongdoers from exploiting their status as a company for criminal gain.

I am also pleased that we will be considering Congressman Lynch's Kleptocracy Asset Recovery Rewards Act. This bill establishes in the Treasury Department, a Kleptocracy Asset Recovery Rewards Program, which may provide rewards to individuals providing information leading to the restraining, seizure, forfeiture, and reparations of stolen assets linked to foreign government corruption.

These are all very important proposals, and I am eager to hear from our witnesses on their perspectives and insight.

I will now recognize the ranking member of the subcommittee, Mr. Stivers, for such time as he may consume.

Mr. STIVERS. Thank you, Mr. Chairman. It is an honor to serve with you as the lead Republican on the National Security, International Development and Monetary Policy Subcommittee. And I want to commend you for your work on anti-money laundering. The draft we have today, I think, is important, and an important conversation to have.

Some of the provisions that you have included originate from bipartisan bills from the last Congress, and I appreciate that bipartisan approach. I also agree that we must modernize our approach to anti-money laundering and the Bank Secrecy Act.

I also want to applaud Congresswoman Maloney for her dedication over the years in combating the use of shell companies by criminals, terrorists, and rogue nations, and commend my colleagues, Steve Lynch and Ted Budd for their work on the Kleptocracy Asset Recovery Rewards Act.

We are fortunate to serve on this subcommittee, because the jurisdiction that we cover is frequently very bipartisan, which I think will make our work easier. But there are a lot of hard things that we have to do. And I know that everyone on this subcommittee is dedicated to preventing criminals and terrorists from accessing our financial network and financial system. While we may disagree about the best way to accomplish these things, we all want to keep money out of the hands of those who would cause us harm.

The two benchmarks I will use when I evaluate bills before today's committee are: number one, will the legislation be effective at accomplishing its stated goals; and number two, will these bills be the most efficient means to accomplish their objective? Or do some of the provisions impose unnecessary burdens that can be improved?

As we try to answer those questions, we should also be careful to ensure our actions don't result in unintended consequences. The provision of the anti-money laundering draft speaks to this point. The provision which I support directs Treasury to conduct a study on de-risking. This is a practice of financial institutions closing accounts they deem high risk. Some of these accounts are genuinely suspicious and are rightfully terminated. Others belong to people who arguably are at the greatest need for access to our financial system such as legitimate international charities responding to humanitarian crises.

Here, timely financial access to payment for medical equipment or supplies can have lifesaving consequences. So I think it is important that we look at this practice. This de-risking is undeniably a result of our well-intended but sometimes current laws and policies. As we examine our bills under consideration today, I want to be mindful to avoid these mistakes in the future.

Thank you to the witnesses for being here today. I am looking forward to hearing your testimony today. And I want to thank the chairman for having this hearing.

And I would like to yield 1 minute to the vice ranking member of the subcommittee, Mr. Riggleman.

Mr. RIGGLEMAN. Thank you, Chairman Cleaver, for calling this important hearing today.

BSA/AML laws and regulations serve as the legal framework to help our financial institutions safeguard the financial system. From its origins in the 1970 Bank Secrecy Act, BSA/AML has attempted to adapt to continued threats of financial crime. I support FinCEN in its mission to enforce BSA/AML, because I believe that preventing illicit finance on all fronts is essential to national security. I personally witnessed the benefits of cutting the head off the snake.

However, I am very worried that the current framework is, at times, both onerous and outdated and, therefore, unable to keep pace with emerging threats and evolved criminals that have adapted to our security posture. Criminals are constantly adapting their tactics, techniques, and procedures (TTPs) to bypass our defenses.

As Congress considers reforms to the law, it is critical that we provide the private sector with a flexible, suitable, and effective regulatory regime that actually assists banks and credit unions in preventing illicit finance. We should strive to equip regulators and

financial institutions with clear directives and critical information, and create strong partnerships with law enforcement. Collaborative data sharing between law enforcement and financial institutions is essential to supporting FinCEN's mission.

I very much look forward to hearing the testimony from our witnesses. And thank you for being here today.

I yield back.

Chairman CLEAVER. Thank you.

Chairman CLEAVER. Thank you, Mr. Stivers.

The Chair now recognizes the gentlelady from California, the Chair of the full Financial Services Committee, Ms. Waters, for such time as she may consume.

Chairwoman WATERS. Thank you very much, Mr. Chairman. And congratulations on convening the first hearing of the Subcommittee on National Security, International Development and Monetary Policy. This hearing is on an important and timely topic: promoting corporate transparency and safeguarding our financial system from terrorists, traffickers, corrupt officials, and other criminals.

Our nation's anti-money laundering framework needs an overhaul. In the past few years, we have seen an increase in human and narcotics trafficking through online marketplaces, large-scale cyber attacks from maligned foreign actors, and the proliferation of shell companies being used to hide illicit funds. It is for this reason that the House debated a resolution I introduced that advocates for the closure of money-laundering loopholes. At the same time, we have experienced tremendous technological advances that can both help detect bad actors, and facilitate terrorism and crime.

The need for responsible innovation of new technologies is especially important in this rapidly changing environment. In addition, the Treasury Department and its partners need better access to actionable financial intelligence. And financial institutions large and small must better understand what is required of them in the shifting landscape.

It is also painfully clear that some institutions unrepentantly abuse our financial system and are willfully blind to money laundering occurring within the banks instead of being held criminally accountable. However, these institutions often get away with penalties and fines that amount to a slap on the wrist.

The legislation being discussed today would address these concerns while also improving compliance and innovation, thus strengthening the anti-money laundering framework.

I yield back the balance of my time.

Thank you.

Chairman CLEAVER. Thank you.

Today, we welcome the testimony of our four witnesses. Our first witness is Mr. Jacob Cohen. Mr. Cohen is a subject matter expert, with over 8 years of policy, regulatory, and operational experience working to combat money laundering and terrorist financing domestically and internationally. From 2012 to 2018, Mr. Cohen held various roles in the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, including as policy advisor in the Office of Terrorist Financing and Financial Crimes. He also served for several years as the Director of the Office of Stakeholder Engagement at the Financial Crimes Enforcement Network

(FinCEN). He currently advises financial institutions and emerging Fintech companies regarding Bank Secrecy Act requirements and potential exposure to economic sanctions, money laundering, and terrorist financial risk. Welcome, Mr. Cohen.

Our second witness is Mr. Dennis Lormel. Over the last 15 years, Mr. Lormel has served as the founder and president of DML Associates, where he provides consulting services and training related to terrorist financing, money laundering, fraud, financial crimes, suspicious activity, and due diligence. Prior to that, Mr. Lormel served as a Special Agent at the Federal Bureau of Investigation for 28 years where, in 2000, he became Chief of the FBI's Financial Crimes Program.

Following the terrorist attacks of September 2001, Mr. Lormel established and directed the FBI's comprehensive terrorist financing initiative, which evolved into the formation of the formal section within the counterterrorism division of the FBI known as the Terrorist Financing Operation Section. Welcome, Mr. Lormel.

Our third witness is Mr. Amit Sharma. Mr. Sharma is the founder and CEO of FinClusive, a digital financial services platform for financially underserved and excluded entities that leverages blockchain technology and risk compliance tools to drive financial inclusion, build economic resilience, and protect financial system integrity. Mr. Sharma previously served as Chief of Staff to Deputy Secretary Robert Kimmitt, and as advisor to Treasury's senior team under Secretary Henry Paulson.

Prior to that, he served at the Treasury's Office of Terrorism and Financial Intelligence, where he developed tools to combat transnational threats and financial crime and anti-money laundering counterterrorist financing strategies. Welcome, Mr. Sharma.

Our final witness is Dr. Gary Shiffman. Dr. Shiffman is an expert in the economics of organized violence, and the CEO and president of Giant Oak, Incorporated. His company supports Federal law enforcement and compliance professionals in regulated industries through software that brings the craft of behavioral science together with computer science and subject matter expertise to better understand patterns of illicit human behavior, such as money laundering, human trafficking, drug trafficking, insurgency, and terrorism.

Dr. Shiffman previously served as Chief of Staff at the U.S. Customs and Border Protection. He also teaches at Georgetown University in the School of Foreign Service.

I welcome all four of you.

Mr. Cohen, you are reminded that your oral testimony will be limited to 5 minutes. And without objection, your written statement will be made a part of the record.

You are now recognized for 5 minutes.

STATEMENT OF JACOB COHEN, FORMER DIRECTOR, OFFICE OF STAKEHOLDER ENGAGEMENT, FINANCIAL CRIME ENFORCEMENT NETWORK (FINCEN)

Mr. COHEN. Thank you.

Chairman Cleaver, Ranking Member Stivers, and distinguished members of the Subcommittee on National Security, International

Development and Monetary Policy, I am honored by your invitation to testify before you today.

Today, I want share my views on the importance of providing FinCEN and the Department of the Treasury with the appropriate resources to expand engagement in collaboration with domestic and global stakeholders. I will focus my remarks on FinCEN engagements efforts domestically, but I will also touch upon Treasury engagements with foreign counterparts through its attache and technical assistance program.

The current AML/CFT landscape in the United States and around the world is complex, dynamic, and requires FinCEN and its private sector partners to constantly adapt. The global dominance of the U.S. economy places FinCEN and U.S. financial institutions at the forefront of combating financial crimes.

To continuously adapt to the ever-evolving threats, FinCEN must have the resources to regularly and systematically engage with all its stakeholders. FinCEN plays an often understated, but outsized role in protecting the integrity of our financial system.

FinCEN serves two roles. First, it is a financial intelligence unit, or FIU, for the United States. FinCEN is responsible for the collection, analysis, and dissemination of financial intelligence to law enforcement agencies and other authorities.

Second, FinCEN is the lead AML/CFT regulator for the Federal Government.

To effectively carry out these roles, FinCEN engages and shares information with the private sector through a variety of mechanisms, including Bank Secrecy Act advisory group (BSAAG) meetings, sharing information through advisories with financial institutions, and select speaking engagements. However, these engagement efforts are not sufficient to keep up with the current threats and the increasing cost from industry for more information to better detect and deter financial crimes.

Held twice a year, BSAAG meetings allow FinCEN and other regulators to have frank discussions with a cross-section of industry representatives regarding the operations of the Bank Secrecy Act. However, engagement with a small fraction of financial institutions twice a year is not sufficient to generate the level of collaboration, continuous change, and learning that FinCEN and the private sector need to engage in to stay abreast of emerging threats and identify innovative approaches to continuously update and modernize our BSA/AML regime.

FinCEN also communicates with industry by issuing public and nonpublic advisories to alert industry of specific financial crime threats. These advisories provide actionable information to financial institutions that allows them to enhance their AML monitoring systems and produce more valuable reporting.

Due to limited resources dedicated to engage stakeholders, not to mention limited analytical support, FinCEN publishes advisories infrequently. This is evidenced by the low number of threat-specific advisories issued by FinCEN over the past 3 years. Advisories on human trafficking, trade-based money laundering, and virtual currency were notably missing.

Today, I would like to express my strong support for a few provisions in the discussion draft that I believe will enable FinCEN and

Treasury to continue to meet the challenges facing our financial system.

The scope of FinCEN's responsibilities require ongoing engagement with stakeholders beyond the Beltway. Providing FinCEN with the resources to deploy domestic liaisons in key cities across the country would allow FinCEN to systematically engage with financial institutions, Federal, State and local partners, and other stakeholders. The benefits of such a program would be substantial. Similar benefits include: identifying region-specific illicit finance risks; issuing region- or industry-specific advisories and geographic targeting orders; communicating priorities and guidance more directly, and with greater frequency to stakeholders; staying abreast of opportunities and challenges of BSA/AML-related innovation.

In December 2017, FinCEN launched a FinCEN exchange program to enable greater information sharing between the public and private sectors. Sharing information about specific threats enables financial institutions to more effectively allocate the limited resources, to identify and report illicit financial activity. This important initiative should be supported with dedicated resources for FinCEN to conduct the necessary research and analysis, and to increase collaboration with the private sector.

Treasury attaches play a key role in advancing U.S. sanctions policy, advocating for implementation of financial action tasks for recommendations, and combating financial crime threats. However, limited resources and the small footprint of the attache program forces Treasury to play a zero-sum game, essentially closing programs in countries that might still offer significant value when a new program elsewhere is required.

Treasury, through its Office of Technical Assistance (OTA) supports foreign regulatory law enforcement, FIUs, and judicial authorities. OTA's approach entails strengthening and integrating the work of the entire spectrum of AML/CFT stakeholders, but with a specific focus on FIUs as a lynch pin of an effective AML/CFT regime.

This enables FinCEN to engage in more productive information-sharing relationships with FIU partners around the world.

While these proposals will enhance FinCEN's ability to increase engagement with industry, without the proper resources to support these new requirements, you will be placing additional burdens on an already resource-strained bureau.

In my experience, one of the greatest challenges for FinCEN has been its ability to hire and retain mission-critical staff. FinCEN is at a disadvantage because it competes for the same experts with Federal banking agencies (FBAs), law enforcement, and the intelligence community, which either have higher salaries, special hiring authority, or both.

Allowing the Director of FinCEN to set salaries at the level of the FBA's will position FinCEN to better compete for quality candidates, and I would also urge this committee to consider providing FinCEN special hiring authority to recruit high-quality candidates for mission-critical, hard-to-fill positions. This would go a long way toward ensuring FinCEN is best positioned to achieve its mission, and to adapt to new and emerging threats to our financial system.

Thank you for the opportunity to testify today.

I look forward to your questions.

[The prepared statement of Mr. Cohen can be found on page 36 of the appendix.]

Chairman CLEAVER. Thank you.

Mr. Lormel?

STATEMENT OF DENNIS M. LORMEL, PRESIDENT & CEO, DML ASSOCIATES, LLC

Mr. LORMEL. Thank you, sir. And thank you for inviting me. I appreciate it, and I want to congratulate the committee for the work you are doing. I think it is really important.

In your opening remarks, I agreed with everything you just said. And, Mr. Stivers, the comment you made about the inclusion and about the unintended consequences is really important. And that is one of the things I want to focus on later.

Thank you for accepting my written statement. And I would like to highlight some things around that.

I have been involved in this space—fighting fraud, corruption, money laundering, and terrorist financing—for over 45 years now. And these are very serious problems, as you pointed out.

Mrs. Maloney, I want to congratulate you and thank you for your perseverance in continually bringing up the beneficial ownership issue. I think that is an incredibly important issue. So, thank you for that.

I know firsthand, having been in law enforcement, and the first shell company I ever dealt was in 1975. So that goes back a long way. I want to strongly encourage the committee to pass this legislation, the beneficial ownership legislation. I have been an advocate for this since 2012, and I think it is really important. I think all of the legislation that you are considering is extremely important.

It's interesting that you bring up the kleptocracy issue with—and Mr. Lynch, thank you for that—the beneficial ownership issue, because kleptocracy, if you want case studies, go to every kleptocracy case out there. One MDB right now is one of your most significant cases. And that has shell companies all over it, and it is so difficult to follow those cases, so thank you for that.

Looking at the beneficial ownership legislation, I think the best-case scenario would be if we had the incorporation information captured and reported at the point with the States' Secretaries of State. That is not a realistic opportunity, so I think the opportunity that Mrs. Maloney is advancing by using FinCEN as the conduit and repository for information is our good-case scenario. And it is our best alternative going forward. I think it helps law enforcement. It certainly gives law enforcement a lot of good access, and I am sure we will discuss that later.

I like what is not included in the other bill, which is the thresholds, the reporting thresholds for SARS and CTRs.

In my written statement, I spent a lot of time on the Bank Secrecy Act. Law enforcement is your number one beneficiary of Bank Secrecy and the reporting. And having been an FBI agent, I was the firsthand beneficiary of suspicious activity reports and CTRs. I think anything to diminish the reporting levels would be very detrimental for law enforcement, and I would encourage you, and en-

courage every committee, to really consult with law enforcement on that issue, because it is so important.

In terms of the other things here, I like the theme in your bill about information sharing and building partnerships. Those are critically important. And the innovation. I am not an IT expert. These two gentlemen are. And I certainly defer to them on that. But innovation is critically important. When you can combine partnerships with innovation, that is a win-win situation for us going forward. And I think that is critically important.

I think the information sharing—if you can expand 314, that is one of the biggest things I hear, one of the detriments, is that we didn't have a consistent feedback mechanism to financial institutions. And I was partly responsible when I was running the financial crimes program. I met with the Director of FinCEN on a regular basis, and we beat that to death trying to figure out how do you do it.

Well, that 314(a), how you recommended it here of providing scenarios and kind of working concepts I think is fantastic. I think that is the type of thing, and I think my old organization, TFOS, in the FBI, they have a tremendous working model just where they do that, where they have a working group of financial institutions, and they share that information.

And on that, I am going to run out of time, so I will stop, and I will look forward to questions.

[The prepared statement of Mr. Lormel can be found on page 42 of the appendix.]

Chairman CLEAVER. Thank you, Mr. Lormel.

You are now recognized for 5 minutes, Mr. Sharma.

STATEMENT OF AMIT SHARMA, FOUNDER AND CEO, FINCLUSIVE

Mr. SHARMA. Ranking and distinguished members of the subcommittee, thank you very much for the opportunity to testify before you today.

In particular, I am grateful for the opportunity to discuss several initiatives that this committee and others in Congress broadly are pursuing to modernize our anti-money laundering and counterterrorist financing regime of the United States, and the attendant issues that emanate from the U.S. Bank Secrecy Act amidst an ongoing and evolving financial crimes threat, not only in terms of the evolution of how criminals move money, but also the attendent consequences or, albeit unintended, of de-risking and the issues related to financial exclusion, which I believe are paramount, and certainly related to our broader national security objective.

I am happy to discuss during the Q&A session additional issues associated with this hearing, including corporate transparency, beneficial ownership, and other parts of Titles I, II, and III. But I am going to focus my short remarks on the issues related to strengthening the coordination between public and private agencies, in particular, in recognition of the evolution of technology to advance some of these issues, not only for inclusion, but also to enhance, modernize, and make much more efficient the anti-money laundering and counterterrorist financing regime for banks and nonbanks alike.

To start, I would say that there are several important trends that are very, very important to recognize, as we think about both the evolution of illicit finance threats, and the evolution in financial services themselves.

The first is the recognition that there has been, and continues to be, an exponential increase in financial intermediation taking place outside of traditionally regulated channels. The direct extension of credit and lending by institutions, and individuals to one another, peer-to-peer transactions, web- and mobile-based banking, the increased digitization and tokenization of financial instruments and assets, and these are just some examples.

Under any rubric, we are seeing financial innovation blossom to assist traditional financial market participants and increasingly nontraditional entrants are driving that innovation. And we have to take notice of the same when we think about modernizing and strengthening the broader BSA requirements that impact them.

Secondly, this growth in financial activities outside traditional channels provides a hugely tremendous opportunity to increase access for the globally underserved, the underbanked, the unbanked, and those otherwise financially excluded. Such efforts have understandably given financial regulators pause as nonbank entities and other nontraditional market participates have come in. Technology and social media companies, online and e-commerce retailers, corporate entities with large recurrent user and consumer populations, and others with large and growing affinity groups are increasingly realizing the commercial benefits and the potential of providing financial intermediation within their infrastructure and their networks.

And while some of these provide tremendous opportunities, the attendant issues that have otherwise impacted and really been relegated specifically to traditional financial institutions, must now necessarily apply to that growing nontraditional space.

Finally, since the tragic events of September 2001, and exacerbated by the credit and financial crisis in 2008, there is a growing body of regulation. Financial oversight rules have understandably caused consternation, not only to traditional market players, but increasingly in the nontraditional, nonbank sector.

With an average governance risk and compliance, GRC spend for most major banks of 25 percent or more, many organizations are presented with this unfortunate economic decision of whether or not to do business with certain sectors, with certain constituents, and has led importantly to financial exclusion and exacerbated de-risking.

I think the comment and the joint statement in December 2018 by the financial regulators to talk about innovation and the AML/CFT space is a very, very good start. But I think some practical steps can emphasize taking that forward in a meaningful way with industry.

One, coordination with examiners. Having senior leadership and director level at individual regulators drive finance, technology, and innovation centers with examiners in the field is paramount. Too often, bank and nonbank entities have to navigate this myriad examination space that is largely uncoordinated between the State and Federal level, and doing so with examiners not only helps with

respect to the assessment and application of technology, but with the examination and audit process itself.

State-based coordination is paramount to enhance that coordination, but also to ensure that bank and nonbank applications of this technology are kept in check, and are done so in a way that financial industry participants, when facing exams with and by State and Federal authorities, where sometimes there may be conflict, can do so and reconcile.

In sum, we have to look at some of these financial inclusion tools as part of the national security tool kit and the AML/CFT process versus looking at it as a binary and false choice between inclusion and AML/CFT implementation.

And I think with that in mind, I certainly commend this subcommittee's and other efforts to modernize the system to do the same.

[The prepared statement of Mr. Sharma can be found on page 52 of the appendix.]

Chairman CLEAVER. Thank you.

Mr. Shiffman?

STATEMENT OF GARY M. SHIFFMAN, CEO, GIANT OAK, INC.

Mr. SHIFFMAN. Distinguished members of the subcommittee, thank you for the opportunity to appear before you today to discuss the important topic of countering financial crime.

I am an economist who focuses on technology, behavioral science, and people who do bad things such as money laundering, human trafficking, drug trafficking, terrorism, fraud, and corruption.

I am the CEO of Giant Oak, a software company focusing on making screening easy. I teach courses at Georgetown University on organized violence. And I am also a Navy Gulf War veteran, and I have served in Federal law enforcement.

I have no interest in reforming AML compliance for compliance's sake. I tell you about my background to emphasize this point. I come to the subcommittee today as a technologist to argue that we can and must do better to combat money laundering, trafficking, terrorism, and other illicit acts.

Our current AML regime requires radical reform. We are inefficient. According to the United Nations, the estimated amount of money laundering globally in 1 year is 2 to 5 percent of global GDP. At the same time, spending to combat money laundering and the financing of terrorism exceeds $7 billion in the United States, and $25 billion globally. However, of the approximately 2 million suspicious activity reports generated by today's AML systems for FinCEN, less than 5 percent of those provide value.

In short, it appears we have an AML regime which compels the industry to spend billions of dollars, generates mostly useless data, and counters less than 1 percent of the problem. We must do better.

We can begin by harnessing available technologies and focusing them on supporting our law enforcement and national security professionals.

When I say, "technology," I refer primarily to machine learning, artificial intelligence, and the application of behavioral science to

patterns in data analytics. I define machine learning as the training of computers to identify patterns in data.

If you imagine a spreadsheet with millions of rows and columns, it is not hard to believe that patterns exist somewhere in the data. But because our human eyes and brains cannot find those patterns, none of us will ever again live in a world without machine learning.

By utilizing machine learning, we can teach computers to find and reveal patterns for us. Any future AML regime must include machine learning, and a future BSA/AML regime without machine learning seems unbelievable.

So what can we do? To build the best machine to detect and deter financial crime, one needs good training data. Machines are literal. If you teach a machine to play chess, it will not learn to play checkers. The best machine on the planet for AML will be built by training it on AML data.

If we apply this to financial crimes, the vulnerabilities and opportunities are obvious. Government agencies know which SARs provided the best quality information, but the banks do not, so they cannot train their tools properly. The few banks using machine learning for AML today train their machines on previous years' SARs data. But if more than 95 percent of past SARs were wrong, then the banks simply perpetuate the inaccuracies, just more efficiently.

However, with feedback from law enforcement, systems can learn and improve. This is where we need to bring the AML regime: information sharing, and priorities.

I do not want to end without raising a word of caution. Computers are powerful tools that can do both good and bad. As far back as the 1968 Stanley Kubrick and Arthur C. Clarke film, "2001, a Space Odyssey," we humans have understood the need to harness the computer. To ensure we maintain the balance between risks and rewards of advancing technologies, I suggest three core principles for the subcommittee to consider as part of any reform or legislative proposal.

First, encourage information sharing between law enforcement, financial institutions, and regulators. This will enable the sharing of priorities and the training data for machine learning.

Second, avoid opaque solutions where humans cannot understand and interpret the internal processes and outcomes of the machines.

And, third, keep humans in the loop. Let machines sort and filter data, but let humans adjudicate good and bad, right and wrong.

To close, machine learning already pervades our lives. Technology will increasingly enable regulated financial institutions to identify threats with increasingly precise measurements that will enable enhanced security, protection of privacy, and promotion of financial inclusion.

We spend billions today to generate mostly useless data, and miss 99 percent of global financial crime. Law enforcement knows that better systems, based upon existing technologies, are available to generate good data and keep us all more safe and secure.

Thank you for your time. I look forward to your questions.

[The prepared statement of Dr. Shiffman can be found on page 61 of the appendix.]

Chairman CLEAVER. Thank you very much.

I now recognize myself for 5 minutes for questions, and begin by making reference to this New York Times article, which is very disturbing. It talks about one of the executives from Goldman who runs their Asian office, and he has pleaded guilty in a Federal criminal investigation of fraud, and has been ordered—this is the part that troubles me; it is not the main part—to forfeit $44 million. That is not insignificant. But that is the extent of his penalty, forfeiting $44 million. This is just one more example of what happens if you wear a tie and are considered to be in a proper job. I know people in jail who stole $44.

That has nothing to do with the hearing, but I had to get it off my chest.

But this particular fraud emanated in Malaysia. And I understand Treasury's Financial Crimes Enforcement Network, FinCEN, is one of 159 financial intelligence units in the world. Through international cooperation, these units are better able to detect and counter transnational crime, including terrorism.

In my home State of Missouri, we have six foreign banking organizations engaged in a range of financial transactions. And so, I am hopeful they are not engaged in any such illicit activities and are not doing any damage to my constituents. But what makes me feel assured is Treasury's work with the international counterparts.

So Mr. Cohen, can you discuss, ever so briefly, FinCEN's efforts with the international counterparts and the value of Treasury's technical assistance international attache's program?

Mr. COHEN. Absolutely.

I will start with FinCEN. FinCEN is part of the Egmont Group of financial intelligence units (FIUs). In fact, it is one of the founding members of that international body. It is a group of, as you said, 159 FIUs that meets on a regular basis to discuss what the operational standards are for information sharing. Between these bodies, these financial intelligence units, every country has more or less an equivalent of FinCEN.

FinCEN has both financial intelligence units and regulatory responsibilities. Other FIUs just have one or the other, or maybe both. And so that engagement is tremendously important for the United States as we are one of the predominant players in that space in sharing information with our partners. And the information that we receive is tremendously helpful for our law enforcement agencies and others.

In regards to the Treasury attache program, that is a program where we have, in select strategic countries around the world, just like you have CBP attaches, FBI attaches around the—I mean, embassies around the world. You have Treasury attaches, but to a much lesser extent. And they advocate for U.S. sanctions policy. They advocate for combating financial crimes, and implementation of international AML standards.

So in that sense, it is tremendously important.

Chairman CLEAVER. Thank you.

I want to get to the FBI. I could hardly wait to ask you this question. What can Congress do? Where can this committee begin in

terms of creating international support and cooperation in fighting money laundering? You have places where people traditionally go to launder money, but what can we do as a body?

Mr. LORMEL. Thank you, sir, for that.

I think there is an awful lot that you can do. And it starts with understanding what the issues and problems are.

And to the point that Mr. Stivers made earlier about what not to overreact to, the first thing for law enforcement is—or the FBI law enforcement in general, is the reporting thresholds. We need to be able to have—and law enforcement needs the ability to access and to use that information. And they do that to a very good degree.

I think part of the answer to the question you are asking is the difference between regulatory requirements and regulatory expectations involving the regulators. And I think there is kind of—if you look at it—the financial institutions and the regulators and law enforcement, there is a triangle here. And there are hard lines between the financial institutions and law enforcement, and financial institutions and the regulators. But there is a broken line between law enforcement and the regulators.

Chairman CLEAVER. Keep that line right there. I will get back to you with that line.

My time is up.

I recognize the distinguished ranking member for 5 minutes.

Mr. STIVERS. Thank you, Mr. Chairman. I really appreciate you calling this hearing. Again, I want to thank all the witnesses for your great testimony. And Mr. Lormel, I want to ask you first, there were 900,000 suspicious activity reports last year, give or take. That is an approximate number. I have to deal in round numbers because it is all I can handle.

But of those, some were very useful, and some were less useful. And to the point you just made, I don't want to reduce the number of suspicious activity reports, but I want us to be able to efficiently process them, which speaks to Mr. Shiffman's point about machine learning.

Are we using machine learning enough, and are we communicating back? I have looked at the draft in Sections 109, 201, 202, and 203. Nothing really refers back to the kind of machine learning and computers that have to happen to go through 900,000 reports. Are we helping create a more efficient system, to my opening statement again? And what can we do in this draft to empower that?

I will go to Mr. Shiffman next. But have we mentioned the right things in here? I like the fact that it requires a feedback loop, but are we doing what we need to do?

Mr. LORMEL. I think this is a very good start. I think this is a great foundation to build on.

The question you are asking, though, sir, it is such a much more complex issue, because if you look at suspicious activity reports from a law enforcement standpoint, the first part of your question was the analytics. And when I was at headquarters and on a program level, we would use those types of analytics. And we need more and better of those analytics, so I will defer to these—

Mr. STIVERS. And I want to go to Mr. Shiffman now, because you brought up a really good point. Machines only learn what we tell

them. So if we are not giving them good feedback, machines aren't getting better. We could be a lot more efficient.

Is there anything in this draft we need to do to acknowledge what is going on, or be more specific about the machine learning that is going on to make it better?

And I want to acknowledge, again, Mr. Chairman, this draft is great. It is a really good start. But I am asking, Mr. Shiffman, can we improve it?

Mr. SHIFFMAN. Thank you, Mr. Stivers.

I agree. I think this draft is very good. I really like the bill and where it is going and take very little exception to anything in the bill.

I would emphasize that—so picture a triangle. You have law enforcement, you have the regulators, and you have the banks. I would argue that communication across all those channels is not good, or is just one way sometimes.

In order to take advantage of technology, the banks need the feedback from law enforcement so they can train their algorithms. The banks are already investing billions of dollars in this. So this isn't a matter of appropriating dollars. This is a matter of giving the banks the data they need to train algorithms and to set priorities. That concept is already in this bill. I would just emphasize it for the members of the committee.

Mr. STIVERS. I guess that goes to the heart of my question. When I read the draft, it does talk about sharing compliance resources in Section 202. It talks about sharing suspicious activity reports within a financial group and the FinCEN exchange with their financial institution counterparts.

Do we need to more expressly define that triangle and that sharing that needs to happen between the three and between the machines at the three places for the computer analysis that needs to happen here? It seems to me we might do a better job of explaining the legislative intent of what we want to help them actually comply with law enforcement and FinCEN and the financial institutions.

Mr. SHIFFMAN. I think that would strengthen the bill. I think the bill is already pointed in the right direction, but that would strengthen it.

Mr. STIVERS. And I believe that, too.

Thank you.

I am going to yield some time to the gentleman from Arkansas, Mr. Hill.

Chairman CLEAVER. The gentleman is recognized.

Mr. HILL. Thank you, Mr. Stivers. And I appreciate you calling this hearing, Mr. Chairman.

Just following up on that question, Mr. Shiffman, how do we protect the privacy of Americans in this triangle you described? What is in this bill that thoroughly protects people's Fourth Amendment right to privacy?

Mr. SHIFFMAN. I can't speak as an expert on this bill itself. But I think that there are ways in which we can move forward, improve a system, take advantage of the vast resources spent in this AML regime and get better results and protect privacy. And I think we need to do that.

I know privacy is addressed in the bill. I am not an expert on what the committee had in mind as they drafted it. But I think we do need to be acutely aware of the tradeoff between law enforcement and privacy, and it is something that we have all been dealing with throughout our careers.

Mr. HILL. I yield back. Thank you.

Mr. STIVERS. I yield back the balance of my time.

Chairman CLEAVER. Thank you.

I would like to ask unanimous consent to allow Mrs. Maloney, who has done enormous amounts of work in this area, to claim 5 minutes for questions.

Mrs. MALONEY. Thank you so much.

Chairman CLEAVER. Without objection.

Mrs. MALONEY. Thank you so much, Mr. Chairman, and Mr. Ranking Member, for holding the hearing. I thank you for allowing me to participate. And I thank all of my colleagues, and I thank all the panelists for your testimony today.

This hearing is examining a bill that I have been working on for 10 years, along with my good friend, Peter King, the Corporate Transparency Act, which requires companies to disclose their beneficial owners to law enforcement and financial institutions.

The problem that we are trying to solve here is very simple: Criminals and terrorists have always used anonymous shell companies to finance their operations. And because they never have to disclose who actually owns the shell companies, there is no way for law enforcement to figure out who is involved in a transaction conducted by a shell company.

Law enforcement tells me that whenever they are following the money in an investigation, they always hit a dead end at an anonymous shell company. They can't figure out who is behind it, so they can't follow the money any further.

This is a very serious problem in the City of New York. This challenge was brought to me by law enforcement who are very concerned about, first and foremost, terrorism financing. We are a terrorist target. Since 9/11, numerous other people have tried to strike us. Where did they get the money? Where did it come from? Where did the technology come from? Where did the bomb-making skill come from? All of this information they would like to know. And when they say they hit this LLC, they can't figure out who owns it.

You can just ride through my district at night, the East side of Manhattan, and you will pass buildings, complete buildings, where there are no lights on. They are bank accounts. And they simply want to know who owns that bank account, for national security.

President Obama was so concerned about this issue that he even formed a task force the last year he was in office with Jim Clapper, head of National Security, and others trying to figure out how to pass this bill that would allow law enforcement to get the tools that they feel they need to protect us.

To help address this problem, FinCEN passed a rule in 2016 that requires financial institutions to identify the beneficial owners of the companies that open accounts with them. My bill would take this burden off of financial institutions, and would require companies to disclose their beneficial owners at the time the company is

formed. FinCEN would collect this information. And the only people who would have access to it would be law enforcement and financial institutions. And in the case of the financial institutions, the person with the information would have to allow that to be disclosed.

I think my bill would help protect our national security, and law enforcement believes the same, and would provide regulatory relief for financial institutions.

I want to submit for the record a statement from the Bank Policy Institute on the importance of beneficial ownership legislation, and a letter from 9 different financial services trade groups supporting beneficial ownership legislation, and also statements from law enforcement in support of the bill.

Chairman CLEAVER. Without objection, it is so ordered.

Mrs. MALONEY. I want to thank the chairman for yielding to me, and Mr. Lormel, I want to ask you about beneficial ownership. I know you have seen my bill, and I want to thank you for your support for this effort.

Now, my colleague, Mr. Hill, has also circulated a bill on beneficial ownership, which I personally think is far, far too weak.

Have you seen Mr. Hill's bill?

Mr. Lormel?

Mr. LORMEL. Yes, ma'am. I have.

Mrs. MALONEY. Do you think Mr. Hill's bill is workable, or do you think Congress would be better off, and the safety of the American people better off passing my Corporate Transparency Act?

Mr. LORMEL. I think your Act is much more comprehensive.

Mr. Hill, I thank you for your effort in this, but I think that—you recommended that the IRS be the collection point, and that is not workable, sir, from my experience. And I think that Mrs. Maloney's bill is much more comprehensive. You also, Mrs. Maloney, you don't have any thresholds. You are asking for all beneficial ownership. I didn't believe that to be the case in the other bill.

Mrs. MALONEY. Are you concerned that—and I congratulate Mr. Hill's interest and hard-working efforts, but are you concerned that Mr. Hill's bill doesn't even have a provision that would give law enforcement access to the beneficial ownership information?

Mr. LORMEL. Yes, ma'am. I think that is a serious problem because as a law enforcement—

Chairman CLEAVER. Go ahead and finish.

Mr. LORMEL. Okay. Just to the point about access, as an FBI agent, I wouldn't have access to that information because I would have to have a court order to get IRS information, especially tax information.

Mrs. MALONEY. You can't collect information if you can't see it, right? Has my time expired?

Chairman CLEAVER. Yes.

Mrs. MALONEY. Thank you.

Chairman CLEAVER. The Chair recognizes the gentleman from the great State of Texas, Mr. Williams.

Mr. WILLIAMS. Thank you, Mr. Chairman. Thank you all for being here today.

And Mr. Lormel, since you have had firsthand experience in the law enforcement perspective, can you walk us through an example where having the beneficial ownership information was crucial for you?

Mr. LORMEL. Yes, sir. I served 10 years in New York. I was a supervisor in New York. Back in 1983, there was a case that we had with a broker-dealer, and it was an internal embezzlement of about, at that time, $18 million, so you can imagine that $18 million today would be a lot more. The subject who embezzled that money set up, at first, four shell companies, and then he expanded to eight shell companies. And working through those shells to get to—and back then, it was a lot more difficult because we didn't have the internet; we had a paper trail. And so, working through those shell companies was very, very difficult. There were so many impediments to get around them, and to develop the evidence that we needed. It was very challenging, sir.

Mr. WILLIAMS. Okay. Thank you. Dr. Shiffman, you mentioned in your testimony that technology and machine learning will be the cornerstone of any future BSA/AML regime. FinCEN has an entire technology division within the department. My question to you is, what is the biggest hurdle in getting this technology into use for BSA/AML purposes?

Mr. SHIFFMAN. Sir, I think FinCEN has great data, because they have all the data sent to them by the financial institutions, but I am not sure it is the right data, but they have a lot of data. The banks also have a lot of data. I think it is about training tools to identify the right data. As I said in my testimony, at least 95 percent of the suspicious activity reports sent to FinCEN never provide any value, so that is a massive investment on behalf of the banks, and it is a massive amount of data at FinCEN that never provides value.

So my concept here is that, let's get the ground truth data, the actual cases of known money laundering, terrorism, drug trafficking, things like that, and train algorithms, both at FinCEN and in the financial institutions, and we will have a much more efficient system.

Mr. WILLIAMS. Mr. Cohen, I would like to hear what you have to say, if you have anything to add to that answer.

Mr. COHEN. Absolutely. I think it is critical for the machinery to work, if I understand it correctly, and I am certainly no expert, but communication and information sharing with the private sector is fundamental.

FinCEN as the FIU aggregates all this information, all the SARs that are submitted by financial institutions, and then they can provide critical insight to financial institutions around the country to be able to better identify the type of activity.

So I think that FinCEN Exchange programs, like the FinCEN liaison program, the domestic liaison program where you have folks engaging with industry, understanding the threats locally, regionally, that will greatly enhance, in my opinion, financial institutions' ability to detect suspicious activity and make the algorithms and machine learning even more powerful when that information then comes out and is looked at by an analyst.

Mr. WILLIAMS. In 2016 alone, there were over 900,000 suspicious activity reports filed with FinCEN along with 3½ million currency transaction reports. With so much information coming in, it seems that bad actors will easily be able to slip through the cracks, since millions of other legitimate transactions are being reported. So my question to you, Mr. Lormel is, I see from your testimony that you are not in favor of raising the thresholds for SAR and CTR. What recommendations do you have, then, in order to make the information within these reports more useful?

Mr. LORMEL. There are a few things, sir. You have to look at different perspectives. Now, from where I have sat at headquarters, we did data mining, and we did analytics, and I think that is one of the ways forward in terms of using that. But if you go down to the grassroots, to the SAR review team level out in the field, they are going through it by hand. So you have two different perspectives that you are dealing with.

But part of the issue, again, comes down to, from where I sit, regulatory expectations versus regulatory requirements and financial institutions kind of getting caught up. If you think about the flow of information from a financial institution to law enforcement, that flow gets impeded by the regulatory requirements to a degree and then the regulatory expectations, so part of the answer also is the feedback. We have to have a better feedback mechanism, like Gary said, from law enforcement, where the banks understand it, and they get those scenarios. I think with the bill that you guys have introduced, you are setting the stage for that with 314.

Mr. WILLIAMS. Thank you for your testimony.

I yield back.

Chairman CLEAVER. Thank you.

The Chair now recognizes the gentleman from Colorado, Mr. Perlmutter.

Mr. PERLMUTTER. Thank you, Mr. Chairman, and gentlemen, thank you for your testimony.

I want to focus, first, on sort of the technology piece of this thing. We have two detectives, one in financial and the Treasury, and one police detective and sort of two technologists who want to provide—help them have the best information they can have. So Mr. Sharma, you said something, and that I was kind of scratching my head. You said that growing regulation IT costs and compliance has led to financial exclusion. Am I quoting that right? What did you mean? I didn't know what you meant.

Mr. SHARMA. Right. Thank you for your question. What we have seen, especially with global financial institutions, certainly western financial institutions, and the U.S. in particular, is that the combination of growing financial sector requirements, vis-a-vis AML compliance, and the ongoing fines that have increased over time, many of which are fully warranted for negligence or willful blindness, et cetera. Many institutions start looking at particular types of transactions, particular types of entities and constituents as just high perceived compliance risk. An example would be global remittance flows. And if I as a bank am spending an increased amount of time, energy, manhours, and money on understanding money services businesses Fintech companies and other non-bank FI activity that are sending money to the tune of hundreds of billions

over the course of a year, but that is costing my business a lot from a compliance perspective, many institutions have just said I am not going to do business at all.

Mr. PERLMUTTER. And so, quickly, how would you remedy that? And I have some questions for Mr. Shiffman.

Mr. SHARMA. This is where I think technology plays a vital role both in terms of the use of applied and advanced analytics like AI and machine learning. Distributed ledger technologies that can bring real-time transaction tracking and client monitoring while preserving the essential personal identifying information in the back end offer great promise to do these things in an environment that has been a very high traditionally man-hour-centric environment or process. So these two technologies have tremendous promise to drive inclusion and keep folks in the system, while, at the same time, following the anti-money laundering, know-your-customer, customer due diligence, monitoring and transaction tracking that are essential to the compliance tool kit.

Mr. PERLMUTTER. All right. Thank you. And so Mr. Shiffman and Mr. Hill brought up the fact that we want to have as much information, make it as effective as possible for our law enforcement, but we are all subjected to the Constitution and our rights to privacy and things like that. So the three of us—Mr. Gonzalez, Ms. Wexton, and I—are all on the Science Committee, and you talked about Hal from "2001, A Space Odyssey." I talked about Skynet from "The Terminator." Why did you bring up Hal? What is it that you are worried about with artificial intelligence in this arena?

Mr. SHIFFMAN. If you recall, Hal wouldn't let Dave back into the spacecraft.

Mr. PERLMUTTER. Right. I know. I mean, in "The Terminator," Skynet became aware.

Mr. SHIFFMAN. Right. Absolutely.

Mr. PERLMUTTER. And singularity is when the computers become aware. I am not trying to minimize it.

Mr. SHIFFMAN. Right.

Mr. PERLMUTTER. I think the concern is that—I am over on the fiction section, not the non-fiction section. The concern, though, is coming back to the Constitution, coming back to the right of privacy, you said we need to focus on three core things: information sharing; avoiding opaque solutions; and keeping humans in the loop. Can you expand on that a little bit?

Mr. SHIFFMAN. Sure. Machines are literal. They will do what they are taught, and they don't know right from wrong. They don't have judgment. So you could intentionally, or inadvertently, program a machine that does the wrong thing, and that is why we always need to have, in my opinion, a human in the loop. Humans do know right from wrong. Machines don't. Machines do what we tell them to do. That is why I want to live in a world—my point is we are not going to stop machine learning, artificial intelligence. It is here. It is here to stay. It is pervading every aspect of our life. Therefore, it will make it into AML, so let's deal with it, and let's keep in mind that we want humans in the loop so that way, we can address things like financial inclusion and things like privacy. And if we don't think a lot about that now, we are going to be in trouble later.

Mr. PERLMUTTER. Okay. Thank you, Mr. Chairman, and it was fun talking about that. I yield back.

Chairman CLEAVER. You and Dr. Shiffman need to go into the corner.

The Chair now recognizes the gentleman from Arkansas, Mr. Hill.

Mr. HILL. Thank you, Mr. Cleaver. I appreciate that. I appreciate Mrs. Maloney's long years of work on the Corporate Transparency Act and her various iterations of it over the past couple of Congresses. And, of course, all of us support the adequate disclosure that we need for law enforcement to do their job. That is really not in question here. And since the know-your-customer rules were promulgated as a part of Gramm-Leach-Bliley, banks have been collecting this information and had obviously a responsibility for 40 years to follow suspicious activity reports.

Mr. Lormel, I was reading your testimony. On page 7 of your testimony, you say your long-time preference is that the States collect this information, and you said they resist doing that. Are you aware of Congress having hearings on the States collecting this information?

Mr. LORMEL. Yes, sir. Back in 2012, I was actually invited to the annual conference of the National Association of Secretaries of State (NASS) where we discussed this issue, and I—

Mr. HILL. They resisted, of course, and, you know, that is their prerogative.

Mr. LORMEL. Yes.

Mr. HILL. We have 50 States. We have a Federal Government, federalism, and we incorporate entities at the State level. Hasn't this been a problem for years? As an FBI agent, you would say that your biggest concern are all the Californians who claim they are Nevadans, right, for tax evasion purposes. Isn't that a big problem in this country, tax evasion, using the laws of Nevada if you are either a California or an Alaska trust?

Mr. LORMEL. Yes, sir.

Mr. HILL. So we have this challenge with the States, but if we had a set of best standards and beneficial ownership requirements that the States could collect, and should collect in your view, I think, based on reading your testimony, you would support the States doing a better job of being transparent, then, wouldn't you?

Mr. LORMEL. In most circumstances, I probably would.

Mr. HILL. Yes. That is the way I took your testimony, so thank you for that. I think we all agree that it would be great if there was consistent information collected by the States in a machine-readable format. We don't have it. I will argue that that has never really been requested by the Federal Government on behalf of national security for tax evasion purposes, not that I can read in the record. So I will leave it at that for the moment. I know Secretary Mnuchin prefers that. I know the members of this committee prefer if the States would do that.

One of the issues, though, you also bring up in your testimony, on page 8, you raise serious concerns about FinCEN's capacity to collect and disseminate beneficial ownership information. Is that in your testimony?

Mr. LORMEL. Yes, it is.

Mr. HILL. Yes. So that is why I focused on this issue of perhaps the normal tax collection process. Like we have changed Schedule B on the Form 1065 many times to collect additional information about foreign bank accounts and foreign activity that we change, that collect beneficial ownership in the same place where we collect all the ownership information of a pass-through entity in the case of an LLC or a partnership and then on the C corp forms or S corp forms for a corporation, and we change the question there. We had that material. In contrary to the testimony you all exchanged in your colloquy, it would be shared with FinCEN from the IRS, so that is the way my bill reads. And I think that is where most small businesses do this kind of work. Instead of having another form with another criminal penalty, Heritage estimates there could be a million unintended felons under the draft bill that we are considering because of the way it is written. I don't know if I agree with that. It could be an exaggeration. But the point is, we are asking charities, every business entity in America, to file directly with FinCEN beneficial ownership information, and yet, we collect all the ownership information, the contact information, the foreign bank account information, everything as a normal part of the income tax preparation. Isn't that right?

Mr. LORMEL. To a degree, yes, but I don't know that we collect all of the beneficial ownership information.

Mr. HILL. We don't do it now. We collect the ownership information undeniably unless you want to be penalty of an IRS—commit IRS fraud. I don't think most people want to do that.

Mr. LORMEL. No. No, not at all, but the other issue you have, Congressman, is the fact that I would need a court order as an FBI agent or another law enforcement officer.

Mr. HILL. So are you suggesting if we use Mrs. Maloney's FinCEN form, you won't have a court order? You can just go look at it? Is that what you are suggesting?

Mr. LORMEL. Yes.

Mr. HILL. You think that protects people's privacy, or should they have a reasonable reason supported by law enforcement to go look at people's information?

Mr. LORMEL. I think that is very reasonable.

Mr. HILL. So if in my paper records—I will yield back. Thank you, Mr. Chairman.

Chairman CLEAVER. Thank you.

The Chair now recognizes the gentlelady from Virginia, Ms. Wexton, for 5 minutes.

Ms. WEXTON. Mr. Chairman, I have no questions for these witnesses.

Chairman CLEAVER. The Chair now recognizes the gentleman from Ohio, Mr. Gonzalez, for 5 minutes.

Mr. GONZALEZ. Thank you, Mr. Chairman. Thank you, everybody, for being here, and for your testimonies today.

When I think of the challenge before us, I think of my home State, and I think of Fentanyl. I think of Fentanyl coming from China, going into Mexico, or going through our mail and coming into my community. In Ohio, over the past few years we have lost, in each individual year, more people due to the opioid crisis than we lost in the entirety of the Vietnam War. More people in a year

than the entirety of the Vietnam War. It has absolutely devastated my community, and so I thank you all for the work. I thank this whole committee for the work and the commitment to stopping money laundering, and making sure that we take care of the people of Ohio.

When I think of machine learning, and Dr. Shiffman, you will correct me if I am incorrect, I think you need good data, and you need it at scale, right? You need a lot of good data, essentially, and the more good data you have, the quicker your machines will be able to train themselves and be able to spot nefarious actors. In your testimony, you talked about 2 million suspicious activity reports, but less than 5 percent provide value. Mr. Cohen, if I could quickly, does that sound accurate? That is a bold claim. I have not heard that before, but is most of the data just not useful?

Mr. COHEN. Again, I can't speak to the numbers. I do know that the data is tremendously useful to law enforcement agencies and our international partners. Again, if you are talking about percentages, I don't know those numbers.

Mr. GONZALEZ. Okay. Dr. Shiffman, can you talk about that a little bit? How are you kind of making that claim?

Mr. SHIFFMAN. Sir, there is a footnote in my testimony for that claim, and it is the clearinghouse article called, "By the Numbers on AML."

Mr. GONZALEZ. Okay. Thank you. My next question, then, would be, again, to Dr. Shiffman. So it sounds like we have a bad data problem, essentially, among others, but what data do we need that we are not collecting, or how can we improve the SAR process generally?

Mr. SHIFFMAN. Sir, thank you for the question. The idea here is that in the world we live in today, where we are talking about this new generation of technology, we have to get data and algorithm into the same place at the same time. So how do we do that? We can compel banks to send data in to FinCEN, and that is what they do. But we don't do a good job of letting the banks know this data was good, this data wasn't, because if we did that, then they could refine their algorithms and send better high quality data more efficiently, right.

So it is just a matter of thinking about data and algorithm in the same place at the same time to do the training, because your understanding of machine learning is exactly right. It is about having good data and quantities of it.

Mr. GONZALEZ. Okay. And then quickly, Mr. Lormel, I talked about the Fentanyl crisis in Ohio. Could you describe, sort of, how that works from a shell corporation standpoint, and how they bury, essentially, what they are doing inside of these shell corporations?

Mr. LORMEL. You could liken that with the Fentanyl to any number of crime problems, but using your example there, if I have an operation, and I have people out there pushing Fentanyl for me, at some point, that money needs to get into the system. And so, one of the ways I am going to get that into the system is through shell companies, and the more opaque I can make that, and the more layers I can put in there, the more I am going to be able to comfortably move my money through and start to legitimize it again. You raise, you move, you store, you spend. And the more that you

store and you move, the more opaque it gets. And that is exactly what I would be doing if I was involved in one of those operations.

Mr. GONZALEZ. Thank you. And with that, I will yield back the balance of my time. Thank you.

Chairman CLEAVER. The gentleman yields back.

The Chair now recognizes the gentleman from Massachusetts, Mr. Lynch.

Mr. LYNCH. Thank you very much, Mr. Chairman, and Ranking Member Stivers. And thank you to the witnesses. We really appreciate it. I am familiar with all of your work. Thank you so much.

Mr. Lormel, I did not realize you had been doing this for 46 years. You must have been violating the child labor laws when you started out. Just like me. You can take the Fifth on that.

So I have been on this committee a while, and for a while, I was the chairman of the Task Force on Terrorist Financing before they made it a subcommittee. We are involved in Kabul Bank. We had a situation with the ATMs in Gaza that were operated by Arab Bank. Nigeria. We had a terrible diversion of natural resources. In all those jurisdictions, we had very weak rule of law. And so, one of the ways that we were able to get at that was that FinCEN—thank you, Mr. Cohen—was able to work with people on the ground in those countries that actually provided firsthand information, so we were able to get at this.

So that is what led to the kleptocracy bill, because in many of these countries, especially developing countries, because of the lack of rule of law, and the lack of a strong independent judiciary, it is the only way we can get at this stuff, and FinCEN has been doing a lot of this stuff already. They just haven't been formalized, but that is what I hope to do in my bill.

I am just wondering, Mr. Lormel, if there is—let me shift. Mr. Sharma, you are dealing with a new area, and I am aware of your work with CGS before on doing a lot of this work. Mr. French Hill and myself have been asked to head up this Fintech task force now. We just started it. Ms. Waters created it. What are the dangers? What are the new and different dangers that we see moving from this sort of brick-and-mortar system to online banking, and the digital dimension of this?

Are there new and different things that we need to upgrade our regulatory framework to address that type of threat? I know you have been doing a lot of that work, and also, you have been doing great work on underbanked areas and things like that, but just the technology change. How would we best respond to that threat?

Mr. SHARMA. A couple of things. I really appreciate the question. So in my opening statement, I talked about a couple of trends that I think that we need to layer in as we look at oversight. One is that increased financial remediation is happening outside the banking network.

Mr. LYNCH. Yes. It is shadow banking, you mean.

Mr. SHARMA. Shadow banking. I often tongue-in-cheek ask the regulators, when was the last time you visited Walmart? When was the last time you visited Target? When was the last time you visited Amazon? These are banks. At the end of the day, these are institutions that have certainly a nationwide, if not a global network and engage in credit, lending, stores of value, et cetera. And so now

you add that to the growing and emerging non-bank and Fintech space, and there is just increased financial intermediation there. And so from a regulatory perspective, we need to start looking in areas outside of what has been traditional covered institutions.

The second is in the context of how some of these new technologies, in particular for the advanced analytics side and in distributed ledger actually provide tremendous opportunity to the unbanked, and some of these are macro challenges that we treat as compliance challenges.

Mr. LYNCH. Let me ask you to pause there, because we have had some major hacks of our blockchain technologies, Bitcoin in particular.

Mr. SHARMA. Yes.

Mr. LYNCH. With Mount Gox and some others, $350 million went in one whack, so have we—and those were fairly recent. I think the last one was in 2014. But have we got to a point where we trust the system? And believe me, I know, in theory, that blockchain will work, and it is probably our best hope, but are we there yet to a point where we can actually, as a Congress, sort of endorse this going forward without having some level of fear for the risk that it creates?

Mr. SHARMA. I believe blockchain and some of these technologies aren't panaceas. They aren't going to be the be-all-end-all. We do need to understand the difference between the applications of these technologies in the areas that are hackable or corruptible, as we have seen in the Mount Gox and other crypto areas. The underlying technology of distributed ledger does hold promise insofar as the encryption, distribution, and immutability of that ledger. It is harnessing that technology in the context of AML/CFT for transaction tracking and the protection of the underlying information, whether it is your personal data or otherwise.

Mr. LYNCH. Data, yes.

Mr. SHARMA. And that is the key.

Mr. LYNCH. Yes.

Mr. SHARMA. And so, no, I would not be here saying you must endorse a particular technology as the be-all-end-all but this is where the coordination and technology and innovation centers with regulators can look at both the application tested both in beta and in live-market situations of that technology to address both the inclusion elements and AML/CFT in tandem.

Mr. LYNCH. Thank you.

Mr. Chairman, I yield back. Thank you for your indulgence.

Chairman CLEAVER. Thank you.

The Chair now recognizes the gentleman from Virginia, Mr. Riggleman.

Mr. RIGGLEMAN. Thank you, Mr. Chairman, and thank you very much to the witnesses. I want to thank my esteemed and venerable colleagues for asking most of the questions I was going to ask. First of all, thank you.

Second, I want to say—I want to go a little bit geeky here. My background is a little bit different, I think, and so I want to tell you guys what I have done before I ask some of these questions, because I looked at your resumes. I looked at your bios, and I am very impressed, and probably, it is going to be all of you trying to

ask some of this. But for about 26 years, I have been in counterterrorism. For the past 15 years, I have been involved in trying to build data ecosystems to automatically predict what would happen in the command and control networks, right, and you guys know that is a complete infrastructure from fiber to cyber.

So listening to this, I don't think this data problem is unique based on what I have gone through, and I want to let you guys know I have broken a lot of capabilities for machine learning and AI in my life. I have completely broken them, and it might have been operator error, but not most of the time.

I want to ask Mr. Lormel something. First of all, thank you for your service for 46 years. I very much appreciate that, and I want to ask you: When you are looking at SARs and CTRs for your teams, are you noticing any attributes? Are you noticing any consistencies in the data that allows you to hone in on something rather than another based on the manual templates that you have built and trying to see what SARs or CTRs are effective?

Mr. LORMEL. Thank you, sir. Yes. Again, if you are looking at SARs from where I sat at a program level, I am looking at it differently, so I am using the data mining capabilities. And so it is easier for us, then, to sort and we are looking at certain things. At the street level, it is going to come down to what we are looking at in those specific locations, which agencies are involved, what violations do we work because that is going to help inform where I am going to look for—what I am going to look for in SARs. So you have the SAR review team. You have an IRS agent. You have an FBI agent. They are going to look at the same SAR. They may see it differently.

Mr. RIGGLEMAN. I put in a couple bills, 1038 and 1039, to be a little bit more clear on the requirements from the Department of the Treasury and what you guys are looking for, and I am wondering, this is for Dr. Shiffman and Mr. Sharma, and I think, Mr. Lormel, I am going to assume something, that some of your teams are very good at SARs and CTRs and tracking down people.

When you look at requirements, and Dr. Shiffman and Mr. Sharma, you are going to smile at this question. If you are going to build an ML template, a machine learning template, we could use Mr. Lormel and his teams to start that ML template to look at what SARs and CTRs are actually effective in going after these certain individuals. Anytime we are parsing data, it is the "gazintas" and the "gazoutas," right? So when you are looking at the "gazintas" and the "gazoutas," that is my operational term for data. When you are looking at that data, and we use Mr. Lormel's template, is it possible that we could actually build within the bill, or whatever bill that we pass, the ability to be more specific on requirements based on the templates that are built, could you, Mr. Sharma and Dr. Shiffman, look at the specific SARs and CTRs, based on machine learning, where we could be more specific on what is to be reported, so it is not everybody in the world trying to report these specific items? And either one of you can start.

Mr. SHIFFMAN. Absolutely, you can do that, sir. You don't want to preclude the ability for the machine to tell you things that the human couldn't identify on their own. The machine can look at a

million attributes where a human can't. So you want to be open to that, but absolutely that is where you start.

Mr. SHARMA. And I would just add where it is the big data, a lot of the data and the associated algorithm to learn, and this is where a human judgment, both on the input and the output side, is critically important. You don't want the machine to just simply reinforce underlying biases in the data, and you don't want it to provide "garbage out" simply because it would be fully learned, because that is effectively what data you gave. This is where the 46-year esteemed career of Dennis Lormel plays a huge part in informing machine learning.

And then secondly, technologies like distributed ledger can, in fact, allow for permissioned access across a number of different data stores that, by mandate, have to be protected.

Mr. RIGGLEMAN. I would say that I don't think we should take a human out of the loop in any of these processes. I think that is what we are going to, right, Mr. Sharma? No human out of the loop. But I think my biggest fear—I have owned multiple companies. I have filled out multiple forms, whether they are OOIs, TTB types of information, all the background check you have to do. I had to do Federal acquisition requirements. I have had a lot of fun in my life, trying to go with regulation. But when I look at what Mr. Hill is talking about, and we are looking at bills across the committee, I think the Treasury is more specific in those requirements, based on maybe machine learning that you guys could do for us. Maybe we can dig down and actually build out of those 1065s, OOIs, background checks that we have and use data parsing to get the information that we have from the templates that are built by Mr. Lormel's team and then actually transition those to machine learning or AI or algorithms that can dictate what we want for requirements, rather than just going wholesale, sort of, beneficial ownership like cataclysmic idea of data.

Mr. SHIFFMAN. Just to build on that, I think you are right, and one of the points that I would emphasize from my testimony is this idea of priorities. What you are talking about is establishing the priorities, and that is going to make the system much, much better. We don't really do a good job of that today.

Mr. RIGGLEMAN. Thank you, gentlemen. I am very impressed by you all. Thank you.

Chairman CLEAVER. Thank you.

The Chair now recognizes the gentleman from Illinois, Mr. Garcia.

Mr. GARCIA. Thank you, Mr. Chairman, and I too want to thank all the witnesses who have provided such valuable testimony here in our endeavor to make an impact on this great challenge that we face.

I would like to ask Mr. Lormel a question. While there are many factors that contributed to the opioid epidemic, a 2016 report from the organization Fair Share explains that a key facilitator of opioid trafficking is the ease with which drug cartels can open anonymous shell companies to launder their illicit gains, and mask their identifies from law enforcement. Has it been your experience that drug cartels hide behind anonymous shell companies to impede law enforcement investigators?

Mr. LORMEL. Yes, sir. Again, you can use a lot of examples, but yes, I mostly worked financial crimes in my career, but where I did assist with drug investigations, that was always a challenge that the people who are responsible for laundering the money, the people involved on the facilitation side like that, that is their job description is to go out and hide that money. They want to disguise it. They want to make sure that it avoids detection.

Mr. GARCIA. Thank you. And do you believe that collecting beneficial ownership information of those companies formed in the U.S. as the draft Corporate Transparency Act proposes to do would help law enforcement pursue criminal traffickers of heroin, Fentanyl, and other illicit opioids?

Mr. LORMEL. The simple answer is yes. I think that is very much so, but I also believe that the bad guys are going to be out there looking to see how they can exploit other avenues, because they are going to look for other vulnerabilities. But to the direct question, yes. It would be very helpful.

Mr. GARCIA. Okay. Thank you.

Mr. Chairman, I would like to enter the Fair Share report into the record, if it is possible.

Chairman CLEAVER. Without objection, it is so ordered.

Mr. GARCIA. And then one final question. Again, Mr. Lormel, can you give us some examples of bad actors using anonymous shell companies in the U.S. from your experience in law enforcement?

Mr. LORMEL. I will use a kleptocrat. Vladimir Montesinos was the head of internal security in Peru. Montesinos, at one point, set up shell companies to launder $400 million around the world. I was running the financial crimes program in the FBI when we tried to help Peru render him back to the United States first. He had over $40 million through shell companies in the United States.

Mr. GARCIA. Any others that you would like—that you can share at this juncture?

Mr. LORMEL. There are just—there are so many. If you look at right now the ongoing 1MDB case, you can see a lot of use of shell companies there. There is just—I am sorry, sir. There are just so many cases you can go through.

Mr. GARCIA. I see some heads nodding, so it must be a known fact. Thank you very much. I yield back, Mr. Chairman.

Chairman CLEAVER. The gentleman from Tennessee, Mr. Rose, is recognized for 5 minutes.

Mr. ROSE. Thank you, Mr. Chairman. I yield my time to Mr. Hill.

Chairman CLEAVER. The gentleman is recognized.

Mr. HILL. I thank the chairman. And I thank Mr. Rose. I appreciate his time and willingness to do that.

Mr. Cohen, I was interested in this issue of balance. We were talking about the most important things, data from CTRs and SARs and beneficial ownership. All of these things are clues to put the puzzle together to catch bad actors, domestic, and to my point, and international. What do you think the most fundamental is from your time at FinCEN? Is it the SAR, the suspicious activity report? Is it the best clue among that group of many things, you think?

Mr. COHEN. I can't single out a single report that is most effective. I think it just depends on the nature, and I think Dennis will

speak better to that. I think every law enforcement agency, every single piece of the puzzle provided by that particular report could sort of break a case. So I certainly don't want to say what report is best or not. Certainly, the suspicious activity report is very important when you talk about the threats to the U.S. financial system, because a lot of that obviously comes through our financial institutions.

Mr. HILL. Yes. I have done it for 35 years in both the brokerage business and the banking business. The nice thing about it from a law enforcement point of view is it isn't quantitative, it is qualitative. There are some rules around it, and there are categories in which you report. But if it is a suspicious activity, you have a duty to report which is an ideal source of clues.

Mr. COHEN. Yes. Absolutely. I would add the sophistication of financial institutions varies around the country and around the world. The resources you have to devote to having—some banks have a dedicated financial intelligence unit internally, but others maybe have a few people. And so, I think working closely with the private sector, with financial institutions, law enforcement, we share a lot of information with them. Having FinCEN as the aggregator, right, because FinCEN has a big picture of all the SARs. They are the ones that collect all the SARs.

Mr. HILL. Right. I appreciate that response.

Mr. Lormel, on the issue of structuring, the big issue, no matter—we had a CDD rule put in place at Treasury last May, and, of course, it arbitrarily took 25 percent of the company you are supposed to report the beneficial owners. And yet, when we look at IRS data, it can be zero, or it can be 100 percent ownership of a company, a shell company, in your example. When we pick a number like 25 percent, like Treasury did in the CDD rule, isn't easily structured around? I know there is no right answer there, but what is your perspective on—and I would say most law enforcement people. You can't give them enough information, and you can't give it to them fast enough, and you can't give it to them better without a warrant. But with that caveat, how do you feel about that 25 percent, and having done it for 4 decades? What is your view of that?

Mr. LORMEL. There is always going to be wiggle room, so you have that 25 percent, I always make the misstatement if it is a "good bad guy." a proficient bad guy who really understands how to move money is certainly going to be able to circumvent that.

Mr. HILL. Yes. And that is an area where if you had aggregated information that you blended with SAR data in a legal way, you have a much better shot at moving that success ratio up.

Mr. Cohen, in your experience at FinCEN, does FinCEN aggregate open source data with that SAR trail as you are building a case, and to kind of respond to Dr. Shiffman and Mr. Sharma's analysis?

Mr. COHEN. I will caveat that by saying it's not analysis at FinCEN they do from my understanding in working closely with them. Yes, they do aggregate open source information with the BSA reporting that we receive, yes.

Mr. HILL. Right. So there are many good things, Mr. Cleaver, in this bill that are really improvements over the work, and I thank Mr. Perlmutter and Mr. Lynch, and Mr. Pearce in the last Con-

gress. We have listened to a lot of this. A lot of what we have heard is captured here like trade-based money laundering, and expanding the target on real estate, something of concern to the Chair and to Mrs. Maloney. So there are many improvements here, but I think we really tried to find some bipartisan consensus on this definition on beneficial ownership. I thank Mr. Rose. I yield the time back to Mr. Rose.

Chairman CLEAVER. The Chair now recognizes Mr. Sherman from California for 5 minutes.

Mr. SHERMAN. I want to focus a little bit on cryptocurrencies. I think, ultimately, they will be swept into the dustbin of history, but for purposes of these questions, let's assume that they will continue to be around for a while. They undercut the power of the United States Government.

First, the U.S. Government makes a lot of profit off of seigniorage, and I may be mispronouncing that term, the profit we make by minting money. We get to spend it first. Our banking sanctions have been incredibly effective, in large part because of the importance of the U.S. dollar, and cryptocurrencies seek to deprive the United States of this money and this power.

Now, among those rejoicing in the hope that cryptocurrencies will be successful are our foreign enemies, and also a strange group of people who view themselves as patriotic Americans. They just want to disempower the U.S. Federal Government, a certain Libertarian stream that wants us to stop terrorism so long as there is no power in the U.S. Government. We want a currency to be a medium of exchange and a store of value. The U.S. dollar is clearly superior to any cryptocurrency in those two things.

So it appears as if from the user's standpoint, the advantage of cryptocurrency is that it is a system for design and transmission designed to evade the U.S. Government. That is not only useful for terrorists, it is useful to ordinary criminals, and it is useful to people who view themselves as law-abiding Americans. They just want to cheat on their taxes.

Does cryptocurrency offer the user an advantage over U.S. currency or other euros or whatever, if they are not intent on evading Federal law? Mr. Sharma?

Mr. SHARMA. Sir, thank you for the question. I think that the first thing that we need to be taking great care of is that not all cryptocurrencies are the same. Not all cryptocurrencies are treated equal. Not all cryptocurrencies are created for purposes of full evasion or anonymity. In fact, there are tremendous benefits with respect to digital assets.

Mr. SHERMAN. The dollar can be a digital asset, too.

Mr. SHARMA. Correct. Exactly.

Mr. SHERMAN. I am saying cryptocurrency as compared to a dollar. Obviously, you wire money. You have been doing that for 100 years.

Mr. SHARMA. Correct.

Mr. SHERMAN. And you can say cryptocurrency is better because you can wire it.

I do want to move on to another question. Mr. Cohen, since 2016, FinCEN has had in place a continuous series of 6-month geographic targeting orders or GTOs. Do these GTOs, title insurance

companies and a number of areas around the country have worked with FinCEN to collect and report beneficial ownership information of LLCs and other legal entities in certain all-cash real estate purchase transactions?

It is my understanding that currently title companies are the only segment of the real estate industry taking part in Federal law enforcement programs to prevent money laundering. How did FinCEN come up with the decision to rely primarily on title companies for the collection of beneficial ownership information to combat money laundering in real estate? And to your knowledge, has beneficial ownership information collected and reported to FinCEN by title companies benefited law enforcement efforts?

Mr. COHEN. I have a quick reply to that because while I am aware of the issue, I was not involved in the specifics of the matter, but I do know that FinCEN worked very closely with law enforcement agencies in industry in order to develop the GTO in question. And I do know that information that has been provided must be—I think it has been reported publicly and has been useful to FinCEN.

Mr. SHERMAN. And have the title companies paid for their efforts in this area?

Mr. COHEN. I am not sure. I am sorry about that.

Mr. SHERMAN. Does any other witness have a response to that question about title insurance and GTOs? Hearing no answer on that, I can go back and ask for another witness to identify some advantage that cryptocurrencies have for the law abiding user over the U.S. dollar. Dr. Shiffman?

Mr. SHIFFMAN. As you said, sir, cryptocurrencies have gained appeal in kind of the Libertarian sort of movements. The advantage to criminals is that it has anonymity or actually pseudonymity, and so therefore, it is like cash, but it is much easier to move around than cash.

Mr. SHERMAN. It is the only currency designed chiefly for law evaders. I yield back.

Chairman CLEAVER. The Chair now recognizes the gentleman from Missouri, Mr. Luetkemeyer.

Mr. LUETKEMEYER. Thank you, Mr. Chairman, and I thank all of the witnesses for being here today.

Mr. Lormel, I just want to first thank you for your service, and then I would like to ask you about—you talked a little bit today about the levels on SARs and CTRs, and I have a concern about that from the standpoint of it hasn't been raised since it was instituted 30, 40 years ago. I think Dr. Shiffman made a comment that most of it was wasted. Can you give me a justification for not raising the SARs and CTRs whenever you have thousands and thousands and thousands of these things, millions of them, quite frankly, and it takes hundreds of thousands of people? How many people at FinCEN does it take to overlook these things when it takes hundreds of thousands of people to put them together?

Mr. LORMEL. You certainly bring up a good point, but in today's environment in particular, I think one of the biggest problems that we are looking at now is micro structuring in smaller amounts. The biggest threat we have is the homegrown violent extremist. I can't give you accurate statistics, because I am not in the FBI right now,

but I believe that the FBI has some statistics that they used last year in 2018 that talked about the percentage of cases that CTRs, in particular, were used in, and it was a pretty high level.

Mr. LUETKEMEYER. I would love to have that information. If you can get ahold of it for me, that would be great. My concern is that we are weaponizing the banks. We are making law enforcement officers out of them. I understand your position. The more information you have, the better chance you have to catch somebody, but let me ask you this question: Would you support putting a policeman on every single corner to prevent crime?

Mr. LORMEL. I'm sorry?

Mr. LUETKEMEYER. Would you like to see a policeman on every single corner to prevent crime?

Mr. LORMEL. In a perfect world, yes.

Mr. LUETKEMEYER. Okay. That is my point. In a perfect world, we had a single SAR for every single transaction, so where do you draw the line? Do you draw the line on having an office to put patrolmen every so many blocks, every so many miles? It is just like the SARs and CTRs. There is a cost benefit here. At some point—right now you have deputized the banks to be law enforcement officers.

Mr. LORMEL. On that point, that is dangerous in the sense that I would never call the bankers, and want to deputize or give them any—

Mr. LUETKEMEYER. They are not enforcing law, but they are gathering data for you, just like a detective would.

Mr. LORMEL. Right.

Mr. LUETKEMEYER. They are gathering data to help you make a case.

Mr. LORMEL. Their responsibility is to identify suspicious activity and report it, and that is really important.

Mr. LUETKEMEYER. I am not trying to say that this shouldn't be done, but I am trying to say, look, we have to find a cost benefit spot, or sweet spot, and I would like to work with you to find a sweet spot where we can raise the threshold to allow the hundreds or thousands or millions—some of these banks are paying millions of dollars to do these SARs, and according to Dr. Shiffman, most of it is wasted.

So Dr. Shiffman, I want to ask you to go back over your numbers for me. Can you give me those numbers again? I think I saw that 5 percent of SARs and CTRs actually provide value. Is that what you said?

Mr. SHIFFMAN. Yes, sir. Nobody knows for certain, but the estimates based upon polling done of the banks and others in the clearinghouse report, it is 5 percent at most.

Mr. LUETKEMEYER. It looks to me like most of the money laundering in today's world, isn't that being done with cryptocurrencies anyway?

Mr. SHIFFMAN. I don't know whether that is true.

Mr. LUETKEMEYER. If you look at the size, the amounts.

Mr. SHARMA. I think what you would find, sir, is that most of the money laundered in the world is in cash, and we are not going to outlaw cash.

Mr. LUETKEMEYER. It is laundered through cryptocurrencies, right?

Mr. SHARMA. In some instances, but no, I would not argue, nor have I seen any data to support that the most laundered instrument in the world is crypto. I don't believe that is true.

Mr. LUETKEMEYER. Really. That is information I have been given by multiple people, so that is interesting. Okay.

Dr. Shiffman, continue.

Mr. SHIFFMAN. I would say just to bring the law enforcement and Mr. Lormel's perspectives and mine together; law enforcement loves the FinCEN database right now, because it is massive, and 5 percent of a lot of data is a lot of data, right? So they have a lot of data that they like, and I wouldn't want to take that away. As Mr. Hill was saying, I don't want to take data away from them.

Mr. LUETKEMEYER. I am not advocating to take it away. I am trying to find a way for everybody to live here—

Mr. SHIFFMAN. Right.

Mr. LUETKEMEYER. —to be able to do your job to find the bad guys, but yet, don't push the cost on the financial institutions and say, if you don't do this, then you are part of the problem.

Mr. SHIFFMAN. Right. I think we love the current system because it is the system we have, but I think across law enforcement, there is this understanding—

Mr. LUETKEMEYER. Part of the bill, the BSA bill we put together last year, Congressman Pearce and I had in there a pilot program that had, I think, using some of your technology, Dr. Shiffman, to have an algorithm sit there and figure out by the transactions that go through a bank in a day's time, you can figure out when you come in the next morning, there will be a program, or a printout sitting there saying, we have three people you need to take a look at for the transactions for the day versus SARs and CTRs. That may be an indication, but there are a whole lot of other transactions, I think, if you use the right algorithm, it can actually do a better job. So that is my point. There is a better way to do this than SARs and CTRs. Thank you very much for your testimony.

Chairman CLEAVER. Thank you, Mr. Luetkemeyer.

I would like to thank all of the witnesses for your testimony today. You have been very helpful to us as we have dealt with an issue, and one of the beauties about this particular hearing is that there is no partisan component to it.

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.

[Whereupon, at 3:53 p.m., the hearing was adjourned.]

A P P E N D I X

March 13, 2019

TESTIMONY OF

Jacob Cohen

Former Director, Office of Stakeholder Engagement, Financial Crime Enforcement Network (FinCEN)

BEFORE THE

United States House of Representatives Committee on Financial Services Subcommittee on National Security, International Development, and Monetary Policy

"Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crimes"

PRESENTED at 2129 Rayburn House Office Building, Washington DC 20515

March 13, 2019
2:00pm

Chairman Cleaver, Ranking Member Stevers, and distinguished Members of the Subcommittee on National Security, International Development and Monetary Policy, I am honored by your invitation to testify before you today.

Today, I want to share my views on the importance of providing FinCEN and the Department of the Treasury with the appropriate resources to expand engagement and collaboration efforts with domestic and international stakeholders. While I will focus my remarks on FinCEN engagement efforts domestically, I will also touch upon Treasury engagements with foreign counterparts through its Attaché and technical assistance programs.

The increasing globalization of financial crime, sophistication of criminal actors, and complexities in AML/CFT regimes around the world requires focused and sustained engagement by FinCEN with U.S. financial institutions and other stakeholders. Expanding FinCEN's engagement, collaboration, and information sharing efforts with the private sector will enable FinCEN to continue adjusting to ever evolving threats, producing actionable financial intelligence and reporting to our public sector partners, while ensuring that the United States continues to have one of the most effective Anti-Money Laundering / Combating the Financing of Terrorism (AML/CFT) regimes in the world.

My testimony draws from the experience I have gained over the past eight years working to shape and implement initiatives to combat financial crimes and other national security threats with the Department of the Treasury, across the U.S. government, with experts and stakeholders in the international AML/CFT community, and the private sector.

Importance of Engagement

The current AML/CFT landscape in the United States and around the world is complex, dynamic, and requires FinCEN and its private sector partners to constantly adapt. The global dominance of the U.S. dollar generates trillions of dollars of daily transactions through U.S. financial institutions, creating significant exposure to potential illicit financial activity and other crimes. This places FinCEN and U.S. financial institutions at the forefront of combating financial crimes. To continuously adapt to the ever-evolving threats to our financial system, FinCEN must have the resources to regularly and systematically engage with financial institutions and other stakeholders.

As the former Director of the Office of Stakeholder Engagement within FinCEN's Liaison Division, I oversaw FinCEN's outreach efforts domestically and internationally. My focus was on developing collaborative partnerships with regulators, industry, law enforcement agencies, and foreign financial intelligence units (FIUs) to identify areas for mutual collaboration and maximize the use of financial intelligence to combat threats to our financial system. In this role, I found that FinCEN had limited resources to systematically engage and collaborate with the private sector given the scope of FinCEN responsibilities and the number of threats facing our financial system. As you consider how to strengthen FinCEN's ability to deter, detect, and disrupt all forms of illicit

financial activity, I urge you to support greater engagement, collaboration, and information sharing by FinCEN with the private sector.

FinCEN plays an often understated, but outsized role in protecting the integrity of our financial system. Created in 1990, FinCEN's mission is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. To fulfill this mission, FinCEN serves two roles. First, as the financial intelligence unit for the United States, FinCEN is responsible for the collection, analysis, and dissemination of financial intelligence to law enforcement agencies and other relevant authorities. Second, as the lead AML/CFT regulator for the federal government, FinCEN is responsible for implementing, administering, and enforcing the Bank Secrecy Act (BSA), the United States' primary AML/CFT regulatory regime.

Current Engagement Efforts

To effectively carry out these roles, FinCEN engages and shares information with the private sector domestically through a variety of mechanisms, including Bank Secrecy Act Advisory Group (BSAAG) meetings, sharing information through public and non-public advisories to financial institutions, and select speaking engagements. However, these engagement efforts are not sufficient to keep up with the challenges facing industry and the increasing calls from the private sector for more information so it may better detect and deter financial crimes.

A key mechanism FinCEN uses to engage with industry is the BSAAG meetings. Held twice a year, BSAAG meetings allow FinCEN and other regulators to have frank discussions with a cross-section of industry representatives regarding the health of the U.S. BSA/AML regime. These meetings facilitate discussions on money laundering risks compared to regulatory obligations, feedback to industry on the use of SARs, and other areas that may require regulatory clarity or an advisory. These meetings with public and private sector stakeholders are tremendously valuable in assessing the effectiveness of the BSA/AML regime and represent the foundation of FinCEN's efforts to promote consistency across our regulatory regime, build collaborative partnerships with industry, and protect the U.S financial system. However, engagement with a small fraction of financial institutions twice a year is not sufficient to generate the level of collaboration, continual exchange, and learning that FinCEN and the private sector need to engage in to stay abreast of emerging threats, and identify innovative approaches to continuously update and modernize our BSA/AML regime.

Another important mechanism FinCEN uses to communicate with industry is through its Financial Institutions Advisory Program. FinCEN issues public and non-public advisories to alert industry of specific suspicious activity possibly related to money laundering or terrorist financing. These advisories often contain illicit activity typologies, red flags to facilitate monitoring, and guidance on complying with FinCEN regulations to address threats and vulnerabilities. Advisories provide valuable and actionable information to financial institutions that allows them to enhance their AML monitoring systems and

produce more valuable reporting. Generating these advisories requires significant FinCEN engagement with law enforcement agencies and financial institutions, among other agencies and stakeholders. Due to limited resources dedicated to engage stakeholders, not to mention limited analytical support, FinCEN publishes advisories infrequently. This is evidenced by the low number of threat specific advisories issued by FinCEN in 2016, 2017, and 2018 when it issued 2, 5, and 3 advisories, respectively. Notably absent during the past three years were FinCEN advisories on human trafficking, trade based money laundering, fentanyl, and virtual currencies, among others.

Enhancing Engagement Efforts

The Treasury Department and FinCEN play a key role in protecting the integrity of our financial system and combating national security threats. Today, I would like to express my strong support for a few provisions in the discussion draft, "To make reforms to the Federal Bank Secrecy Act and anti-money laundering laws, and for other purposes" that I believe will enable FinCEN and Treasury to continue to meet the challenges facing our financial system.

Domestic Liaison Program

The breath and scope of FinCEN's responsibilities require ongoing engagement and collaboration with stakeholders beyond the beltway. I believe that providing FinCEN with the resources to establish a Domestic or Regional Liaison Program would allow FinCEN to meaningfully and systematically engage with financial institutions, large and small, federal, state, local and tribal partners, and non-traditional stakeholders like non-governmental organizations. The benefits of such a program would be substantial. Specifically, Domestic Liaisons in cities such as Miami, Los Angeles, San Francisco, Chicago, New York, and Dallas would allow FinCEN to:

- Readily identify region specific illicit finance risks working with industry and law enforcement agencies to potentially issue region or industry specific advisories or geographic targeting orders;
- Partner with federal law enforcement agencies and task forces on cases of strategic importance;
- Receive regular feedback from financial institutions regarding the operations of the U.S. BSA/AML regime;
- Communicate priorities and guidance more directly and with greater frequency to stakeholders;
- Stay abreast of opportunities and challenges of BSA/AML-related innovation.

On this last point I would add that as banks and non-bank financial institutions pursue innovative change, early engagement would allow for a better understanding of their approaches, as well as provide a means to discuss expectations regarding compliance and risk management. Monitoring industry developments throughout the country and encouraging responsible innovative approaches in BSA/AML compliance programs will enable FinCEN to stay at the forefront of BSA/AML-related innovation.

FinCEN Exchange Program

In December 2017, FinCEN launched the FinCEN Exchange Program to enable greater information sharing between the public and private sectors. FinCEN and U.S. law enforcement agencies rely on financial institutions to file SARs and other reports to identify and disrupt illicit financial activities. However, in many cases, financial institutions do not have adequate information about the nature of the illicit financial activity and as a result are unable to produce actionable information about the threats of greatest concern. Sharing information about specific threats would enable FinCEN and law enforcement to provide guidance that would permit financial institutions to more effectively allocate limited resources to identify and report illicit financial activity. This two-way sharing of information would also create a positive feedback loop allowing FinCEN to share the typologies learned from these exchanges with the broader financial community, enabling other financial institutions to identify and report similar activity.

This important initiative should be supported with dedicated resources for FinCEN to conduct the necessary research and analysis, and to increase its engagement with U.S. law enforcement agencies and the private sector. Moreover, supporting the Domestic Liaison Program would enable the FinCEN Exchange Program to inform and shape its information sharing efforts to address the needs or threats faced by financial institutions in regions where FinCEN has a domestic liaison.

International Engagement

Treasury Attaché Program

The U.S. Department of the Treasury engages with foreign counterpart agencies, foreign financial institutions, and foreign companies to advance U.S. sanctions policy, advocate for the implementation of international AML/CFT standards, and combat financial crimes threats. Treasury Attaches play a key role in advancing these efforts. However, limited resources and the small footprint of the Attaché program forces Treasury to play a zero-sum game, essentially closing programs in countries that might still offer significant value when a new program elsewhere is required. The Treasury Attaché program covers only a small fraction of the overseas presence of U.S. law enforcement and other U.S. agencies. Allocating resources to place more Treasury Attaches in countries of strategic importance to the United States would be a welcomed step.

Technical Assistance

The Treasury Department, through its Office of Technical Assistance (OTA) promotes compliance with international standards and best practices, in particular the Financial Action Task Force (FATF) Recommendations, aimed at the development of effective AML/CFT regimes. OTA's Economic Crimes Team provides technical assistance to foreign counterpart regulatory, law enforcement, financial intelligence units, and judicial authorities tasked with ensuring a safe, sound and transparent financial system. These

efforts are particularly valuable when OTA works with countries of strategic importance to the United States. OTA's approach entails strengthening and integrating the work of the entire spectrum of AML/CFT stakeholders, but with a specific focus on the financial intelligence units as the lynch pin of an effective AML/CFT regime. As a result, this engagement enables FinCEN to engage in more productive information sharing relationships with FIU partners around the world.

Conclusion

The current AML/CFT landscape is complex and requires focused and sustained engagement by FinCEN with its domestic and global partners. While these proposals would enhance FinCEN's ability to increase industry engagement, without the proper resources to support these new requirements you will be placing additional burdens on an already resourced strained Bureau.

From my experience, one of the greatest challenges for FinCEN has been its ability to hire and retain mission critical staff. FinCEN is at a disadvantage because it competes for the same intelligence, policy and enforcement experts with the Federal Banking Agencies (FBA), Law Enforcement, and Intelligence Community that have either higher salaries, special hiring authority, or both. The proposal included in the discussion draft to allow the Director of FinCEN to set salaries at the levels of the FBAs will position FinCEN to better compete for quality candidates; however, I would also urge this Committee to consider providing FinCEN special hiring authority to recruit high quality candidates for mission critical, hard-to-fill positions. This would go a long way to ensure FinCEN is best positioned to achieve continuous collaboration and information sharing with the private sector to effectively address emerging challenges, while simultaneously identifying new approaches to combat financial crimes.

Thank you for the opportunity to testify today and for your continued efforts to strengthen Treasury and FinCEN's efforts to protect our financial system. I look forward to your questions.

Testimony of
Dennis M. Lormel
President & CEO
DML Associates, LLC

Before the
United States House of Representatives
Committee on Financial Services
Subcommittee on National Security, International Development, and Monetary Policy

At the Hearing "Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crimes"

March 13, 2019

Good afternoon Chairman Cleaver, Ranking Member Stivers and distinguished members of the Subcommittee. Thank you for holding this hearing and for giving me the opportunity to testify before you today. I applaud the Subcommittee for taking a leadership role in promoting and considering legislative enhancements to strengthen the Bank Secrecy Act (BSA). BSA reporting plays an integral role in safeguarding national security and furthering our economic wellbeing. Dating back to my days as a senior executive in law enforcement, and continuing as a private sector consultant, I have had the privilege to experience considerable interaction with Congressional members and staff regarding the effectiveness and efficiency of BSA reporting. This is one area in which I have continually witnessed bipartisan consensus regarding considerations to enhance BSA regulations.

You asked me to testify today and comment about three legislative proposals. The first is a discussion draft "to make reforms to the Federal Bank Secrecy Act and anti-money laundering laws, and for other purposes." The second, the Corporate Transparency Act of 2019, addresses the issue of beneficial ownership. The third, the Kleptocracy Asset Recovery Rewards Act, establishes a rewards program involving foreign corruption cases. You also asked me to provide comments regarding proposed legislative reform. I will do so in reverse order. I would like to start by focusing on the purpose and challenges of the Bank Secrecy Act (BSA) and anti-money laundering (AML) reporting, in order to build on them to enhance the BSA/AML regime.

I have been engaged in the fight against money laundering, fraud, corruption, terrorist financing and other predicate offenses or specified unlawful activity for 46 years. Between my law enforcement experience and my private sector consulting experience, as a subject matter expert, I have developed a unique perspective regarding the benefits, burdens and challenges of the BSA. Having served for 31 years in the government, 28 years as a Special Agent in the Federal Bureau of Investigation (FBI), I was the direct beneficiary of BSA reporting. Now, having been in the private sector for 15 years, working as a consultant and subject matter expert, primarily with the financial services industry, I have become sensitive to the burdens and challenges of BSA reporting encountered by financial institutions. Those

burdens and challenges are driven in part by regulatory requirements and expectations, as well as by the lack of consistent feedback mechanisms from law enforcement regarding the value of BSA reporting. Make no mistake, BSA reporting is essential to law enforcement's ability to defend our national security and the economy from the threats posed by bad actors.

My government investigative and private sector consulting experience has provided me a unique opportunity to understand and appreciate two very distinct perspectives regarding the BSA. Two of the principal stakeholders of the BSA are law enforcement and financial institutions. Putting this in the context of the flow and utilization of financial information, law enforcement is the backend user and beneficiary of BSA data. Financial institutions serve as the frontend repository and custodian of financial intelligence. Financial institutions also serve the critical function of being the monitor for identifying and reporting suspicious activity and other BSA data to law enforcement. Simply put, law enforcement uses BSA data to predicate or enhance investigations from a tactical standpoint. Law enforcement also uses BSA data for strategic purposes. From a simplistic standpoint, the flow of BSA data that is continuously filtered to law enforcement is invaluable. When you layer the complexities of regulatory compliance requirements and expectations over the monitoring and filtering process financial institutions must follow, the effectiveness and efficiency of BSA reporting from the frontend monitor to the backend beneficiary, becomes flawed.

The BSA/AML environment is fraught with much inefficiency, but the system works. Law enforcement consistently receives valuable intelligence from BSA data. The challenge is that the BSA system can and should be much more effective and efficient. In this regard, I commend the Subcommittee for dedicating the time to consider measures to strengthen BSA related regulations. An informed and thoughtful discussion about various mechanisms to strengthen the BSA/AML environment and to diminish the illicit flow of funds is in our best interests as a nation.

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

As noted in the introduction of the BSA, "the implementing regulations under the BSA were originally intended to aid investigations into an array of criminal activities, from income tax evasion to money laundering. In recent years, the reports and records prescribed by the BSA have also been utilized as tools for investigating individuals suspected of engaging in illegal drug and terrorist financing activities. Law enforcement agencies have found CTRs (currency transaction reports) to be extremely valuable in tracking the huge amounts of cash generated by individuals and entities for illicit purposes. SARs,

(suspicious activity reports) used by financial institutions to report identified or suspected illicit or unusual activities are likewise extremely valuable to law enforcement agencies". This statement is a true reflection of BSA reporting. However, there is a troubling backstory about perceived regulatory expectations that have resulted in systemic inefficiencies.

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

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

In the aftermath of the terrorist attacks of September 11, 2001 (9/11), as a senior executive in the FBI, I testified before the House Financial Services Committee on October 3, 2001. One of the issues I was asked to address was what the FBI considered as vulnerably or high risk areas in the financial services sector. I testified that wire transfers, correspondent banking, fraud and money services businesses were the biggest areas of vulnerability to the financial services industry at that time. As a consultant, I testified at a hearing before the House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence on May 18, 2012. During that testimony, I repeated and refined my October 3, 2001 testimony about the vulnerabilities of wire transfers, correspondent banking, fraud and money laundering. The refinement I made was that I placed the vulnerabilities into two categories: crime problems and facilitation tools. I stated that the most significant crime problems we then faced were fraud and money laundering. I identified the key facilitation tools used in furtherance of fraud and money laundering as: wire transfers, correspondent banking, illegal money remitters, shell companies and electronic mechanisms.

Today, March 13, 2019, I believe the most significant crime problems we face continue to be fraud and money laundering. Most, if not all, other predicate offenses or specified unlawful activities contain elements of fraud and require money laundering. The key facilitation tools used in furtherance of fraud

and money laundering continue to include: wire transfers, correspondent banking, illegal money remitters (informal value transfer systems), shell companies (beneficial ownership) and electronic mechanisms. I find it quite striking and troubling that the same vulnerabilities we face today regarding our financial services industry are the same vulnerabilities we faced in October 2001.

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

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

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

One of the inherent disadvantages we have in our financial system and AML environment is that we are reactive. Criminals and terrorists have the advantage of being proactive. Our ability to add innovative ideas and proactive measures to an otherwise reactive system can achieve impactful investigative results. In fact, there have been recurring innovative and proactive law enforcement investigations. I speak from firsthand experience when I talk about developing proactive techniques. I can point to specific proactive law enforcement initiatives following 9/11 that were the direct result of innovative public and private sector partnerships. My emphasis here is we can be innovative within the current framework. We can also improve the current landscape through enhancements to encourage and/or incentivize innovation. For example, financial institutions conduct baseline transaction monitoring to alert to anomalies that can lead to identification of suspicious activity. By developing rule sets and scenarios that are targeted to specific transactions or financial activity, we are more likely to identify specific or targeted suspicious activity regarding specific crime problems such as human trafficking. Financial institutions are reluctant to employ targeted monitoring initiatives because of concern for the potential regulatory expectations or other perceived impediments such innovative thinking could incur.

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

Throughout my career, I have worked closely with financial institution AML and fraud compliance professionals. I have the utmost respect for their dedication and commitment to protecting the integrity of their financial institutions and for identifying the misuse of the financial system by bad actors. Next to my former law enforcement colleagues, I hold my friends in AML and fraud compliance in the highest regard. It is important to note that the BSA shortcomings we face are systemic problems caused by multiple factors and not by groups of individuals.

The most important BSA report is a SAR. In most instances, the biggest regulatory compliance breakdown resulting in some sort of enforcement or regulatory action is the failure to file SARs or to adequately file SARs. I cannot underscore enough that law enforcement is the direct beneficiary of SARs. Regardless of systemic inefficiencies, law enforcement consistently benefits from SAR filings. SARs are used tactically to predicate and/or enhance criminal investigations. SARs are also used strategically for analytical purposes. When attempting to measure effectiveness and efficiency of SAR filing, we cannot solely rely on the percentage of SARs filed versus the number of SARs used to predicate or enhance an investigation. We must also factor in how SARs are used strategically for trend analysis and analytical purposes. Finding accurate metrics to determine the effectiveness and efficiency of SAR filing is extremely difficult.

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

Following my retirement from the FBI and as I have gained more of a financial institution perspective, based on my experience as a consultant, I have become more sensitive to the perceived lack of feedback to financial institutions from the Financial Crimes Enforcement Network (FinCEN) and law enforcement

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

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

One of the most important issues where law enforcement should be the primary stakeholder to potential legislation is the issue of CTR and SAR reporting thresholds. Since SARs were first implemented, the reporting thresholds have been the same. Periodically, banking associations and financial institutions have recommended that reporting thresholds be adjusted to account for inflation. I strongly believe that CTR and SAR reporting thresholds should remain as they are. Law enforcement would lose valuable financial intelligence if thresholds are raised. This is especially true for terrorist financing, where our primary threat is from homegrown violent extremists involved in more minimal financial flows.

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

When considering new legislation or enhancements to current legislation, we need to assess the theoretical and practical applications of the law. This is where understanding stakeholder perspective can be important. What needs to be remembered and consistently applied is that BSA reporting requirements are intended to provide law enforcement with information to support investigations. Either real or perceived, financial institutions are frequently frustrated by the difference between regulatory requirements and regulatory expectations. The difference between required and expected can impede the practical application of providing law enforcement with information in order to satisfy perceived regulatory expectations.

It is interesting that two of the Bills under consideration by the Subcommittee deal with Kleptocracy and beneficial ownership. Kleptocracy is a form of public corruption where political leaders embezzle or misappropriate State funds. Frequently, they do so through gatekeepers and shell companies by disguising there beneficial ownership of the ill-gotten gains.

Kleptocracy Recovery Reward Act

Kleptocracy is a serious problem that undermines the stability of victim countries. The FBI recently announced the formation of a fourth international corruption squad to address the national impact of foreign bribery , kleptocracy, and international anti-trust schemes. Squads are based in Los Angeles, Miami, New York and Washington, D.C. Frequently, Kleptocrats rely on gatekeepers and shell or front companies to move and hide their plunder.

According to the FBI, among the most challenging money laundering investigations are those targeting gatekeepers, which may include bankers, brokerage houses, trust companies, attorneys, accountants, money managers, notaries, or real estate agents. The FBI's International Corruption Squads investigates these international business people who provide professional services to illicit actors wishing to disguise the source or nature of the money. The Kleptocracy Asset Recovery Reward Act is a good bill. It would serve as a viable tool for law enforcement to develop evidence for prosecution, as well as identify, recover and repatriate stolen funds to victim countries.

Corporate Transparency Act of 2019

As a former law enforcement executive, I have been advocating beneficial ownership legislation since 2012. Beneficial ownership through shell companies has been a series vulnerability to our financial system and an impediment for law enforcement for much too long. I encountered my first case involving money laundering in 1975, as a Revenue Agent in the Internal Revenue Service working with the Organized Crime Strike Force in Newark, New Jersey.

One facilitation tool that consistently garners Congressional attention is the issue of beneficial ownership. Year after year, potential bills are introduced regarding beneficial ownership. I strongly encourage the Subcommittee to support this beneficial ownership legislation as an enhancement to the BSA. Throughout my law enforcement career, I dealt with the challenge of shell companies and identifying true beneficial owners.

I believe that the best case scenario would be to collect beneficial ownership at the point of incorporation by the Secretaries of State. Secretaries of State have consistently been resistant to this. A good case alternative is presented in this legislation. We need to have a central repository for beneficial ownership. FinCEN is the best alternative available for collection of beneficial ownership information. As with BSA data, FinCEN will be a viable conduit for law enforcement for obtaining beneficial ownership information. By collecting beneficial ownership information, and making it available to law enforcement, valuable investigative time will be saved.

On May 11, 2016, FinCEN issued Customer Due Diligence Requirements for Financial Institutions (the CDD Rule). The rule went into effect in May 2018. The rule strengthens existing customer due diligence (CDD) requirements and requires banks to identify and verify the beneficial owners of legal entity customers. From a practical perspective, with FinCEN collecting beneficial ownership information, the burden of the CDD requirements on financial institutions would be lessened, especially if FinCEN establishes an identification verification mechanism.

I firmly believe that beneficial ownership legislation is necessary and long overdue. My only concerns about this legislation are the potential differences or inconsistencies between information provided to Secretaries of State at point of incorporation and information provided to FinCEN at point of registration. In addition, from a practical perspective, I'm concerned about FinCEN's capacity to collect and disseminate beneficial ownership information in an effective and efficient manner.

Discussion Draft to Reform BSA/AML Laws

I believe the Discussion Draft sets the foundation for meaningful enhancements to BSA/AML legislation. Again, I'd like to commend the Subcommittee for your leadership role in considering legislative measures to enhance the BSA. Two important themes that resonate throughout the draft are information sharing and partnerships. Throughout my career I have been a strong advocate for sharing information and for establishing public-public and public-private partnerships. Meaningful partnerships lead to proactive and innovative initiatives. Without question, the more we can do to establish practical and sustainable information sharing mechanisms and viable partnerships, the more effective and efficient BSA reporting will become. Going back to considering financial institutions as being facilitation tools or detection mechanisms for fraud, money laundering and other predicate offenses, the end result of more effective and efficient BSA reporting is minimizing facilitation and maximizing detection.

I would like to offer some observations about select provisions in the Draft Discussion:

- Sections 103 and 104 regarding Civil Liberties

As an FBI Agent, I took an oath to uphold the Constitution and protect Civil Liberties. Any BSA/AML enhancements, particularly where law enforcement gains authority, must ensure we protect Civil Liberties.

- Section 109 FinCEN Exchange

In theory, the FinCEN Exchange is a good idea. Facilitating the public-private sharing of information between financial institutions and law enforcement is extremely important and valuable. From a practical perspective, FinCEN is not a law enforcement agency; and this type of public-private partnership may be better served directly between financial institutions and law enforcement. There

are examples of very productive law enforcement led working groups with financial institutions that facilitate productive information sharing.

- Section 111 De-Risking Report

There are adverse consequences for de-risking. De-risking is a concern and challenge for law enforcement. When individuals and/or entities are de-risked, the prospect of them going underground and losing transparency is problematic. It should be pointed out that a cause for de-risking is the result of regulatory expectations versus regulatory requirements. Real or perceived, financial institutions are influenced by how they believe the regulators view their risk management and determinations of what presents risk.

- Section 201 Sharing of Suspicious Activity Reports Within Financial Groups

Permitting financial institutions to share SAR information as articulated in the section would ultimately be beneficial to law enforcement.

- Section 202 Training for Examiners on AML/CFT

Training examiners for AML/CFT is a good idea. I believe this training should go beyond AML/CFT to include perspective training. What I mean by perspective training is that examiners may not know how financial institution employees think or operate. Bank operational training should be required in addition to AML/CFT training. Terrorist financing is extremely difficult to identify. From a practical perspective, it is extremely difficult for anyone to understand or identify terrorist financing.

- Section 203 Sharing of Compliance Resources

Sharing resources, especially by smaller financial institutions would have a tremendous cost benefit and could enhance the effectiveness and efficiency of BSA reporting.

- Section 206 Section 314(a) Improvements and Section 207 Sharing of Threat Pattern and Trend Information

Information sharing through Section 314 is extremely important. Any enhancements to improve information sharing would result in more effective, efficient and qualitative BSA reporting. In Section 206, from a practical perspective, it would be challenging to maintain current law enforcement points of contact. However, it would be a worthwhile effort. In Section 207 sharing typologies on emerging money laundering and counter terror financing threat patterns and trends would be extremely beneficial. One model for this type of information sharing exists on a small scale. The FBI's TFOS had an outstanding Bank Security Advisory Group where typologies were shared and acted upon. There are other examples of similar working groups, especially in the area of Human Trafficking.

- Section 214 Application of Bank Secrecy Act to Dealers in Arts and Antiquities

Arts and antiquities have for a long time, quietly been a mechanism for hiding ill-gotten gains and serving as a money laundering tool. This was never more evident than with the theft and black market sales of art and antiquities from Iraq and Syria by the Islamic State to help support their terrorist organization.

Beyond arts and antiquities, exemptions from BSA/AML requirements should be lifted from Non-Bank Financial Institutions to include persons involved in real estate closings and settlements and sellers of vehicles, including automobiles, airplanes and boats.

In addition to arts and antiquity dealers, consideration should be given to include gatekeepers, especially formation agents, who form corporations and trusts.

- Section 215 Revision to Geographic Targeting Order

Geographic Targeting Order referred to for real estate should be expanded. It should apply nationwide and consideration should be given to making it permanent.

- Section 301 Encouraging Innovation in BSA Compliance

Innovation is extremely important and should be broadly encouraged.

Once again, I thank the Subcommittee for the opportunity to testify. I look forward answering your questions or providing further clarification.

Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crime

Subcommittee on National Security, International Development, and Monetary Policy
(Committee on Financial Services)

Amit Sharma
Founder and CEO, FinClusive
March 13, 2019

Introduction

Chairwoman Waters, Ranking Member McHenry, and distinguished members of the House Financial Services Committee, I am honored by your invitation to testify before you today.

In particular, I am grateful for the opportunity to testify in support of several initiatives this committee and Congress are pursuing to modernize the anti-money laundering / counter-terrorist financing (AML/CFT) regime of the United States, and the attendant issues emanating from the U.S. Bank Secrecy Act (BSA) to strengthen the integrity of our financial system, and importantly recognizing the value in new technology capabilities and the innovation taking place within and outside the traditionally regulated financial services industry that can also drive financial inclusion.

Congressional efforts to strengthen and codify engagement between the regulatory community and the financial services industry – taking into consideration the growth in particular in the non-bank financial institutions sector and exploding financial technology (fintech) and regulatory technology (regtech)—is of paramount importance given the ever changing nature of technology and the applicability of some of these important advancements to not only aid in strengthening regulatory compliance associated with the BSA and broader AML/CFT, but also importantly and significantly, such efforts can and would support financial inclusion as doing so has a direct benefit to our collective national security.

Several important trends are important to recognize as we look at the evolution of financial services and the manner and methodology employed by many individuals and entities to financially and commercially transact between each other.

The first is the recognition that there has been, and continues to be, an exponential increase in financial intermediation taking place outside traditionally covered or regulated channels. These include, but are not limited to: peer to peer (p2p) transactions, the extension of credit and provision of lending by institutions (or individuals) to other institutions and individuals directly and without regulated intermediaries, the growth in mobile (phone and web-based) banking, the increasing 'digitization' and 'tokenization' of financial instruments and assets (e.g. cash, stored value, marketable securities, etc.) and the emerging and growing 'crypto-currency' sector. Under any rubric, we are seeing financial innovation blossom, where traditional financial market participants—and increasingly non-traditional entrants, are innovating in both the form of, and manner in which, counterparties are engaging in modern financial engagement, asset building and wealth creation. Some of these efforts hold tremendous promise, while others may present addressable risks, and still others, unfortunately, look to deliberately circumvent or avoid the basic fundamentals of prudential financial intermediation.

Secondly, the growth of financial activities *outside* of traditionally regulated channels is also noteworthy and provides tremendous opportunity to increase access for the globally underserved, unbanked, underbanked and those otherwise financially excluded. Such efforts have understandably given financial regulatory agencies pause as nonbank entities and other non-traditional finance companies have emerged into the financial services sector. Technology, social media, online/e-commerce retailers, corporate entities with large recurrent user/consumer populations and others with large and growing affinity groups, are increasingly realizing the commercial potential of providing financial products and services through their infrastructure and existing networks. While these efforts provide great promise in reaching traditionally underserved/excluded populations, doing so without essential safeguards to safety, soundness, consumer protection and financial system integrity could indeed lead to broader and systemic

risks or the facilitation of illicit activities to which the BSA and other US regulations governing AML/CFT are intended to address.

Finally, since the tragic events of September, 2001, and exacerbated by the credit and financial crisis of 2008, a growing body of regulations and financial oversight rules have understandably caused consternation among financial market participants – traditional and non-traditional alike – working to adhere to a growing body of regulatory and compliance requirements. With an average governance/risk/compliance (GRC) spend of 25% of their operating budgets, global banks have faced the 'economic' reality of servicing otherwise labelled "high perceived compliance risk" individuals and entities or suffer the consequences of regulatory fines and punitive measures for lack of demonstrably strong AML/CFT controls. By no means do I sympathize with those institutions that have willfully chosen to turn a blind eye to money laundering, sanctions evasion, terrorist financing and other illicit activity, or underinvested in foundational AML/CFT controls, however, we are indeed seeing the consequence of growing regulation and the associated economic consequences stemming from "de-risking" or the jettisoning of business otherwise considered "high perceived compliance risk." Such efforts have unfortunately fallen disproportionately on those constituents –individuals and entities—whose financial engagement and access serve as essential to building economic resilience, and sustainable financially responsible behaviors—the US and global poor, international remittances, humanitarian assistance and charitable works, and international correspondent banking, among others.

The manner in which financial exclusion has grown in the last two decades, and/or the myriad and diverse reasons that exacerbate financial exclusion, are far beyond this testimony, however, the attendant risks of 'de-risking' due to ongoing AML/CFT uncertainty amidst a growing trend of nontraditional and technology-led initiatives to provide financial services, behooves us to look at these market participants in a fundamentally new light – and find ways in which new technology can in fact drive financial inclusion and strengthen financial sector integrity in tandem.

Supporting Innovation and Technology Advancement in Financial Sector Integrity and Inclusion

Financial innovation has continued to grow exponentially in the last decade. The advent of new technologies such as mobile and digital banking, alternative payments, advanced analytics (including artificial intelligence (AI) and machine learning) and distributed ledger technologies (DLT), have expanded opportunities never before afforded to financial market participants. Importantly, such technologies give us ability and insight in reducing friction and oftentimes redundant processes (especially as related to know-your-customer / customer-due-diligence (KYC/CDD) and ongoing monitoring), dramatically increasing analytics and processing speeds within a traditionally 'man-hour'-centric compliance environment (aiding investigations, law enforcement coordination and reporting), and improving information sharing by and between financial intermediaries, regulators and law enforcement while protecting essential data and personal identifying information (PII).

For example, AI and machine learning capabilities have the potential for driving enhanced and bespoke analytics related to targeted investigations or specific illicit finance typologies (e.g. human trafficking-related financial activities or sanctions evasion) in financial institutions. Many new regulatory technologies have added tremendous value to financial institutions to ensure compliance officers and teams the ability to carry out 'look backs,' suspicious transaction reviews, enhanced or targeted investigations and the like, to specific money laundering and illicit finance typologies where human-centric reviews and analysis can be both cumbersome and expensive endeavors.

More routinely, however, distributed ledger technology (DLT) has emerged as an additional potential value additive capability that has tested application to both driving secure, cost-efficient payments as well as enhanced compliance to meet AML/CFT goals and obligations. DLT is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. There is no central administrator or centralized data storage. Blockchain is one form of DLT that uses independent computers (referred to as nodes) to record, share and synchronize transactions in their respective electronic ledgers (instead of keeping data centralized as in a traditional ledger). There are several characteristics of DLT – in particular, blockchain, that facilitates stronger compliance and inclusion in tandem:

- Distributed: Blockchain creates a shared system of record among business network members – eliminating the need to reconcile disparate ledgers.
    - Transactions via blockchain networks can be constructed and held throughout the network and ultimately accessible via secured channels for audit and tracking purposes. This can be very helpful with respect to both client and transaction-related data.
- Immutability: Consensus is required from all members and all validated transactions are permanently recorded. Even a system administrator cannot delete or alter a transaction.
    - Transactions can be recorded for auditability and transaction monitoring. The near-real-time settlement functionality can facilitate near real-time payments between counterparties vs 3-5-day settlement times via traditional channels. Transaction history and specifics cannot be altered once inputted. The immutability of the ledger can therefore benefit ongoing client and transaction monitoring real time – increasing process efficiencies and reducing costs associated with compliance activities.
- Permissioned: Each member of the network must have access privileges and information is shared only on a need-to-know basis between network nodes.
    - Information regarding the transaction origin and recipient can be permissioned between nodes for easy and secure access without disclosure to third parties without permission, and be leveraged for verification/validation purposes, managing against fraud, and assist network participants in a common financial ecosystem.

While the applications for DLT are far reaching, one can easily see where it can add value in particular to underserved/excluded markets as well as in the furtherance of AML/CFT goals. Responsible and disciplined application testing and deployment of such technology alongside regulatory oversight would indeed pay dividends to the industry, regulators and law enforcement alike.

Codifying Regulatory Commitment to Financial and Regulatory Technologies

As an initial observation, I commend the regulators and their joint statement made in December, 2018 to support innovative efforts to combat money laundering and terrorist financing. That statement, while necessarily not an endorsement of any specific kind or type of technology, reinforced to both the traditional banking community as well as the growing fintech and non-bank financial services community of the important role new technological advancements can make in streamlining AML/CFT processes, ensuring cost effective and frictionless approaches for financial services participants of all types – with and through banks and non-banks alike – and in effort to keep the financial system safe and secure from illicit activities.

While the statement was an important start, a statement alone is not sufficient in delivering practical and tested solutions to the financial services industry without proactive, ongoing, dedicated and funded support by financial regulators directly. Moving to make this innovation guidance more permanent

through concrete mechanisms by individual regulators and across them collectively, and that directly engage both financial services institutions AND technologies in their application to AML/CFT, will pay important dividends. It is worth noting that in large part, fintech companies and other non-traditional nonbank financial institutions very much want for their operations and activities to comport with essential financial system integrity safeguards, and that their efforts meet the attendant goals of driving both commercial opportunities as well as ensure risk is appropriately understood and managed within the financial sector. While there are indeed those companies, rogue individuals and efforts in non-traditional financial service channels that deliberately look to avoid regulatory scrutiny or oversight, my comments today reflect instead the broader majority of enterprises looking to provide financial intermediation, products and services in a way that enhances transparency and that are attendant to the inherent compliance risks associated with the financial sector.

Connecting Financial Inclusion to Ongoing AML/CFT Modernization and Financial Sector Resilience

As discussed above, we encourage stronger, codified and financially and legislatively supported private-public cooperation in the application of new technology to financial system integrity – in particular in the modernization of the United States AML/CFT regime. There are several ways we encourage this 'permanency' of the December statement by the regulators; below are several concrete and practical efforts that would indeed be welcome by industry participants – whose goals are indeed shared to drive a more transparent and safe financial system that is also inclusive.

- Creation of Dedicated Technology / Innovation Units and Coordination Centers:
  - We encourage Congress to mandate, authorize funding for, and support the creation of dedicated technology/innovation centers driven individually by regulators – in particular the Office of the Comptroller of the Currency (OCC), the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of Federal Reserve, and the National Credit Union Association (NCUA). Each of these regulators differ in both their mandate and jurisdiction, and as such, have a unique perspective in understanding the specific challenges faced by financial sector participants covered by their oversight and subject to their examination activities. Importantly, by having dedicated technology and innovation units resourced and led, at the explicit direction of a director/ senior leadership to engage in outreach, assessment, and testing (both in "beta" and "in-market") of new technological applications, companies shall benefit from the practical feedback and impact to specific regulatory issues for which covered institutions can/would be examined. In this way, such testing and practical deployment can be managed in the context of regulatory requirements vs outside of their purview or merely in response or avoidance of the same.
  - Furthermore, as existing or newly regulated institutions adopt new technology processes, such centers would be the natural place for those institutions to effectively time and coordinate the management of parallel processes in coordination with their functional regulators to ensure essential safety/soundness measures, redundancy practices and other risks are taken into consideration as new technology is rolled into live market production, and while others are ceased. This process would give tremendous comfort to new market entrants, non-traditional financial services companies – in particular nonbank FIs and fintech companies – as they look to participate in what is otherwise interpreted by many as a 'gotcha-oriented' financial regulatory environment. We are not necessarily offering or suggesting that such efforts should come with guaranteed safe-

harbor or immunity measures, but instead an affirmation that such efforts do not put undue or unknown regulatory risks on financial market participants—traditional and non-traditional.

- Enhancing Coordination/Engagement with Field Examiners:
  - Regulators should consider ensuring appropriate engagement within these centers by their field examiners. There is ongoing reluctance on the part of financial market participants and technology companies of revealing new capabilities to regulators for fear that examiners will remain steadfast to oversight and audit that serve to discourage or dismiss innovative processes or applications. Regardless of the many proactive outreach efforts by new market entrants (e.g. non-banks and fintech companies to federal financial regulators), too often there remains a disconnect between well-intentioned sector participants in bringing new technologies and methodologies to market – both within their own enterprises and as solutions to regulated financial institutions—and uninformed field examiners have often approached their work in *a tick-the-box* fashion for assessing regulatory adherence. This has served to significantly cool outreach by fintech and regtech companies, even when their commercial solutions can serve to benefit banks and other regulated financial institutions to better carry out their AML obligations more cost effectively and in keeping with the spirit of the BSA. Importantly, many solutions have benefits of application to AML/CFT among non-traditional/non-bank entities, whose activities to date fall outside the purview of federal regulators.
  - Reinforcing that there is senior leadership dedication to innovation and new technology applications would create an additional linkage between Washington DC-based policy makers and regulators with field examiners, such that their audit and review of covered institutions take into consideration measured approaches to meet AML/CFT obligations in robust ways. We would recommend that an explicit goal of senior leadership charged with management and oversight with these centers engage field examiners in the process of assessment, review and deployment of these new technologies in advancement of AML/CFT and other oversight goals.

- Enhancing Regional Efforts and State Coordination:
  - Increasingly, individual states are taking a lead, often through their individual Departments of Financial Services – or equivalent agencies – to liaise with industry by welcoming new technology innovation and coordination with financial industry participants. These efforts, while very welcome in particular to bank and non-bank financial institutions domiciled in those respective states, many find themselves potentially engaging in otherwise welcome testing and deployment of new reg-tech or fintech applications at the State level, but potentially running afoul or at cross-purposes with federal regulatory requirements. The simple reality that nonbank financial institutions, such as many money service businesses and money transfer operators (MSBs/MTOs), fintech companies, digital asset exchanges and others in the growing crypto-currency sector must ensure individual state-by-state registration in tandem with potential US federal oversight from one or more of the aforementioned regulatory agencies can be both commercially and regulatory burdensome.
  - Further, ongoing legal challenges between individual states and one or more federal regulators has served to exacerbate these challenges for companies working diligently to ensure regulatory compliance but could potentially be reinforcing processes that may be in conflict between one or more State or Federal agency regulations. We would

encourage that established innovation and technology centers provide for regional and state-to-state coordination as new market participants would be able to approach these efforts with similar good faith cooperation with both state and federal-level authorities in tandem. As such, we encourage that these centers be staffed and driven by regional sub-heads or similarly constructed senior leadership that would include regulatory professionals outside of Washington DC. Ensuring augmented staffing at each regulatory agency comes with appropriate senior level assignments and power will further reinforce their ability to speak with appropriate authority in representation of their respective agency's position and in furtherance of overall US policy goals.

- Strengthening Coordination By and Between Regulatory Agencies:
  - Alongside individual agency-led technology and innovation units, we encourage by mandate that agencies work within existing frameworks including the Financial Stability Oversight Council (FSOC) and the Federal Financial Institutions Examinations Council (FFIEC) processes for sharing knowledge, practical applications of new technology and reporting of such activities to Congress on a regular and timely basis.
    - Prior to the formation of the FSOC, no single regulator had responsibility for monitoring and addressing overall risks to financial stability, which the US is comprised of a myriad of financial firms operating across multiple markets. The formation of this important council was to facilitate regulatory coordination and information sharing that can better inform financial services policy development, consolidate the supervision of nonbank financial companies in particular, regardless of their form, and designated systemic financial market utilities and systems.[1] These goals are not only noteworthy in terms of their practical utility, but the FSOC also helps streamline activities in the US finance and banking community amidst an already crowded and often confusing landscape of cross-functional state and federal regulators operating across jurisdictional authorities. As we continue to see the growth of financial intermediation activities undertaken by non-traditional institutions and non-bank financial services companies, the FSOC can and should be a consolidation of authorities and oversight, and importantly a coordination and information center that should govern assessment and reporting of innovation and new technology development and related deployment in the industry. The FSOC could very well be, in form and function, the go-to Council for companies providing new technology applications that impact essential financial services activities, including payment processing and settlement, AML/CFT compliance and other activities impacting safety, soundness and consumer protection. In addition, innovative non-bank and fintech efforts that drive greater financial access can and should be shared through the FSOC to address important development goals and rules including those

[1] https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc

related to community development finance and the Community Reinvestment Act (CRA) among others.

- The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by a number of the core federal financial regulators, including the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). Importantly, in 2006, the State Liaison Committee (SLC) was added to the Council as a voting member, which brought to the Council representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).[2] This Council too, can and should serve as a coordination center for the sharing of information and insights regarding technological innovation and applications into the financial services sector by both bank and non-bank entities alike. With ongoing confusion in non-bank and fintech circles as to the manner in which to consolidate outreach between state-based and federal regulators, reporting up and to the FFIEC of and by individual regulator-led innovation and technology centers will prove invaluable to the sector.

- Regular reporting by individual regulators to the FSOC and FFIEC of specific technology applications driven to specific AML/CFT compliance goals and BSA obligations, and/or the application of new technologies in the delivery of specific products and services (e.g. secure payments, alternative lending, mobile banking, etc.) would be essential for regulators to share knowledge and application of such technologies across the industry. Such efforts would also reinforce and aid in consistent oversight and examination mechanisms across multiple regulatory authorities—at both the federal and state levels—as well as help codify new rulemakings impacting industry as related to AML/CFT or other important areas.

It is important to note that these efforts must not be limited to their mere establishment by Congressional mandate. The seriousness of these efforts needs to be reinforced with adequate funding support, including the increase in staffing numbers and pay-level for individuals charged with managing these regulator-led innovation and technology centers. Ensuring equity of pay and support between regulators and equality of opportunity across regions in the US for innovation center activities will serve to limit internal regulatory arbitrage and facilitate the recruitment, management and retention of participating professionals, who will feel empowered to speak and act on behalf the agencies they represent. Such support shall also allow for industry participants to be incentivized to participate in targeted innovation efforts and the practical deployment of new technologies to modernize AML/CFT activities by both bank and non-bank financial institutions – including the increasing efforts by a number of smaller, community-oriented regional and sub-regional financial institutions to form value-added partnerships with fintech and regtech companies to remain competitive in an increasingly evolving financial services sector. As stated above, such efforts shall pay dividends to other important policy goals

[2] https://www.ffiec.gov/

supporting inclusion, community based finance, and building economic resilience – all of which directly contribute positively to our financial integrity and AML/CFT goals and consequently to our national security priorities.

Conclusion: Financial Inclusion as a Matter of National Security

I am hopeful that my recommendations offered above will assist the Committee in considering further ways to strengthen this proposed legislation and drive greater public-private sector cooperation – in particular as it relates to innovation and the testing and deployment of technology to strengthen and modernize AML/CFT efforts and importantly drive financial inclusion. More importantly, I am hopeful that my testimony will help address the doubts and concerns that have prevented prior Congresses from adopting similar legislation in the past.

In sum, we must look at the tools we have created to drive financial inclusion, community-based financial engagement, and risk-based approaches to financial facilitation that ultimately bring more activity to regulated financial channels. New technologies, including in advanced analytics, mobile and digital banking and distributed ledgers, can serve to provide additional financial engagement highways that are more easily accessible and afford the essential protections (in both privacy and personal data as well as personal financial assets) that remain inherent challenges to many financially underserved and excluded parties from securely engaging the financial system. These same technologies can serve to dramatically decrease the friction, redundancies and inefficiencies of the AML/CFT activity set while preserving the essential controls inherent in facilitating safe and secure financial intermediation.

The United States has one of the most effective AML/CFT regimes in the world. As we have relied more on this regime to address various threats to our national and collective security, our efforts are increasingly undercut by the misinformed and false binary choice we have brought to driving financial inclusion vs protecting our financial system from abuse by illicit actors. New technologies at work today, have the power and capability of addressing "actual" vs "perceived" risk, strengthen coordination among and between financial market participants and intermediaries (both traditional and non-traditional) as well as financial regulators and law enforcement, and provide gateways for access in ways that can strengthen financial system controls for the many licit and otherwise legitimate activities and participants we need the system to serve, while strengthening the ability to identify and root out illicit activities. These gateways and technologies can bring down barriers to access while preserving essential safeguards for traditional and non-traditional financial market participants. The strength of United States globally is founded on, among other things, a strong and unparalleled financial and economically resilient foundation; extending this to the 25+% of the country's financially underserved and excluded—and ultimately to the 2.5-3B people globally underserved/excluded—ultimately serves to drive overall financial system integrity and security moving forward, but also underpins our collective national security at home and abroad.

Gary M. Shiffman, Ph.D.

"An Economist's View on Technology in the future of BSA/AML"

Before the Subcommittee on National Security, International Development, and Monetary Policy

House Committee on Financial Services

United States House of Representatives

March 13, 2019

Introduction

Distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss the important topic of countering financial crime.

I am an Economist who focuses on technology, behavioral science, and people who do bad things such as money laundering, human and drug trafficking, terrorism, fraud, and corruption. I am the CEO of Giant Oak, a software company focusing on making screening easy. I teach courses at Georgetown University on organized violence. I am also a Navy Gulf War veteran and I have served in a federal law enforcement agency.

I have no interest in AML compliance for compliance sake; I tell you about my background to emphasize this point. I come to the sub-committee today as a technologist to argue that we can and must do better at combatting money laundering, trafficking, terrorism, and other illicit acts.

Background

Our current AML regime requires radical reform. We are inefficient. According to the United Nations, "The estimated amount of money laundered globally in one year is 2 - 5% of global GDP".[i]

At the same time, spending to combat money laundering and the financing of terrorism (AML/CFT) exceeds $7 billion[ii] in the US and $25 billion[iii] globally. However, of the approximately 2 million Suspicious Activity Reports (SARs) generated by today's AML systems for FinCEN, less than 5% provide value.

In short, it appears we have an AML regime that compels the industry to spend billions of dollars, generates mostly useless data, and counters less than 1% of the problem.

We must do better. We can begin by harnessing available technologies and focusing them on supporting our law enforcement and national security professionals.

Machine Learning

When I say technology, I refer primarily to Machine Learning (ML), Artificial Intelligence (AI), and the application of behavioral science to data analytics. I define Machine Learning as the training of computers to identify patterns in data.

If you imagine a spreadsheet with millions of rows and columns, it is not hard to believe that patterns exist somewhere in the data, but because our human eyes and brains cannot find those patterns, none of us will ever again live in a world without Machine Learning.

By utilizing Machine Learning, we can teach computers to find and reveal the patterns for us.

Any future AML regime must include Machine Learning, and a future BSA/AML regime without without Machine Learning seems unbelievable. So what shall we do?

How to Create the Best *Machine* to Detect and Deter Financial Crime

To build the best *machine* to detect and deter financial crime, one needs good training data. Machines are literal. If you teach it to play chess, it will not learn to play checkers. The best *machine* on the planet for AML will be built by training it on the best AML data.

If we apply this to financial crimes, the vulnerabilities and opportunities are obvious: government agencies know which SARs provided the best quality information, but the banks do not, so they cannot train their tools properly.

The few banks using Machine Learning for AML today train their *machines* on previous years' SAR data. If more than 95% of past SARs were wrong, then these banks simply perpetuate inaccuracies (just more efficiently). However, with feedback from law enforcement, systems can learn and improve. This is where we need to bring the AML regime.

Call to Action

I do not want to end without raising a word of caution. Computers are powerful tools that can do both good and bad. As far back as the 1968 Stanley Kubrick and Arthur C. Clarke film *2001: A Space Odyssey*, we humans have understood the need to harness the computer.

To ensure we maintain the balance between risks and rewards of advancing technologies, I suggest three core principles for the subcommittee to consider as part of any reform or legislative proposal:

1. Encourage information sharing between law enforcement, financial institutions, and regulators. This will enable the sharing of priorities and training data for Machine Learning. This will also help regulators better judge the quality of the data

generated, and not just the volume. It will also provide tools for measuring biases in data.
2. Avoid opaque solutions where humans cannot understand the internal processes or outcomes of the *machines.*
3. Keep humans in the loop; let machines sort and filter data, but let humans adjudicate good vs. bad and right vs. wrong.

Closing

To close, Machine Learning already pervades our lives. Technology will increasingly enable regulated financial institutions to identify threats with increasingly precise measurements that will enhance security, protect privacy, and promote financial inclusion.

We spend billions today to generate mostly useless data and miss 99% of global financial crime. Law enforcement knows that better systems based upon existing technologies are available to generate good data and keep us all safer and more secure.

Thank you for your time, and I'm happy to answer any questions you may have.

---

[i] https://www.unodc.org/unodc/en/money-laundering/globalization.html
[ii] https://www.theclearinghouse.org/banking-perspectives/2016/2016-q3-banking-perspectives/departments/by-the-numbers-aml
[iii] https://www.prnewswire.com/news-releases/anti-money-laundering-compliance-costs-us-financial-services-firms-25-3-billion-per-year-according-to-lexisnexis-risk-solutions-300728586.html

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

March 13, 2019

The Honorable Emanuel Cleaver
Chairman
Financial Services Subcommittee on
National Security, International Development and Monetary Policy

The Honorable Steve Stivers
Ranking Member
Financial Services Subcommittee on
National Security, International Development and Monetary Policy

Dear Chairman Cleaver and Ranking Member Stivers:

On behalf of the American Gaming Association (AGA), I write to express our appreciation for today's Subcommittee hearing on *"Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crime."*

As a national trade association representing licensed commercial and Tribal casino operators and gaming suppliers supporting 1.8 million jobs across 40 states, AGA welcomes the opportunity to engage with the Subcommittee as we all work to foster the most robust and effective anti-money laundering (AML) programs.

Industry-wide, fostering a strong culture of compliance continues to take an increasingly prominent role across all corporate structures as AGA members make significant investments within their organizations to ensure compliance with the Bank Secrecy Act (BSA) and all applicable AML laws and regulations.

The AGA values its working relationship with the Treasury's Financial Crimes Enforcement Network ("FinCEN") – serving on the Bank Secrecy Act Advisory Group (BSAAG) and supporting FinCEN's efforts to enhance compliance with the BSA.

The industry's commitment to compliance is also illustrated in:

- AGA's Best Practices for AML Compliance[1]; and
- The Financial Action Task Force's (FATF) most recent U.S. Mutual Evaluation which applauded the gaming industry for having "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]

[1] American Gaming Association, 'Best Practices for Anti-Money Laundering Compliance' (January 2017), https://www.americangaming.org/wp-content/uploads/2018/12/Best-Practice-2017.pdf.
[2] Financial Action Task Force (FATF), Fourth Mutual Evaluation Report on U.S. Anti-Money Laundering and Counter-Terrorist Financing Measures (December, 2016), http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

As this Subcommittee explores potential modernization of the current AML framework, we respectfully urge your consideration of the following gaming industry reform priorities, which recognize the importance of ensuring effective AML compliance while also alleviating unnecessary industry burden:

- **Modernize BSA Reporting Thresholds:**
  - *Harmonize currency transaction reports and suspicious activity reporting (SAR) thresholds with inflation.*

- **Streamline the SAR Regime: Create Consolidated form for Structuring:**
  - *Create a "SAR lite" for structuring related offenses that streamlines the amount of required information, such as elimination of the detailed factual narrative.*

- **Enhance Feedback to Augment AML Priorities**:
  - *Utilize technology and data analysis capabilities to provide more real-time feedback and data on government and law enforcement utilization of industry BSA reports.*

We thank the Subcommittee for your attention to these important matters and look forward to future engagement opportunities.

Sincerely,

Christopher Cylke
Vice President, Government Relations

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

Credit Union National Association
CUNA

Jim Nussle
President & CEO

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

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

March 13, 2019

The Honorable Emanuel Cleaver
Committee on Financial Services
Subcommittee on National Security,
International Development and Monetary Policy
House of Representatives
Washington, DC 20515

The Honorable Steve Stivers
Committee on Financial Services
Subcommittee on National Security,
International Development and Monetary Policy
House of Representatives
Washington, DC 20515

Dear Chairman Cleaver and Ranking Member Stivers,

On behalf of America's credit unions, thank you for holding the hearing entitled, "Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crime." The Credit Union National Association (CUNA) represents America's state and federal credit unions and the 115 million members that they serve.

Credit unions support efforts to track money laundering and terrorist financing, but also believe it is important to strike the right balance between the compliance costs to financial institutions, like credit unions, and the benefits to the federal government. As such, we support legislative and regulatory changes to address the redundancies, unnecessary burdens, and opportunities for efficiencies within the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) statutory framework.

Credit unions appreciate the importance of financial institutions, law enforcement, and the federal government all working together to combat money laundering, however, we would argue that the compliance burden for some of the BSA/AML requirements outweigh the value of the information reported.

The dollar amount thresholds included in the BSA/AML have not been updated since the law was originally enacted in 1970. In today's market the Currency Transaction Report (CTR) $10,000 threshold has the same buying power as $1,500 when the law was enacted fifty years ago – according to the Consumer Pricing Index's Inflation Calculator provided by the Bureau of Labor and Statistics. And yet, credit unions are required to report every cash transaction of $10,000 or more, even when the credit union knows that the transaction has no criminal implications. This is a clear example of the compliance burden far outweighing the value of the information to law enforcement.

On behalf of America's credit unions and their 115 million members, thank you for your leadership on this important issue. We look forward to working with you.

Sincerely,

Jim Nussle
President & CEO

March 13, 2019

The Honorable Maxine Waters
Chairwoman
U.S. House Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Patrick McHenry
Ranking Member
U.S. House Committee on Financial Services
4340 O'Neill House Office Building
Washington, D.C. 20024

Re: Kleptocracy Asset Recovery Rewards Act (H.R. 389)

Dear Chairwoman Waters and Ranking Member McHenry,

We are writing on behalf of the Financial Accountability and Corporate Transparency (FACT) Coalition to convey our support for the Kleptocracy Asset Recovery Rewards Act (H.R. 389), sponsored by Representatives Stephen Lynch (D-MA), Ted Budd (R-NC), and Steve Cohen (D-TN).

The FACT Coalition is a non-partisan alliance of more than 100 state, national, and international organizations promoting policies to combat the harmful impacts of corrupt financial practices.[1]

H.R. 389 would establish a rewards program for whistleblowers — encouraging individuals to inform the U.S. government about assets in the U.S. financial system that are connected to foreign corruption, enabling authorities to reclaim and return the money and deter foreign corruption moving forward.

Foreign corruption is a major economic and national security threat to the United States. Corruption undermines the rule of law, provides the lifeblood of authoritarian regimes and enables transnational organized crime to flourish. It diverts precious resources away from those who most need them, and fosters disillusionment with government — sometimes leading to the rise of terrorist networks.

The bipartisan Kleptocracy Asset Recovery Rewards Act is a sensible tool to safeguard American citizens and businesses from the scourge of corruption.

Should you have any questions, please feel free to contact Clark Gascoigne at +1 (202) 810-1334 or cgascoigne@thefactcoalition.org.

Sincerely,

Gary Kalman
Executive Director
The FACT Coalition

Clark Gascoigne
Deputy Director
The FACT Coalition

CC Members of the House Financial Services Committee

[1] For a full list of FACT Coalition members, visit https://thefactcoalition.org/about/coalition-members-and supporters/

Jubilee USA NETWORK
110 Maryland Ave. NE, Ste. 210
Washington, DC 20002
202.783.3566
www.jubileeusa.org

March 12, 2019

The Honorable Maxine Waters
Chairwoman
U.S. House Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Patrick McHenry
Ranking Member
U.S. House Committee on Financial Services
4340 O'Neill House Office Building
Washington, D.C. 20002

Re: March 13th Transparency Hearing and the Corporate Transparency Act of 2019

Dear Chairwoman Waters and Ranking Member McHenry:

On behalf of Jubilee USA, I want to thank-you for your support of our bipartisan initiatives to promote transparency, accountability and protections for the vulnerable in our financial system. Jubilee USA supports your March 13th, 2019 hearing on "Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crime."

As you know from our work together in the past, Jubilee USA's religious institutions, members and founders include more than 700 Christian, Jewish and Muslim faith communities and the US Episcopalian, Presbyterian, Methodist, Evangelical Lutheran, Catholic and United Church of Christ Churches. On behalf of our network, we are concerned with how financial secrecy, corruption and tax evasion impact vulnerable communities in the United States and around our world.

Some anonymous shell companies facilitate the theft of development aid and debt relief, the exploitation of vulnerable communities and the support of corrupt regimes in the developing world. Shell companies contribute to an estimated one trillion dollars leaving the developing world annually through tax evasion and corruption. In the United States, anonymous shell companies contribute to Medicare fraud, thefts from vulnerable communities and human trafficking.

The draft of the 2019 Corporate Transparency Act takes important steps toward ending abuses of anonymous companies. Increasing corporate transparency reduces corrupt behavior and can provide resources for US and global development. By identifying the owner who benefits from the existence of a corporation or collecting "beneficial ownership" data, law enforcement has tools to find criminals, corrupt public officials and deter enterprises that exploit the poor. Legislation that offers a clear and comprehensive definition of beneficial ownership avoids the pitfalls of inadequate definitions that only identify managers, directors or other stand-ins for the true owner(s).

The 2016 release of the "Panama Papers" was instructive in this regard. Due to lax rules around corporate ownership information, a single employee at the Panamanian law firm, Mossack Fonseca, served as the named entity for approximately 20,000 companies. She had little-to-no knowledge of the beneficial owners of those 20,000 companies.

Another crucial area in the draft is the provision governing access to information gathered. State and local law enforcement must have access because most investigations into illegal activity are performed by state and local officials in the United States. Financial institutions, which have anti-money laundering responsibilities, should have appropriate access to beneficial ownership by simple request.

On behalf of all at Jubilee USA we hold you in prayer as you work to ensure that our financial system protects the poor and fights corruption.

Sincerely,

Eric LeCompte
Executive Director

CC: Members of the House Financial Services Committee

NATIONAL
FRATERNAL ORDER OF POLICE®

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

CHUCK CANTERBURY
NATIONAL PRESIDENT

JAMES O. PASCO, JR.
EXECUTIVE DIRECTOR

13 March 2019

The Honorable Maxine M. Waters
Chairman
Committee on Financial Services
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Patrick T. McHenry
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Emanuel Cleaver II
Chairman
Subcommittee on National Security, International Development and Monetary Policy
Committee on Financial Services
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Steven E. Stivers
Ranking Member
Subcommittee on National Security, International Development and Monetary Policy
Committee on Financial Services
U.S. House of Representatives
Washington, D.C. 20515

Dear Madam Chairman, Mr. Chairman and Representatives McHenry and Stivers,

I am writing on behalf of the members of the Fraternal Order of Police to advise you of our continued support for the collection of beneficial ownership information to combat terrorist financing, money laundering and other criminal activities. We strongly agree with many of the points raised in H. Res. 206 as they pertain to the collection of this information and we look forward to working with the Committee on Financial Services and the Subcommittee on National Security, International Development and Monetary Policy to address these issues, in the months ahead.

For years, the FOP has supported the collection of beneficial ownership information and we've been proud to partner with Representatives Carolyn B. Maloney (D-NY) and Peter T. King (R-NY) on legislation entitled the "Corporate Transparency Act." A discussion draft sharing that same title is being considered by the committee today and the FOP is once again prepared to support this important legislation.

Transnational criminal organizations and terrorist operations are using our banks, financial institutions and other means to profit from their illegal activity. This is a well-documented problem for our financial institutions and for law enforcement as we work together to shut down these sophisticated criminal enterprises.

Congress and this committee have played a leadership role in identifying the problem and working with law enforcement to develop legislation like the "Corporation Transparency Act." In addition, this Administration also agrees with this approach—last July U.S. Secretary of the Treasury Steven T. Mnuchin testified before this committee and stated that there is a real need to "have access to beneficial ownership information for law enforcement and for combating terrorist financing."

The Secretary's remarks were very clear that this is a pressing issue and the vulnerability of our financial institutions poses a genuine threat to public safety and national security. Under current laws, shell corporations may be used as front organizations by criminals conducting illegal activity such as money laundering, fraud, and tax evasion. Legislation like the "Corporation Transparency Act" and other measures identified in H. Res. 206, propose to combat this misuse of U.S. corporations by requiring the U.S. Department of the Treasury, specifically the Financial Crimes Enforcement Network (FinCEN), to collect beneficial ownership information for corporations and limited liability companies formed under State laws unless the State is already collecting this information. It is vital that such information, once collected, be available to law enforcement at every level—local, State, tribal and Federal—upon a lawful request. The sharing of this information will help speed the ability of law enforcement to investigate any possible connection between these corporations and terrorist funding.

All too often, investigations will hit a dead end when we encounter a company with hidden ownership. Just as robbers or burglars wear masks to hide their faces and make identifying them more difficult; the criminals we are chasing in these cases use shell corporations as masks, concealing themselves while still profiting from their crimes. When we are able to expose the link between shell companies and drug trafficking, corruption, organized crime and terrorist finance, law enforcement will be able to bring these criminals to justice and make our citizens and our nation safer.

We would also like to raise our concerns about proposals that would increase the monetary threshold for filing Currency Transaction Reports and Suspicious Activity Reports, thereby reducing the information law enforcement currently receives. It is not clear what policy or public safety aim such a change is intended to accomplish. Organized criminal enterprises are already aware of the current thresholds and often take steps to avoid triggering these alerts and bringing scrutiny to their operations. Increasing these thresholds may negatively impact law enforcement and investigations into money laundering and other financial crimes.

On behalf of the more than 345,000 members of the Fraternal Order of Police, I want to thank this committee for its leadership on this issue and most of all, for its willingness to engage and work with the law enforcement community on the collection of beneficial ownership information. By working together, I believe we can make our financial system and our nation safer from criminal and terrorist organizations. If I can provide any additional information on this matter, please do not hesitate to contact me or my Executive Director, Jim Pasco, in my Washington office.

Sincerely,

Chuck Canterbury
National President

March 13, 2019

The Honorable Maxine Waters
Chairwoman
Committee on Financial Services
United States House of Representatives
2221 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
United States House of Representatives
2004 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairwoman Waters and Ranking Member McHenry,

We, the undersigned trade associations, are pleased to support Congressional efforts to end the misuse of anonymous shell corporations and pass meaningful anti-money laundering reform legislation. These efforts will help modernize the anti-money laundering and countering the financing of terrorism (AML/CFT) regime in the United States and help prevent the use of corporate structures to hide the identities of their beneficial owners from law enforcement.

Although the Financial Crimes Enforcement Network (FinCEN) adopted a customer due diligence regulation requiring financial institutions to collect information about beneficial owners, there is no existing mechanism for financial institutions to verify that information. When FinCEN issued the rule in May 2016, it urged Congress to pass companion legislation to enhance

the rule by creating a federal registry of the beneficial owners of legal business entities. Having a single federal registry would provide a verifiable and centralized source of beneficial ownership information, meeting the needs of law enforcement and helping financial institutions satisfy their regulatory obligations.

The failure to require legal entities to register beneficial ownership information represents a significant gap in the U.S. regulatory system that allows criminals, money launderers, kleptocrats, and terrorist financiers to obscure their identities from law enforcement. The federal government and, importantly, the law enforcement community do not have ready access to ownership information for certain corporate structures to assist them with their investigations into alleged money laundering and human trafficking activities. Closing this gap is an important reason why we, along with the Fraternal Order of Police and the National District Attorneys Association, support legislative plans to address these concerns.

While establishing a single federal registry for this purpose would create new obligations for legal entities and their beneficial owners, those obligations are neither burdensome nor overreaching. Indeed, we agree with the founder of the Small Business Majority that "providing the name, address and identification of the true owner of a business is not a burden. They are well aware of who controls and who benefits from their proceeds. The definition....is clear, easy to follow, and workable for small businesses who have no need to hide their owners' identity." We understand the concerns raised by some members of the small business community about the potential challenges this could present, however we believe that they can be appropriately addressed through accompanying education and outreach efforts, to ensure that small businesses are not caught unawares.

In addition to creating a federal beneficial ownership registry of legal entities, we encourage the Committee to address and amend the outdated and inefficient Bank Secrecy Act (BSA) regulatory framework. The current regime is nearly 50 years old, and has not fundamentally changed since its adoption in 1970. It is still operated as an individual, bilateral reporting system despite advances in technology that could improve its efficiency and effectiveness. A core problem is that today's regime incentivizes financial institutions to achieve compliance with technical requirements that bear little relationship to the actual goal of preventing, detecting, or halting financial crime. Moreover, the regime fails to consider collateral damage that may impact national security or financial inclusion goals. In other words, bank examiners focus on technical compliance, not the provision of valuable information to law enforcement or other measurements of effectiveness. Fundamental change is required to make this system an effective law enforcement and national security tool.

A set of articles in *The Economist* details the unfortunate consequences that the misalignment in AML/CFT expectations and standards has created as financial institutions have

worked to balance fear of enforcement and supervisory expectations with the AML compliance costs of maintaining a global business.[1] Often, and unfortunately, the best and most straightforward solution for financial institutions is simply not to serve certain customers, sometimes referred to as de-risking. De-risking can result in the withdrawal of financial services from already underserved populations and a migration of transactions out of the traditional financial services sector into unregulated channels that are not monitored for suspicious activity. The Government Accountability Office (GAO) found in its 2018 study on de-risking along the southern U.S. border that 80% of Southwest border banks de-risked due to a perceived AML/CFT compliance burden. Accordingly, the GAO recommended the regulatory agencies consider BSA reforms.[2]

To address these problems with the current regime, we recommend four key reforms to help clarify the complex regulatory reporting structure. Specifically, we believe that the Treasury Secretary should be required to:

1. Publish regularly updated national priorities for the AML/CFT regime; and take steps to better align the examination/compliance framework with these priorities (e.g., ensuring examinations focus on identification and management of risk, versus emphasis on technical compliance absent risk indicators);
2. Facilitate information sharing and feedback from law enforcement to financial institutions and further facilitate information sharing between financial institutions;
3. Update and streamline the process of filing Suspicious Activity Reports and Currency Transaction Reports to provide more timely and relevant information to law enforcement; and
4. Encourage and support the use of technology and artificial intelligence within financial institutions' AML programs.

We believe these reforms would represent great steps towards reducing the burden on customers, while at the same time improving the quality of information given to law enforcement.

---

[1] See The great unbanking: swingeing fines have made banks too risk-averse, *The Economist*, July 6, 2017, available at https://www.economist.com/leaders/2017/07/06/swingeing-fines-have-made-banks-too-risk-averse. See also "Rolling up the welcome mat: A crackdown on financial crime means global banks are derisking", *The Economist*, July 8, 2017, *available* at https://www.economist.com/international/2017/07/08/a-crackdown-on-financial-crime-means-global-banks-are-derisking.

[2] See "BANK SECRECY ACT: Further Actions Needed to Address Domestic and International Derisking Concerns," U.S. Government Accountability Office, June 26, 2018, *available at* https://www.gao.gov/products/GAO-18-642T.

We are pleased to support the Committee's work and stand ready to assist your efforts to modernize and enhance the effectiveness and efficiency of our nation's AML/CFT regime. We look forward to working with you on this important endeavor.

Sincerely,

The Bank Policy Institute
Institute of International Finance
Consumer Bankers Association
Institute of International Bankers
Mid-Size Bank Coalition of America
Bankers Association for Finance and Trade
Securities Industry and Financial Markets Association
The American Bankers Association
National Association of Federally-Insured Credit Unions

cc: Chairman Mike Crapo, Senate Committee on Banking, Housing, and Urban Affairs

Ranking Member Sherrod Brown, Senate Committee on Banking, Housing, and Urban Affairs

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

March 12, 2019

The Honorable Emanuel Cleaver
Chairman
Subcommittee on National Security,
International Development and Monetary Policy
Committee on Financial Services
United States House of Representatives
Washington, D.C. 20515

The Honorable Steve Stivers
Ranking Member
Subcommittee on National Security,
International Development and Monetary Policy
Committee on Financial Services
United States House of Representatives
Washington, D.C. 20515

Re: Tomorrow's hearing on "Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crime"

Dear Chairman Cleaver and Ranking Member Stivers:

I write today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) in regard to tomorrow's hearing entitled "Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crime." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 115 million consumers with personal and small business financial service products.

NAFCU has consistently recognized the importance of the Financial Crimes Enforcement Network (FinCEN), *Bank Secrecy Act* (BSA), and Anti-Money Laundering (AML) requirements in assisting in the prevention of tax evasion, money laundering and terror financing. Credit unions support efforts to combat criminal activity in the financial system. Our members have a good working relationship with FinCEN, and they consistently inform us that the publication of periodic AML/BSA guidance is very helpful. However, BSA/AML requirements still remain a burden to implement. We believe that the BSA/AML system is in need of improvements and reform, and we are pleased that the Subcommittee is examining draft legislation to strengthen and improve the system as part of tomorrow's hearing.

BSA/AML Reform

NAFCU supports FinCEN encouraging more coordination between law enforcement priorities and credit union examiners. Our members have consistently reported a lack of consistency among examiners in reviewing BSA policies and procedures, which makes it difficult to accurately anticipate how extensively to prepare for an exam. Additionally, many of our members have indicated that prudential examiners are too heavily focused on auditing absolute numbers of Suspicious Activity Report (SAR) filings and absolute compliance. As an example, many of our members have experienced situations where an examiner makes a finding on a SAR based on a purely technical issue, such as a strict timing deadline, which does not truly affect the usefulness of the SAR. Instead, NAFCU believes that FinCEN should encourage prudential examiners to conduct more holistic and systemic audits, such as reviewing a credit union's procedures and practices. We are pleased to see the focus on training for examiners on countering the financing of terrorism (CFT) and AML issues found in Section 202 of the draft legislation and believe that this is an important step to help improve the credit union experience with examiners in this area.

We are also pleased to see the focus on modernizing the AML system found in Title III of the draft legislation, such as encouraging innovation and providing exemptive relief to facilitate the testing of new technologies and innovations. For example, some of NAFCU's member credit unions would like to see

an updated database for SAR and Currency Transaction Report (CTR) filings to streamline the narrative reporting that law enforcement often requests from financial institutions. We also support the efforts in the bill to increase information sharing and allow the sharing of compliance resources in this area. Taken together, these steps can help strengthen and improve the system.

NAFCU would also encourage the Subcommittee to consider expanding and improving the draft legislation in two areas.

First, NAFCU believes that FinCEN could minimize the burden of information collection by raising the required SAR reporting threshold. The current threshold of $5,000 was set in 1996, which today equates to approximately $8,000 due to inflation. As more transactions cross the threshold, more SARs are filed in response. This increased volume potentially obfuscates the activities of bad actors. Increasing the threshold and indexing it for inflation would help to prevent the frequency of SAR filings from increasing beyond a manageable level, leading to more accurate FinCEN estimates for record keeping. We also support raising the threshold for CTRs.

Second, many credit unions are affected by BSA/AML compliance burdens and must spend significant time and resources on BSA/AML compliance. NAFCU believes that FinCEN could provide opportunities for technical grants or training to help assist with the cost of software or technological capabilities to reduce the number of man-hours involved. Such a move would be in direct alignment with FinCEN's objectives, as training and technological subsidies would enable more credit unions to have robust BSA/AML procedures in place, thereby furthering FinCEN's goals.

Corporate Transparency

NAFCU also supports efforts such as the draft *Corporate Transparency Act of 2019* from Representative Carolyn Maloney. The bill would help financial institutions, including credit unions, comply with the new Customer Due Diligence (CDD) Rule by requiring companies to disclose their true "beneficial owners" to FinCEN for creation of a database of beneficial ownership information that would be available to law enforcement agencies and financial institutions. We believe this draft legislation is an improvement over previous versions of the bill. We encourage the Subcommittee to further examine the "customer consent" requirement for financial institutions to obtain beneficial ownership information from FinCEN, as well as any potential costs associated with financial institutions' requests to access this important information. We want to ensure that these issues do not become a hurdle to credit unions accessing beneficial ownership information as it would hamper their ability to comply with the requirements of the CDD rule.

NAFCU appreciates this opportunity to provide comments on ways to improve the current BSA/AML regulatory compliance regime, and we are pleased to see the draft legislation before the Subcommittee today. We look forward to collaborating with the Subcommittee as it continues to examine this issue. Should you have any questions or require any additional information, please do not hesitate to contact me or Alex Gleason, NAFCU's Associate Director of Legislative Affairs, at 703-842-2237.

Sincerely,

Brad Thaler

Brad Thaler,
Vice President of Legislative Affairs

cc: Members of the Committee on Financial Services

The New York Times

2 Former Goldman Executives Barred From Banking Industry After Malaysia Fraud Scandal

By David Enrich and Matthew Goldstein

March 12, 2019

The Federal Reserve on Tuesday barred two former Goldman Sachs executives from working in the banking industry because of their roles in a multibillion-dollar fraud involving a Malaysian government investment fund.

One of the executives, Tim Leissner, who was one of Goldman's top investment bankers in Asia, has pleaded guilty in a federal criminal investigation of the fraud and has been ordered to forfeit about $44 million. The other executive, Roger Ng, has been charged in the United States with participating in money laundering and bribery, but is in custody in Malaysia.

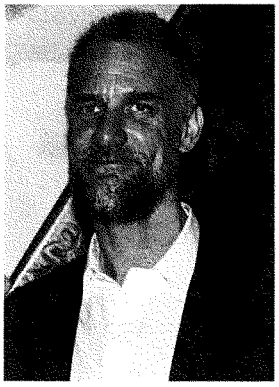
Goldman Sachs helped the fund, 1Malaysia Development Berhad, commonly known as 1MDB, sell more than $6 billion of debt to investors, ostensibly for projects that would benefit the Malaysian people. But federal prosecutors contend that at least $2.7 billion of that money went to fuel the lavish lifestyles of several people close to a former Malaysian prime minister, including the flamboyant financier Jho Low.

Prosecutors have said some of the money raised for the fund went toward paying bribes to secure business for Goldman Sachs.

Mr. Low, who also has been charged in the United States and Malaysia, attended at least two meetings where Lloyd Blankfein, the former Goldman chief executive officer, was present. But Goldman Sachs has painted Mr. Leissner, the husband of the fashion designer and model Kimora Lee Simmons, as a rogue operator who bears the responsibility for the bank's role in the scandal.

The bank has said that it took steps to make sure that neither Mr. Low nor any other intermediaries played a role in arranging the 1MDB financing deals.

Tim Leissner, who was one of Goldman Sachs's top investment bankers in Asia, has pleaded guilty in a criminal investigation of a Malaysian fraud scandal.
Rodin Eckenroth/Getty Images



[Read more about Goldman Sachs's efforts to distance itself from Mr. Leissner.]

"Given the Department of Justice's charges last year, this development is hardly surprising," said Jake Siewert, a Goldman spokesman.

Federal prosecutors and banking regulators have continued to investigate Goldman's role in the scandal. The bank has said it faced the prospect of a significant fine to resolve the matter.

In addition to permanently barring Mr. Leissner from the banking industry, the Fed fined him $1.4 million. The banking authorities in Singapore barred Mr. Leissner from working in that country late last year.

A lawyer for Mr. Leissner, who consented to the Fed ban, declined to comment. He is free on bail, which was originally set at $20 million. But the specific terms of Mr. Leissner's bail were kept under seal when a redacted version of a transcript of his Aug. 28 guilty plea was made public in November. Lawyers for The New York Times asked a federal judge last month to unseal the portions of the transcript that describe the terms of Mr. Leissner's bail.

Mr. Leissner is scheduled to be sentenced on June 28.

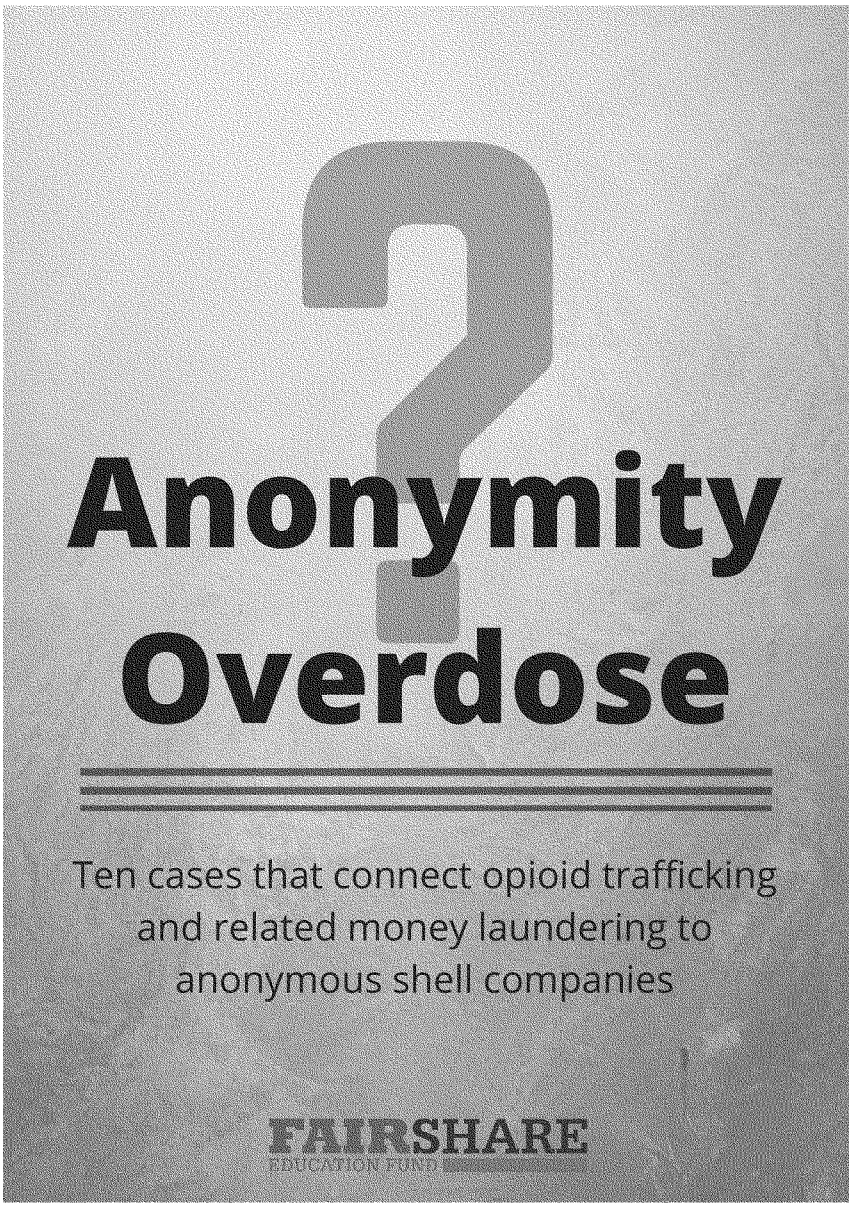
Mr. Ng's lawyer, Marc Agnifilo, declined to comment on the Fed's action on Tuesday. He previously said his client planned to plead not guilty after he was returned from Malaysia to face the pending charges filed by United States prosecutors in federal court in Brooklyn.

Investigators in the United States have said 1MDB was raided by the former Malaysian prime minister Najib Razak and other officials, including Mr. Low, with billions of dollars in siphoned funds used on luxuries including diamonds, designer handbags and fine art, and to help finance the Hollywood film "The Wolf of Wall Street."

Mr. Najib was ousted in last year's election and charged by Malaysian prosecutors with money laundering in August.

Mr. Low, who remains at large, is believed to be staying in China.

A version of this article appears in print on March 13, 2019, on Page B3 of the New York edition with the headline: Fed Bars 2 Ex-Goldman Executives Tied to Malaysia Scandal


Anonymity
Overdose
Ten cases that connect opioid trafficking and related money laundering to anonymous shell companies
FAIRSHARE
EDUCATION FUND

Anonymity Overdose;

Ten cases that connect opioid trafficking and related money laundering to anonymous shell companies

Written by:
Nathan Proctor and Julia Ladics
Fair Share Education Fund

Special thanks to Mark Hays, Gideon Weissman, John Cassara and the FACT Coalition

August 2016

Executive Summary

"[W]e have become convinced that we cannot stop the drug trade without first cutting off the money that flows to drug trafficking organizations." – The Bipartisan United States Senate Caucus on International Narcotics Control.[1]

Over the last 15 years, opioid overdose deaths have quadrupled, and opioid abuse has become a full-blown crisis.[2] As lawmakers, law enforcement and other public officials struggle to address this problem, we can make it easier to go after the money used in drug trafficking by ending the gaps in our laws that allow companies to be incorporated anonymously.

Drug money is laundered with astonishing effectiveness. The Office of National Drug Control Policy estimates that $65 billion is spent by Americans every year on illegal drugs, but only $1 billion, or roughly 1.5%, of that money is seized per year domestically by all federal agencies combined.[3] In other words, it is likely that 98.5% of the proceeds derived from drug trafficking remain in the hands of traffickers.

One of the tools that criminals use to launder their money so successfully are shell companies, especially anonymous shell companies. These companies only exist on paper and, in most cases, law enforcement does not have access to information about who owns and controls them. Indeed, in most cases such information isn't even collected when companies are formed. As such, many promising investigations are abandoned when law enforcement runs into an anonymous shell company. Authorities may have good reason to suspect someone of being involved in criminal activity. However, without the basic information necessary to show that a suspect is directly linked to a shell company used to facilitate illegal activity, they are unable to make their case, or run out of the time and resources needed to do so.

In this report we found ten case studies that connect opioid trafficking and shell companies, where law enforcement did succeed in untangling the web of secrecy and anonymity. However, these cases represent a minority.

In some of the cases that we've found, profits made by the perpetrators were spent fairly brazenly on items such as luxury real estate, diamond encrusted watches or race horses. Often little of that was recovered by investigators. For example, the biggest of Mexico's drug gangs, the Los Zetas cartel, used anonymous shell companies to launder millions, in part by purchasing race horses with drug proceeds – they even named one horse "Number One Cartel." In one of the largest oxycodone busts in Oregon history, Kingsley Iyare Osemwengie and his associates were found to use call girls and couriers to transport oxycodone, and then move profits through an anonymous shell company aptly named High Profit Investments LLC. Similarly, even after he was officially designated under the Foreign Narcotics Kingpin Designation Act as a drug lord, Fernando Melciades Zevallos Gonzalez was able to sell his Miami properties and escape with the proceeds through anonymous companies. His empire continues to operate. You can read more about these and other examples on pages 10-15.

Our recommendation: Require the collection of beneficial ownership information and provide that information to law enforcement.

We need to equip our law enforcement officers with tools they can use to put an end to drug cartels. Simply requiring that all companies formed in the U.S. disclose their beneficial owners would enable law enforcement to more effectively follow the money trail and make it harder for criminals to hide their money. We should use every tool at our disposal to tackle the opioid crisis, and going after the money is just such a critical tool.

"One of the Worst Public Health Epidemics" in U.S. History

Opioid addiction is growing across the United States, and is a public health crisis – 78 Americans die every day from an opioid overdose. [4] As of last year, opioid overdoses accounted for more deaths than motor vehicle crashes.[5]

Roughly 75% of opioid users say they started with prescription pain killers.[6] Then, because it is easier to abuse and significantly cheaper, heroin often becomes the next stage in their addiction.[7]

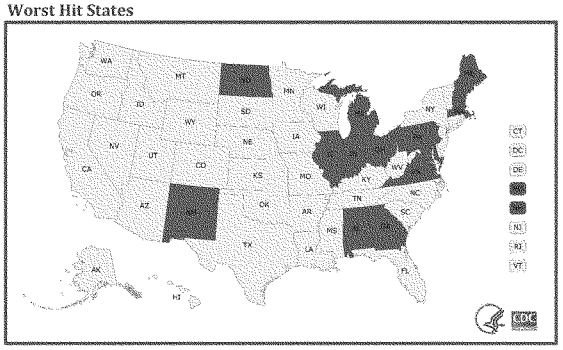
Common Opioids

- Oxycodone
- Codeine
- Fentanyl
- Hydrocodone
- Morphine
- Opium
- Heroin

Drug cartels are competing on price with prescription opioids, and they are winning. In most states heroin costs less than a packet of cigarettes[8] which range from $4.38 in Missouri to $10.45 in New York. Meanwhile, OxyContin can sell for over $80 a pill.[9]

Overdose deaths from prescription pain killers and heroin have quadrupled since 1999[10] while the number of heroin users nearly doubled between 2005 and 2012.[11] The White House and others have labeled this as one of the worst public health epidemics in U.S. history.[12]

Worst Hit States



Statistically significant drug overdose death rate increase from 2013 to 2014, US states CDC Injury Center, http://www.cdc.gov/drugoverdose/data/statedeaths.html

A Price Tag North of $193 Billion

The opioid epidemic has had an immeasurable impact on families, congregations, communities, local law enforcement and medical providers. And while the largest costs have been human, there are also significant public financial costs to both local governments and others working on the front lines of the issue.

A 2007 estimate, the most recent one available, put the economic cost of opioid addiction at $193 billion.[13] Given how much the crisis has grown since 2007, the price tag is likely many times this level. The $193 billion estimate includes:

- $120 billion in lost productivity, mainly due to labor participation costs, participation in drug abuse treatment, incarceration and premature death;
- $11 billion in healthcare costs – for drug treatment and drug-related medical consequences; and
- $61 billion in criminal justice costs, primarily due to criminal investigation, prosecution and incarceration, and victim costs.

"In order to have the biggest impact on its mission as the nation's drug enforcement agency, DEA has identified and targeted those illegal proceeds that flow back to sources of supply as the top priority of its financial enforcement program; since this is the very money that is destined to finance the next cycle of illegal drugs that will be marketed to our consumer markets."

- Drug Enforcement Agency

https://www.dea.gov/ops/money.shtml

Going After the Money is a Key Strategy

As communities struggle to respond to the growing opioid crisis, we must use all the tools available to help those efforts. As such, we need to consider better tools for law enforcement to go after the proceeds of drug trafficking.

Clearly, one of the largest motivations behind drug trafficking is the huge amount of profit that comes from engaging in such activity.[14] If authorities could seize those profits or make it more difficult for profits to move from the street-level trafficking to the bank accounts of kingpins, they could lower this incentive.

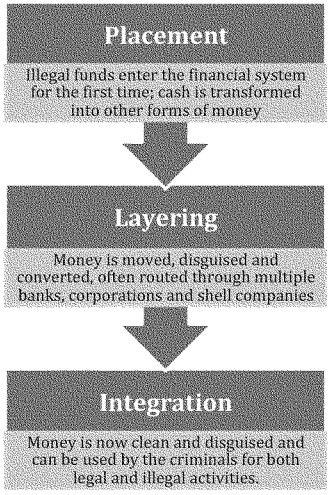
Currently law enforcement says that drug profits are most vulnerable and easiest to tie back to the traffickers when they are in cash form.[15] However, even in its most vulnerable state, law enforcement officials estimate we are seizing less than one percent of illicit outbound cash flows on the southwest border and even less of the money laundered through the international financial system.[16]

John Cassara, a former special agent for the Department of the Treasury agrees that going after the money is key, yet difficult. In an article from 2013 he wrote: "Today's complex financial fraud cases sometimes take years to complete. From a management point of view, it is a tremendous investment. They can't afford to waste scarce resources that lead to investigative dead-ends. What most outsiders do not realize is that a very large percentage of investigations are unsuccessful.

"Although commentators argue the point, the bottom-line metric that quantifies success for law enforcement is the number of investigations that result in successful prosecutions and convictions. Another key metric for certain crimes is criminal assets forfeited…Within law enforcement, there is a subtle and sometimes selective weeding of cases that are chosen to be pursued."[17]

The Basics of Money Laundering

Money laundering refers to activities that are undertaken specifically to hide the true source of the money. This source is usually a criminal enterprise or activity, and laundering is done to make the income seem legitimate to allow it to be used in the normal economy.[18]



There are three stages to money laundering: placement, layering and integration. Placement is how the illegal money enters the financial system. This usually involves turning cash into something easier to transfer, such as a bank account deposit, a wire transfer, a pre-paid stored value card, travelers check, etc.

The next step, layering, refers to how this money is disguised. Typically, this is done through multiple wire transfers through many banks and shell companies and corporations in order to make the money trail very hard to trace. These are also often done through multiple jurisdictions, for example from the U.S. to the Cayman Islands, to the Bahamas and then back to the U.S. The final stage, integration, is when the money is clean enough (or far enough removed from the criminal activity) to be useable for legal and legitimate transactions.[19]

Anonymous, LLC: How a company ends up with no owner

In the U.S., companies are formed at the state level. However, in most states, very little information is required from the people forming companies – generally less than it takes to get a library card.[20] Typically, a new company must list a company name, the name of an 'agent' authorized to accept legal service on behalf of the company, and a contact address for that agent. A few states require a bit more information – say, the name of at least one 'manager' of the company being created. But not a single U.S. state requires people forming companies to disclose the real, living person or persons that

own, control and ultimately 'benefit' from the company's existence – the so-called 'beneficial' owners of a company.

What is a Shell Company?

When you think of a company, you imagine a business with employees, operations, products and sales. But unlike a regular company, a shell company is a hollow structure, set up for the purposes of performing financial manoeuvres. Essentially, it only exists on paper.

One of the key features of companies is that they can set up bank accounts – hence shell companies, especially anonymous ones, are often used simply for monetary and other bank transactions.

http://www.economist.com/blogs/graphicdetail/2016/04/using-and-abusing-offshore-accounts

This state of affairs means that there are many easy ways in which someone who wants to set up a shell company and hide the fact that they own it, can do so. For example, anonymous shell companies often have nominee owners or directors, people who are unrelated to the activities of the company. Their role is to be the public face of the company on paper, while the real owners remain hidden. Sometimes, the nominee owners or directors aren't even people but companies, law firms or other entities. In egregious cases, the nominee owners or directors can sometimes simply be made-up names.

All this allows the true beneficiaries, the people who benefit from the activities of the company, to remain hidden. It is often difficult and sometimes impossible to link the nominee owners or directors back to the real beneficiary.

Financial Getaway Cars

While a shell company might sometimes serve a purpose in law-abiding business operations, keeping information about the real owner of a business from law enforcement is harder to defend. Saying "I can't think of a reason not to do that," Patrick Fallon, Jr., head of the FBI's financial crimes section, said he believes all shell companies should be required to disclose their true owners.[21]

According to a 2012 academic study, out of 60 countries examined, the United States was found to be the easiest place in the world for criminals to incorporate an anonymous shell company for illegal activities.[22] And since there is no process in place to keep track of the beneficial owners of companies formed in the U.S.,[23] there is no way to trace criminals' identities let alone hold them responsible for their actions.

That makes anonymous shell companies formed in the U.S. a favorite tool for moving illicit money. As Story County Iowa Sherriff Paul Fitzgerald wrote, "Think of them as financial getaway cars — companies set up to move ill-gotten money without leaving anyone to be held accountable." [24]

Anonymous shell companies are also used in:

- Terrorist financing
- Human trafficking
- Tax avoidance and evasion
- Fraud (e.g. insurance)
- Ponzi schemes
- Arms dealing

Law Enforcement Struggles to Go After Drug Money

Most arrests for drug trafficking involve low level distributors[25] whose ranks can easily be replenished.[26] These arrests resemble a large game of whack-a-mole, where distributors substitute one another very quickly. Many law enforcement experts believe that in order to disrupt the drug trade more substantially, we need to arrest the kingpins and cartel bosses.

The DEA and other law enforcement and public policy organizations have determined that the biggest impact they can have on drug trafficking is to intercept their illegal profits and interrupt their monetary flows.[27] This would help dethrone those in the highest seats of authority in drug operations and stop the demand-fueled regeneration of street level operations.

As long as these easy money laundering mechanisms are in place, there will always be people willing to traffic drugs.

We need to fix the system to close the loopholes that allow any criminal with the inclination to traffic drugs to do so.

However this can often be difficult if not impossible. Law enforcement frequently runs up against a brick wall when they encounter an anonymous shell company; many investigations need to be abandoned when they run into one because law enforcement loses the money trail.[28] "On a near-daily basis we encounter a company or network of companies involved in suspicious activity, but we are unable to glean who is actually controlling and benefiting from those entities, and from their illicit activity. In other words, we can't identify the criminal," said Cyrus Vance Jr., District Attorney for New York County, NY.[29] Not only do they have trouble accessing paperwork about the beneficial owners of a company, if they succeed, they often see documentation that lists no owners or other anonymous companies as owners.

"Our statement of national transparency standards should be something more than: 'U.S. financial transparency: Better than Lichtenstein and trying to catch up to Panama.' Simply put, we lag behind many other countries in the world in this regard, and it makes our statements concerning transparency and tax evasion ring hollow and hypocritical."

- Robert M. Morgenthau, District Attorney
New York County, NY, in testimony before the Committee on Homeland Security and Government Affairs, June 18, 2009.

Because of the challenges of tracing money beyond the placement stage, there is little chance of connecting cash deposited in a bank to the eventual use by those higher up in the drug-trafficking enterprise. Once drug traffickers manage to get beyond the placement stage, and layer their money into the financial system, it is effectively lost to law enforcement.

According to Adam Szubin, the acting under secretary for terrorism and financial intelligence at the U.S. Treasury, "with every threat that we track, be it foreign terrorists, narcotics cartels, sanctioned regimes or cyber hackers, our investigators encounter American shell companies used to hide and move money." [30]

Ending the use of anonymous shell companies would assist law enforcement in making it more difficult for drug traffickers to hide and launder their money.[31]

The Insider Perspective

All too often investigations are stymied when we encounter a company with hidden ownership. These nameless, faceless companies can do business just like any other, but it is difficult, if not impossible, to identify the real people behind them.

"Follow the money" is a standard investigative strategy. Law enforcement agents start at the street level — the drug dealer or low-level lackey — and try to follow the paper trail to the ringleader. When we can identify the owners of anonymous shell companies, we can track down those kingpins and bring them to justice.

An anonymous company in Nevada may be owned by another in Delaware, which is owned by a trust in the Cayman Islands, and so on. Criminals use layers of shell companies to frustrate investigators and protect themselves from prosecution. Sometimes we find alternate routes to bring evidence against the kingpins, but more regularly our investigations are thwarted at the low end of the criminal food chain. We may arrest low-level lackeys, who get easily replaced. So we go after them and fail to prosecute the top-level crooks.

This is a problem wherever anonymous companies can be incorporated. That includes virtually every U.S. state, for very few collect any information about the real owner of a company. For all the grumbling about offshore shell companies, many U.S. states are no better. Secrecy has become a big business in places like Delaware, Nevada and Wyoming, where even the people named on a company's board of directors are often little more than a fiction. For a small fee an incorporation agent can provide your company with a set of "nominees," or random individuals, to stand in as representatives for your board of directors and shareholders. It's a practice perfectly legal in most states. In fact, the only two states that require information identifying corporate owners – a standard practice in most countries – are Maine and Alaska.

Once a company has the legitimacy afforded by incorporation in the United States, opening bank accounts to access the global financial system is easy. You or I have to show proof of identity to put a few hundred dollars into a checking account, but a corporation can instantly move millions of dollars to distant points on the globe without so much as a real person's name — someone who can be held accountable if the corporation violates a law — associated with the transaction.

It is almost a certainty that, at this very moment, a terrorist cell, drug cartel or corrupt government official is using an anonymous U.S. shell corporation to finance illicit activities. We should provide law enforcement with the tools necessary to thwart these activities and set a standard for the rest of the world.

Cyrus Vance Jr., District Attorney for New York County, State of New York
Op-Ed published by Reuters
October 2012

"In order to succeed, terrorists, organized crime, drug cartels and major fraudsters must have the ability to raise, move, store and spend money. Anonymous shell companies, that shield beneficial ownership, are one of the primary tools used by bad guys to openly acquire and access nefarious funds."

Former Chief of the FBI's Terrorist Financing Operations Section, Dennis M. Lormel, op-ed in the Cleveland Plain Dealer, August 16, 2013.

"Years of research and law enforcement investigations have conclusively demonstrated the link between the abuse of legal entities, on the one hand, and, on the other hand, WMD proliferation, terrorist financing, sanctions evasion, tax evasion, corruption and money laundering for virtually all forms of serious criminal activity. As these reports and investigations indicate, this abuse is particularly prevalent with respect to legal entities created in the United States."

Assistant Secretary for Terrorist Financing, U.S. Department of the Treasury, David S. Cohen, Testimony before the Committee on Homeland Security and Government Affairs, June 18, 2009.

"While [some] notorious drug trafficking famil[ies] may be beyond our reach, the proceeds from their decade's long money laundering scheme are not."

Manhattan U.S. Attorney, Preet Bharara, DEA Press release, October 10th 2012

"The lack of corporate transparency has allowed criminal entities a gateway into the financial system and further veils their illicit activity. Investigations can be significantly hampered in cases where criminal targets utilize shell corporations."

Deputy Assistant Director, Office of Investigations, U.S. Immigration and Customs Enforcement, Janice Ayala, Testimony before the Committee on Homeland Security and Government Affairs, June 18, 2009.

"DEA realizes that there are not enough time or law enforcement resources to adequately address all illegal drug proceeds. Therefore, in order to have the biggest impact on its mission as the nation's drug enforcement agency, DEA has identified and targeted those illegal proceeds that flow back to sources of supply as the top priority of its financial enforcement program."

Drug Enforcement Administration, Programs: Money Laundering, https://www.dea.gov/ops/money.shtml

"TCOs [Transnational Criminal Organizations] continue to exploit the banking industry to give illicit drug proceeds the appearance of legitimate profits. Money launderers often open bank accounts with fraudulent names or businesses and structure deposits to avoid reporting requirements."

2015 National Drug Threat Assessment Summary, 96-97

Case Studies

Drug Traffickers Use Call Girls to Transport Oxycodone All Across the U.S.

Kingsley Iyare Osemwengie and his associates used call girls and curriers to transport oxycodone and the money made from selling it across the United States. He disguised his income through an anonymous shell company, aptly named High Profit Investments LLC.

Kingsley Iyare Osemwengie of Las Vegas, Nevada, was part of a sophisticated drug trafficking organization that diverted legitimate medicine such as oxycodone into the black market. The ring involved drug trafficking and money laundering activity in Massachusetts, Nevada, Texas, Florida, Georgia, Utah, Colorado, New York, Washington, Alaska, Pennsylvania and Oregon. This was the largest oxycodone trafficking case in the history of the District of Oregon based on the sheer volume of oxycodone distributed, the geographic scope of the conspiracy, and the enormous profits generated. A single 80 milligram oxycodone pill sold for a range of $30 wholesale to $80 retail. Osemwengie invested in luxury real estate and flashy jewelry including a watch decorated with over 1,000 diamonds.[32]

The traffickers used call girls to transport the drugs across the country, and Osemwengie even used one of them as the nominee for an anonymous shell company used to launder proceeds from his drug trafficking scheme. The company was aptly named High Profit Investments LLC[33] and was incorporated in Nevada.

Fraudulent Online Pharmacy Diverts Prescription Drugs

Mihran and Artur Stepanyan operated at least four anonymous shell companies which they allegedly used to hide a wide-ranging criminal enterprise engaged in racketeering. Their biggest business consisted of diverting prescription drugs such as oxycodone from unlicensed sources to unknowing customers through a website pharmacy.

Mihran and Artur Stepanyan, along with at least 19 other people, are considered to be part of a nationwide drug diversion, money laundering and fraud enterprise, an online pharmacy. So much of the pharmacy's business was criminal that it qualified as a racketeering enterprise. The Stepanyans diverted legitimate prescription drugs and obtained other prescription drugs from unlicensed sources. **They used several anonymous shell companies, such as GC National Wholesale Inc.,[34] Nationwide Payment Solutions Inc.,[35] FM Distributors Inc.[36] and more to sell the drugs and launder the money.** During their operations over $393 million worth of drugs was distributed and over $5 million was stolen in financial crimes.[37] The operation was just beginning to experiment

with a murder-for-hire scheme when they got caught. The majority of their enterprises were based in Northern California, but also included Puerto Rico, New Mexico and others.

Drug Money Laundering Disguised As "International Tax Planning, Asset Protection and Other Wealth Preservation Techniques"

Martin Tremblay ran a complex criminal operation centred around his use of multiple anonymous shell companies and training as an investment banker to launder drug money. His company fittingly claimed to be a leader in, amongst other things, "wealth preservation techniques."

Tremblay was the president and managing director of the Bahamas based **anonymous shell company, Dominion Investments Ltd.,[38] which he used to launder over $1 billion** from the firm's clients. The money he laundered came from all sorts of illegal activity including drug trafficking involving cocaine, GHB and other drugs. His money laundering scheme ran from 1998 to roughly 2005, and his company owned bank accounts all over the U.S. To further conceal the source and nature of these funds, Tremblay and his co-conspirators created shell companies and fictitious entities all over the world, including the U.S, using the same false nominees, addresses, and telephone numbers, to launder these illegal proceeds.[39]

Money Launderers 'Teach' Undercover IRS How to Hide Drug Money

Pavel Sosa Medina and Amado Vazquez Jr. laundered money for others for profit using shell companies based in Kentucky and Florida. In a secret IRS sting operation, the pair laid out step by step instructions to undercover IRS agents on how to launder and hide their purported drug profits using anonymous shell companies.

Vazquez and Sosa Medina conspired to launder money for profit. The two were suspected money launderers from previous cases involving laundered drug profits through a Miami-Dade check-cashing company.[40] Using their history as a stepping stone, in an undercover operation, IRS agents approached the pair asking them to help launder around half a million dollars in supposed drug money. The pair, saying they were willing to help as their business was already involved in criminal activity,[41] laid out a step-by-step money laundering plan to the IRS that included shell companies, blank checks and multiple wire transfers.[42] **The anonymous shell companies they used were incorporated in Florida and Kentucky, and they included ZAN Providers LLC[43] and R.C. & Son Enterprise LLC.[44]** Both are in prison in Florida.

Peruvian Airline Owner and Drug Kingpin Continues Criminal Activity From Prison

Notorious and violent drug trafficker **Fernando Zevallos**, founder of the airline Aero Continente, used two anonymous shell companies, La Hacienda (USA) LLC and Running Brooks LLC, to funnel his drug money into real estate in Florida.

Although in prison in Peru, Fernando Melciades Zevallos Gonzalez's criminal network continues to operate. Since the 1980s, **Zevallos has operated a drug trafficking organization and used two anonymous shell companies based in Miami, La Hacienda (USA) LLC**[45] **and Running Brook LLC,** [46] **both incorporated in Florida, to hide his drug profits.** After being designated a "significant foreign narcotics trafficker" under the Kingpin Act which froze his U.S. assets, Zevallos still managed to use the shell companies to move $1.4 million of his $1.7 million out of the United States. It is likely that to achieve this, Zevallos transferred the shell companies to be under his wife's name,[47] which is how the authorities tracked him. Key members of his associates and family continue to operate his drug network,[48] and the rest of his finances are still out of reach of the U.S. and Peruvian authorities.

Fake Gold Miners Produce and Traffic Drugs

The elusive **Sanchez-Paredes family** have been operating a drug trafficking organization based in Peru for decades. They use Florida based anonymous shell companies such as Comarsa, a gold mining company, to produce cocaine and launder their profits.

Since the early 1980s Peruvian authorities have investigating the Sanchez-Paredes family who allegedly operate the Sanchez-Paredes Drug Trafficking Organization (DTO). There is a criminal complaint pending against the family in Peru, whilst in the U.S. investigations continue. Peruvian law enforcement believe that the Sanchez-Paredes DTO has financed various businesses including mining companies, farms, real estate investments, transportation companies and more, for the purpose of laundering many millions of dollars in narcotics trafficking proceeds. For example, **the Sanchez-Paredes DTO owns two anonymous mining companies, CIA Minera Aurifera Santa Rosa SA ("Comarsa") and CIA Minera San Simon ("San Simon"). Both of these firms claim to be mining gold but are believed to be manufacturing cocaine**; calcium oxide is used for both gold mining and cocaine production, and the amount seized by Peruvian authorities in 2007 was significantly more than the amount necessary to mine gold.

More generally, the Sanchez-Paredes DTO uses many shell companies[49] and bank accounts linked to them to hide and launder their drug profits. They used various distant family members as the nominal owners of the company while the names of the real owners remained hidden. Followed by a seizure of 12 bank accounts containing over $31 million from the family, Manhattan U.S. Attorney Preet Bharara said: "While this allegedly notorious drug trafficking family may be beyond our reach, the proceeds from their decade's long money laundering scheme are not."[50] Successful cases such as

this show how following the money can be an effective way of cracking down on drug trafficking, however this case is the exception to the rule due to lack of incorporation transparency.

Former USC Athlete Leads Massive International Drug Trafficking and Money Laundering Organization

Owen Hanson allegedly the lead a violent international narcotics trafficking and gambling ring based in San Diego, California. His activities reached as far as Australia, and he used a U.S. based anonymous shell company called Big Dog Memorabilia Inc., to disguise his activities.

22 people were indicted in relation to the racketeering enterprise they allegedly named "ODOG", an international drug trafficking, illegal sports gambling and money laundering organization. The organization used runners to both collect gambling debts and deliver drugs such as heroin to customers. Along with many others, a Certified Public Accountant (CPA), Luke Fairfield, assisted the enterprise by setting up anonymous shell companies and advised them on how to structure their bank transfers to remain inconspicuous. **One of these anonymous shell companies' real name was Big Dog Sports Memorabilia Inc.,[51] which was a front company used to manage the money behind the organization's operations.** The enterprise employed violence and threats of extreme violence to ensure people paid their drug or gambling debts, and their reach extended as far as Peru and Australia. The case against Hanson and his associates is still ongoing in California.[52]

Over 50 Luxury Vehicles Used to Launder Heroin Trafficking Money

Addonise Wells and Mario Freeman used anonymous shell companies to invest their heroin trafficking profits in luxury vehicles. They also employed **Jimmie Goodgame,** who also bought luxury vehicles and was involved in the money laundering aspect of the enterprise.

Addonnise Wells and Mario Freeman are accused of leading a large scale heroin trafficking ring in Ohio. The pair used an anonymous front company, Moe's Tire Company, to deliver the drugs and launder the profits. They also employed Jimmie Goodgame and his wife Stacey to **launder money for them through more anonymous shell companies. One of these companies was called J&G Enterprises I LLC,**[53] which was anonymous until 2008, when the agent's name was changed to that of Jimmie Goodgame.[54] It is unclear why this change occurred.

While the Goodgames bought luxury vehicles to protect and hide the money, Wells and Freeman bought real estate in the names of their relatives for the same purpose. These luxury vehicles were also used by Wells and his associates to transport drugs.[55]

Authorities had suspected the Goodgames' involvement in drug trafficking for years. At a coincidental traffic stop outside Chicago, police found over $500,000 in cash hidden in containers in one of the cars registered to Goodgame. With this evidence, they were able to build a strong enough case to go after the operation. Goodgame alone controlled at least $1.5 million in profits.[56]

Los Zetas Drug Cartel Launders Money Using Race Horses

The leader of the infamous Los Zetas cartel, **Miguel Angel Trevino**, used anonymous shell companies to launder money. The cartel and its leader purchased race horses in Oklahoma, which they gave names such as 'Number One Cartel' both to keep their money safe and profit off horseracing.

The biggest of Mexico's drug gangs is the Los Zetas cartel, whose former leader...[is] Miguel Ángel Treviño...From 2008, **the Zetas used [anonymous] shell companies, in a scheme to launder millions of dollars of drug money into the United States, with the true ownership hidden behind front men.**[57] The money was hidden behind the purchase of race horses, some of whom were given names such as 'Number One Cartel' and 'Morning Cartel'. The horses were incredibly successful and reported to win the cartel several million dollars.

Fourteen people, including Treviño, were indicted on money laundering charges by the U.S. in 2012.[58] Treviño was captured in Mexico in July 2013.[59] As of September 2013, four co-defendants from the original indictment have yet to be caught. Nine people have been sentenced for their role in the scheme. [60] [61]

This case study was excerpted from "The Great Rip Off" by Global Witness.

'Boss of Bosses' Crime Lord and Drug Trafficker Still Free in Moscow

Known as the 'boss of bosses', the Russian **Semion Mogilevich** uses anonymous shell companies all around the world, including the U.S., to launder money for his vast criminal enterprise. Mogilevich traffics drugs, cheats on the stock market, facilitates prostitution, and more. Although several arrest warrants have been issued against him, he still lives freely in Moscow.

The FBI has described Semion Mogilevich as "the most dangerous mobster in the world," allegedly "involved in weapons trafficking, contract murders, extortion, drug trafficking, and prostitution on an international scale." [62]According to an indictment, that reputation did not stop the Russian from setting up a **vast network of anonymous companies, stretching from Eastern Pennsylvania to the United Kingdom[63], which allowed him to cheat the stock market and steal over $150 million from investors**

in the United States and overseas[64]...By inflating the price of his companies through manipulating securities and false reporting, including reportedly lying to the Securities and Exchange Commission, Mogilevich convinced investors to purchase millions in stocks in a company that allegedly did no real business. Those involved lost millions.

In spite of several arrest warrants issued against him, Mogilevich still lives freely in Moscow, according to the FBI. He has not been convicted for these crimes.[65] This case is a clear demonstration of how some drug trafficking organizations are part of a larger criminal enterprise involved in many different criminal activities. This it illustrates how money laundering tools such as anonymous companies can be used to hide and finance all kinds of illicit activities and layers of complexity that make it even more difficult for law enforcement to monitor, track and seize the proceeds derived from drug trafficking.

This case study was excerpted from The Great Rip Off by Global Witness.

Recommendations

This report recommends that federal law makers end the use of anonymous shell companies by mandating the collection of true beneficial ownership information from all companies. This information then needs to be easily and efficiently accessible by law enforcement, who can then act on it to help curb drug trafficking and hence the ongoing opioid crisis.

"U.S. shell companies [have] the dubious distinction of being the only money laundering method where secrecy is provided by a government entity...This is simply unacceptable."

- **Adam Szubin,** Acting Under Secretary for Terrorism and Financial Intelligence of the U.S. Treasury

Quote from column published in the Hill, quoted in the Daily Sabah, July 12th 2016, http://www.dailysabah.com/americas/2016/07/12/us-shell-companies-cover-money-transfers-of-terrorists-traffickers-rough-states-treasury-official-warns

Citations

[1] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. 3
[2] Health and Human Services, http://hhs.gov/sites/default/files/Factsheet-opioids-061516.pdf
[3] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. 11
[4] Centers for Disease Control and Prevention, *Injury Prevention & Control: Opioid Overdose*, http://www.cdc.gov/drugoverdose/epidemic/index.html
[5] The White House, *FACT SHEET: Obama Administration Announces Public and Private Sector Efforts to Address Prescription Drug Abuse and Heroin Use* (2015), https://www.whitehouse.gov/the-press-office/2015/10/21/fact-sheet-obama-administration-announces-public-and-private-sector
[6] National Institute on Drug Abuse, *What is the Federal Government Doing to Combat the Opioid Abuse Epidemic?* (2015), Presented by Nora D. Volkow, Director, National Institute on Drug Abuse, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations https://www.drugabuse.gov/about-nida/legislative-activities/testimony-to-congress/2016/what-federal-government-doing-to-combat-opioid-abuse-epidemic
[7] National Institute on Drug Abuse, *America's Addiction to Opioids: Heroin and Prescription Drug Abuse* (2014), Presented by Nora D. Volkow, M.D., Senate Caucus on International Narcotics Control, https://www.drugabuse.gov/about-nida/legislative-activities/testimony-to-congress/2016/americas-addiction-to-opioids-heroin-prescription-drug-abuse , figure 3
[8] Lenny Bernstein, "Why a bag of heroin costs less than a pack of cigarettes", *Washington Post*, August 27, 2015, https://www.washingtonpost.com/news/to-your-health/wp/2015/08/27/why-a-bag-of-heroin-costs-less-than-a-pack-of-cigarettes-2/
[9] Sergeant Stephen Opferman of the Los Angeles County Sheriff's Department, quoted by CNN (2011) http://money.cnn.com/2011/06/01/news/economy/prescription_drug_abuse/
[10] Centers for Disease Control and Prevention. Morbidity and Mortality Weekly Report, (2011), http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6043a4.htm?s_cid=mm6043a4_w#fig2
[11] National Institute on Drug Abuse, *America's Addiction to Opioids: Heroin and Prescription Drug Abuse* (2014), Presented by Nora D. Volkow, M.D., Senate Caucus on International Narcotics Control, https://www.drugabuse.gov/about-nida/legislative-activities/testimony-to-congress/2016/americas-addiction-to-opioids-heroin-prescription-drug-abuse
[12] Michael Botticelli, Director of the National Drug Control Policy, White House quoted in WNYT (2016) http://wnyt.com/news/white-house-drug-policy-director-albany-heroin-epidemic-public-health-epidemic/4158338/
[13] The White House, *How Illicit Drug Use Affects Business and the Economy*, https://www.whitehouse.gov/ondcp/ondcp-fact-sheets/how-illicit-drug-use-affects-business-and-the-economy
[14] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. 23
[15] Drug Enforcement Administration, *Programs: Money Laundering*, https://www.dea.gov/ops/money.shtml
[16] ibid pg. 3
[17] John Cassara, "Predictive Analytics: The Future of Successful Law Enforcement?", *Government Computer News* (2013), accessed from: http://www.johncassara.com/articles.html
[18] Internal Revenue Service, *Overview – Money Laundering*, https://www.irs.gov/uac/overview-money-laundering
[19] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. -19

[20] Raymond Baker, "Incorporation Transparency Laws", *Huffington Post* November 4th, 2009, Accessed from: http://www.gfintegrity.org/press-release/updating-incorporation-transparency-laws/
[21] Kevin G. Hall and Marisa Taylor, "The Crux Over Shell Companies: Who are the True Owners?", *McClatchy DC*, April 7th 2016, http://www.mcclatchydc.com/news/nation-world/national/article70602352.html
[22] Global Financial Integrity, *Anonymous Companies,* http://www.gfintegrity.org/issue/anonymous-companies/
[23] *The Buck Stops Here: Improving U.S. Anti Money Laundering Practices*, a report by the United States Senate Caucus on International Narcotics Control (April 2013), pg. 24
[24] Paul Fitzgerald, "It's Time for Congress to Stop 'Financial Getaway Cars'", *The Des Moines Register,* May 12th, 2016 http://www.desmoinesregister.com/story/opinion/abetteriowa/2016/05/12/s-time-congress-stop-financial-getaway-cars/84250750/
[25] Federal Bureau of Investigation, *Crime in the United States: 2014,* https://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2014/crime-in-the-u.s.-2014/persons-arrested/main
[26] Cyrus Vance Jr., District Attorney for New York County, State of New York, op-ed published by Reuters, October 9, 2012.
[27] Drug Enforcement Administration, *Programs: Money Laundering,* https://www.dea.gov/ops/money.shtml
[28] Janice Ayala, Deputy Assistant Director, Office of Investigations, U.S. Immigration and Customs Enforcement, Testimony before the Committee on Homeland Security and Government Affairs, June 18, 2009
[29] Cyrus Vance Jr., District Attorney for New York County, State of New York, included in his testimony before the U.S. House of Representatives Task Force to Investigate Terrorism Finance, June 24, 2015.
[30] "U.S. Shell Companies Cover Money Transfers of Terrorists, Traffickers, Rough States; Treasury Official Warns", *Daily Sabah Americas,* July 12th 2016
[31] Daniel Glaser, Asst. Secretary for Terrorist Financing, U.S. Department of the Treasury, Testimony before the Senate Committee on the Judiciary, November 1, 2011
[32] Drug Enforcement Administration, "Nationwide Oxycodone Trafficking Ring Dismantled", April 29th, 2013 https://www.dea.gov/divisions/sea/2013/sea042913.shtml
[33] "High Profit Investments, LLC.", https://opencorporates.com/companies/us_nv/E0845552006-6
[34] "GC National Wholesale INC", https://opencorporates.com/companies/us_ca/C3441251
[35] "Nationwide Payment Solutions, INC." https://opencorporates.com/companies/us_ca/C3698786
[36] "FMC Distributors, INC." https://opencorporates.com/companies/pr/90905-111
[37] The Department of Justice, "Thirty-Three Defendants Charged in Massive Criminal Conspiracies Including Allegations of Fraud, Prescription Drug Diversion, and Money Laundering" May 7th, 2015 https://www.justice.gov/opa/pr/thirty-three-defendants-charged-massive-criminal-conspiracies-including-allegations-fraud
[38] "Dominion Investments Limited" https://opencorporates.com/companies/bs/19800B
[39] Drug Enforcement Administration, "International Money Manager Pleads Guilty to Laundering Drug Proceeds in Government Sting", November 21st 2006, https://www.dea.gov/pubs/states/newsrel/nyc112106.html
[40] Alfonso Chardy, "2 South Florida Men are Arrested on Money Laundering Charges", *Miami Herald,* December 19th, 2014, http://www.miamiherald.com/news/local/crime/article4677768.html
[41] ibid
[42] The United States Attorney's Office, Southern District of Florida, "Second Defendant Sentenced for Laundering over $400,000 in Currency from Purported Narcotics Transactions",

January 28th 2015 https://www.justice.gov/usao-sdfl/pr/second-defendant-sentenced-laundering-over-400000-currency-purported-narcotics

[43] "ZAN Providers, LLC" https://opencorporates.com/companies/us_ky/0851952

[44] "R.C. & Son Enterprise, LLC" https://opencorporates.com/companies/us_fl/L10000064587

[45] "La Hacienda (USA), LLC" https://opencorporates.com/companies/us_fl/L99000003231

[46] "Running Brook, LLC" https://opencorporates.com/companies/us_fl/L00000010931

[47] "La Hacienda (USA), LLC" http://www.companies-florida.com/la-hacienda-usa-llc-1ao9h/

[48] Drug Enforcement Administration, "Peruvian Kingpin and his Wife Indicted", July 27th 2007 https://www.dea.gov/pubs/states/newsrel/mia072707.html

[49] "Pacific Gateway Corp." https://opencorporates.com/companies/us_fl/P07000054235
"Advancer Logistics, LLC" https://opencorporates.com/companies/us_fl/L11000100906
"Exim Logistics Corp" https://opencorporates.com/companies/us_fl/P10000010063

[50] Drug Enforcement Administration, "Manhattan U.S. Attorney Announces Seizure of Over $31 Million in Connection with an International Drug Trafficking and Money Laundering Scheme", October 10, 2012 https://www.dea.gov/divisions/nyc/2012/nyc101012.shtml

[51] "Big Dog Sports Memorabilia Inc." https://opencorporates.com/companies/us_wy/2014-000663606

[52] The Department of Justice, "Twenty-Two Charged with Racketeering Conspiracy and Related Crimes Involving Drug Trafficking, Illegal Gambling and Money Laundering", January 27th, 2016 https://www.justice.gov/usao-sdca/pr/twenty-two-charged-racketeering-conspiracy-and-related-crimes-involving-drug

[53] "J&G Enterprises I, LLC." https://opencorporates.com/companies/us_oh/1549532

[54] Ohio Secretary of State's Office, Business filing portal, business search for 'J&G Enterprises I LLC' http://www5.sos.state.oh.us/ords/f?p=100:7:0::NO:7:P7_CHARTER_NUM:1549532

[55]Federal Bureau of Investigation, Cleveland Division, "Eight people indicted for roles in large-scale heroin trafficking and money laundering ring", May 12th 2011, https://www.fbi.gov/cleveland/press-releases/2011/eight-people-indicted-for-roles-in-large-scale-heroin-trafficking-and-money-laundering-ring

[56] Peter Krouse, "Heroin ring laundered drug money through luxury cars and real estate", *Cleveland.com,* May 13th 2011, http://blog.cleveland.com/metro/2011/05/post_459.html

[57] New York Times, A drug family in the winner's circle, 12 June 2012, http://www.nytimes.com/2012/06/13/us/drug-money-from-mexico-makes-its-way-to-the-racetrack.html?_r=0

[58] FBI, Federal grand jury indicts Los Zetas leader in money laundering scheme, http://www.fbi.gov/sanantonio/press-releases/2012/federal-grand-jury-in-texas-indicts-los-zetas-leader-in-money-laundering-scheme

[59] The Guardian, Mexico captures Zetas leader Miguel Angel Treviño Morales, known as Z-40, http://www.theguardian.com/world/2013/jul/16/mexico-drugs-trade

[60] U.S. Attorney's Office Western District of Texas, "Austin Horse Trainer Sentenced To Federal Prison In Multi-Million Dollar Money Laundering Conspiracy Involving Los Zetas Drug Trafficking Proceeds, Extortion, And Bribery", http://www.justice.gov/usao/txw/news/2013/Zetas_sentencings_2nd.html; Borderl and Beat, Carlos Nayen Borbolla sentenced to 15 years in zetas money laundering case, http://www.borderlandbeat.com/2013/12/carlos-nayen-borbolla-sentenced-to-15.html

[61] The Great Rip Off Map, "Los Zetas Drug Trafficking in Racehorse Scandal" http://greatripoffmap.globalwitness.org/#!/case/58010

[62] FBI, Top ten fugitives, http://www.fbi.gov/news/stories/2009/october/mogilevich_102109

[63] U.S. District Court for the Eastern District of Pennsylvania, USA vs. Semion Mogilevich, Superseding Indictment, pages 14-15, https://www.documentcloud.org/documents/1278690-indictment-%20mogilevich.html#annotation/a175321 and https://www.documentcloud.org/documents/1278690-indictment-mogilevich.html#annotation/a175322

and https://www.documentcloud.org/documents/1278690-indictment-mogilevich.html#annotation/a175322

[64] U.S. District Court for the Eastern District of Pennsylvania, USA vs. Semion Mogilevich, Superseding Indictment, https://www.documentcloud.org/documents/1278690-indictment-mogilevich.html#annotation/a175320

[65] The Great Rip Off Map, "Russian Crime Boss Conned Investors out of Millions" http://greatripoffmap.globalwitness.org/#!/case/57957

FACTCOALITION
Financial Accountability & Corporate Transparency

March 13, 2019

The Honorable Maxine Waters
Chairwoman
U.S. House Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Patrick McHenry
Ranking Member
U.S. House Committee on Financial Services
4340 O'Neill House Office Building
Washington, D.C. 20024

Re: Kleptocracy Asset Recovery Rewards Act (H.R. 389)

Dear Chairwoman Waters and Ranking Member McHenry,

We are writing on behalf of the Financial Accountability and Corporate Transparency (FACT) Coalition to convey our support for the Kleptocracy Asset Recovery Rewards Act (H.R. 389), sponsored by Representatives Stephen Lynch (D-MA), Ted Budd (R-NC), and Steve Cohen (D-TN).

The FACT Coalition is a non-partisan alliance of more than 100 state, national, and international organizations promoting policies to combat the harmful impacts of corrupt financial practices.[1]

H.R. 389 would establish a rewards program for whistleblowers — encouraging individuals to inform the U.S. government about assets in the U.S. financial system that are connected to foreign corruption, enabling authorities to reclaim and return the money and deter foreign corruption moving forward.

Foreign corruption is a major economic and national security threat to the United States. Corruption undermines the rule of law, provides the lifeblood of authoritarian regimes and enables transnational organized crime to flourish. It diverts precious resources away from those who most need them, and fosters disillusionment with government — sometimes leading to the rise of terrorist networks.

The bipartisan Kleptocracy Asset Recovery Rewards Act is a sensible tool to safeguard American citizens and businesses from the scourge of corruption.

Should you have any questions, please feel free to contact Clark Gascoigne at +1 (202) 810-1334 or cgascoigne@thefactcoalition.org.

Sincerely,

Gary Kalman
Executive Director
The FACT Coalition

Clark Gascoigne
Deputy Director
The FACT Coalition

CC Members of the House Financial Services Committee

[1] For a full list of FACT Coalition members, visit https://thefactcoalition.org/about/coalition-members-and supporters/

The Washington Post

Opinions

Putin and other authoritarians' corruption is a weapon — and a weakness

By David Petraeus and
Sheldon Whitehouse
March 8

David Petraeus is a retired U.S. Army general and the former director of the Central Intelligence Agency. Sheldon Whitehouse, a Democrat, is a U.S. senator from Rhode Island.

Thirty years after the end of the Cold War, the world is once again polarized between two competing visions for how to organize society. On one side are countries such as the United States, which are founded on respect for the inviolable rights of the individual and governed by rule of law. On the other side are countries where state power is concentrated in the hands of a single person or clique, accountable only to itself and oiled by corruption.

Alarmingly, while Washington has grown ambivalent in recent years about the extent to which America should encourage the spread of democracy and human rights abroad, authoritarian regimes have become increasingly aggressive and creative in attempting to export their own values against the United States and its allies. Russian President Vladimir Putin and other authoritarian rulers have worked assiduously to weaponize corruption as an instrument of foreign policy, using money in opaque and illicit ways to gain influence over other countries, subvert the rule of law and otherwise remake foreign governments in their own kleptocratic image.

In this respect, the fight against corruption is more than a legal and moral issue; it has become a strategic one — and a battleground in a great power competition.

Yet corruption is not only one of the most potent weapons wielded by America's authoritarian rivals, it is also, in many cases, what sustains these regimes in power and is their Achilles' heel.

For figures such as Putin, the existence of America's rule-of-law world is intrinsically threatening. Having enriched themselves on a staggering scale — exploiting positions of public trust for personal gain — they live in fear that the full extent of their thievery could be publicly exposed, and that the U.S. example might inspire their people to demand better.

Corrupt regimes also know that, even as they strive to undermine the rule of law around the world, they are simultaneously dependent on it to a remarkable degree. In contrast to the Cold War, when the Soviet bloc was sealed off from the global economy and sustained by its faith in communist ideology, today's autocrats and their cronies cynically seek to spend and shelter their spoils in democratic nations, where they want to shop, buy real estate, get health care and send their children to school.

Ironically, one of the reasons 21st-century kleptocrats are so fixated on transferring their wealth to the United States and similar countries is because of the protections afforded by the rule of law. Having accumulated their fortunes illegally, they are cognizant that someone more connected to power could come along and rob them too, as long as their loot is stuck at home.

Fortunately, the United States has begun to take steps to harden its rule-of-law defenses and push back against foreign adversaries. The passage of the Global Magnitsky Act in 2016, for instance, provided a powerful new tool for targeting corruption worldwide that is being increasingly utilized. But there is more to do.

In particular, the United States should make it more difficult for kleptocrats, and their agents, to secretly move money through the rule-of-law world, whether by opening bank accounts, transferring funds or hiding assets behind shell corporations. Failure to close loopholes in these areas is an invitation to foreign interference in America's democracy and a threat to national sovereignty.

Congress should tighten campaign-finance laws to improve transparency given that U.S. elections are clearly being targeted for manipulation by great-power competitors.

At the same time, the United States must become more aggressive and focused on identifying and rooting out corruption overseas. Just as the Treasury Department has developed sophisticated financial-intelligence capabilities in response to the threat of terrorism and weapons of mass destruction, it is time to expand this effort to track, disrupt and expose the corrupt activities of authoritarian competitors and those aligned with them.

Hardening the nation's rule-of-law defenses is not, of course, a substitute for traditional forms of U.S. power, including military strength and economic dynamism. But it can provide an additional set of tools to bolster national security.

In the intensifying worldwide struggle between the rule of law and corruption, the United States cannot afford neutrality. Complacency about graft and kleptocracy beyond U.S. borders risks complicity in it — with grave consequences both for the nation's reputation abroad and Americans' well-being at home.

Read more:

Catherine Rampell: The GOP has become the Soviet party

Letters to the Editor: 'Kleptocracy' is the key

Anne Applebaum: Trump is hinting at concessions to Putin. So what do we get back?

Opinion: Manafort trial coverage is missing a key issue: Kleptocracy

March 11, 2019

Bob Carlson
President, American Bar Association
321 North Clark Street
Chicago, IL 60654

Re: Beneficial Ownership Legislation

Dear President Carlson,

We write to ask the ABA to reconsider its opposition to legislation to be submitted to the Financial Services Committee of the US House of Representatives later this month, which would require U.S. corporations and LLCs formed in any of the 50 states to disclose their beneficial owners. As we understand it, the new version of the legislation will eliminate the concern regarding interference with the attorney client relationship that was at the heart of the ABA's opposition to prior versions.

Who we are

We are lawyers with expertise in the field of business and human rights[1], a field that has grown rapidly following the unanimous endorsement by the UN Human Rights Council of the UN Guiding Principles on Business and Human Rights (UNGPs) in 2011[2], which the ABA also endorsed in February 2012[3]. Many of us are ABA members who worked to secure that endorsement and/or have been involved in the Association's efforts to advance the UNGPs since then.

The UNGPs have become "the global authoritative standard, providing a blueprint for the steps all states and businesses should take to uphold human rights."[4] They are increasingly reflected in national laws and regulations, in the work of multi-stakeholder and standard-setting bodies, in the practices and policies of leading companies, and in the advocacy of civil society.

The ABA's opposition to modern slavery

Commendably, the ABA has also called for the elimination of slavery in all its modern forms, including: forced labor; sex trafficking, labor trafficking, trafficking in persons;

---

[1] We are signing this letter in our personal capacities only. Affiliations, where listed, are solely for identification purposes.

[2] Guiding Principles on Business and Human Rights (2011), available at https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf

[3] ABA House of Delegates Resolution 109, available at https://www.americanbar.org/content/dam/aba/administrative/human_rights/hod_midyear_109.authcheckdam.pdf .

[4] Zeid Ra'ad Al Hussein, 'Ethical Pursuit of Prosperity' (23 March 2015), available at https://www.lawgazette.co.uk/comment-and-opinion/ethical-pursuit-of-prosperity/5047796.article .

and trafficking in women and children. The ABA has urged governments around the world, the private sector, and the legal community to take strong action to combat modern slavery.

Beneficial ownership legislation is essential to fight sex trafficking and other human rights abuses involving U.S. companies

As lawyers involved in business and human rights issues, we believe that it is critically important for the U.S. Congress to fight modern slavery and other human rights abuses by passing beneficial ownership legislation that enables sex traffickers and other rights abusers to flourish in the U.S.

The need for such legislation is urgent, as highlighted by the recent solicitation charges filed against hundreds of men in Florida for use of illicit massage parlors that are engage in sex trafficking. According to a very recent New York Times article[5], this use of massage parlors "has exploded into a $3 billion-a-year sex industry that relies on pervasive secrecy, close-knit ownership rings and tens of thousands of mostly foreign women ensnared in a form of modern indentured servitude." However, the article points out that law enforcement efforts to combat sex trafficking outlets is hamstrung by the opacity of their ownership structures:

> Above these site managers is usually a person who appears on paperwork as the massage parlor owner, but is often just a frontman running a shell company. The payouts from the shell company go to what is legally known as the "beneficial owner."
>
> "Very little is known of the behind-the-scene owners," Mr. Myles [of Polaris Project, an anti-trafficking organization] said. "They are hiding behind shell companies, hiding behind mamasans. They are hiding behind fake people."

This is not new. Lack of transparency of beneficial ownership is absolutely essential for sex trafficking schemes like this to grow and prosper. It is also essential for facilitating a wide range of abuses, including the use by kleptocrats of anonymous U.S. companies to shield their assets and their activities from scrutiny.[6]

The new bill will address the ABA's core concern regarding interference with the attorney client relationship

---

[5] Nicholas Kulish, Frances Robles and Patricia Mazzei, *Behind Illicit Massage Parlors Lie a Vast Crime Network and Modern Indentured Servitude* (March 2, 2019), available at https://www.nytimes.com/2019/03/02/us/massage-parlors-human-trafficking.html .

[6] For example, the laundering in the U.S. of Equatorial Guinea's sovereign wealth, which was siphoned off by its kleptocratic ruling family. See, e.g., *United States of America v One White Crystal-Covered "Bad Tour" Glove and other Michael Jackson Memorabilia, Real Property Located on Streetwater Mesa Road in Malibu, California, One 2011 Ferrari 599 GTO*, Second Amended Verified Complaint, USDC CDCal, No. CV 2 11-3582-GW-SS (June 11, 2012); and Lisa Mosal, *Manna From Heaven"? How Health and Education Pay the Price for Self- Dealing in Equatorial Guinea* (June 15, 2017), available at https://www.hrw.org/report/2017/06/15/manna-heaven/how-health-and-education-pay-price-self-dealing-equatorial-guinea

Yet the ABA to date has opposed prior versions of the legislation that would create a central register of beneficial ownership information for U.S. corporations and LLCs. The ABA has raised a number of objections, but its core issue appears to be grounded in concerns that the legislation would interfere with the attorney-client relationship.

As we understand it, however, the new bill to be submitted to the Financial Services Committee of the House of Representatives would eliminate that fundamental concern. Earlier versions of the bill would have subjected formation agents to anti-money laundering (AML) rules applicable to banks, including the need to establish AML programs and filing suspicious activity reports (SARs) with the Treasury Department. This would have included lawyers helping applicants without U.S. passports or drivers licenses if the lawyer did not contract to a separate formation agent in the U.S.

The new bill has removed language that would subject formation agents (including lawyers) to the AML rules. With that removal, the basis for the ABA's core concern about interference with the attorney-client relationship disappears.

The ABA should reconsider its opposition to transparency reform of beneficial ownership of U.S. companies

Given the widespread and severe human rights abuse suffered by many human beings by slavery; the ABA's endorsement of the UNGPs and its strong commitment to end slavery; and the essential role played by lack of corporate transparency in enabling such abuse, we respectfully urge the ABA to reconsider its opposition to transparency reform on beneficial ownership of U.S. companies.

Thank you for considering this new information. We would be pleased to address any questions you or your staff may have.

Sincerely,

John F. Sherman, III, Esq.
Former adviser to the Special Representative of the UN Secretary General on Business and Human Rights, Professor John G. Ruggie, author of the UN Guiding Principles on Business and Human Rights.
Former co-chair, International Bar Association Corporate Social Responsibility Committee
Former chair, International Bar Association Business and Human Rights Working Group
General Counsel and Senior Advisor, Shift
Boston, Massachusetts

Douglass Cassel, Esq.
Emeritus Professor of Law, Notre Dame Law School
New York, New York

Carey R. D'Avino, Esq.
New York, New York

Elise Groulx Diggs, Esq., Ad.E. LL.M
Washington, DC
Convener of the Business and Human Rights Advisory Board of the American Bar Association Center for Human Rights
Vice-chair of the Business and Human Rights Committee of the International Bar Association.
Doughty Street Chambers, London, UK

Anthony Ewing, Esq.
Lecturer in Law, Columbia Law School
Co-Director, Teaching Business and Human Rights Forum
New York, New York

Silvia M. Garrigo, Esq.
Key Biscayne, Florida

Vivek Krishnamurthy, Esq.
Lecturer on Law, Harvard Law School
Affiliate, Berkman Klein Center for Internet & Society, Harvard University
Senior Fellow, Carr Center for Human Rights Policy, Harvard Kennedy School
Cambridge, Massachusetts

Amy K. Lehr, Esq.
Former adviser to the Special Representative of the UN Secretary General on Business and Human Rights, Professor John G. Ruggie, author of the UN Guiding Principles on Business and Human Rights
Washington, D.C.

Mitt Regan, Esq.
McDevitt Professor of Jurisprudence
Director, Center on Ethics and the Legal Profession
Co-Director, Center on National Security and the Law
Georgetown University Law Center
and
Senior Fellow, Stockdale Center for Ethical Leadership
United States Naval Academy
Washington, DC

Gare A. Smith, Esq.
Chair, Corporate Social Responsibility Practice
Foley Hoag, LLP
Washington, DC

Robert C. Thompson, Esq.
Member, Working Group on Business and Human Rights Arbitration
New York, New York

Copies to:

Holly Cook
Director, ABA Governmental Affairs Office
1050 Connecticut Ave, NW
Washington, DC 20036

The Honorable Maxine Waters
Chairwoman, Financial Services Committee
United States House of Representatives
Washington, DC 20024

The Honorable Patrick MacHenry
Ranking Member, Financial Services Committee
United States House of Representatives
Washington, DC 20515