AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

MANAGING TERRORISM FINANCING RISK IN REMITTANCES AND MONEY TRANSFERS

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JULY 18, 2017

Printed for the use of the Committee on Financial Services

Serial No. 115–32



U.S. GOVERNMENT PUBLISHING OFFICE

29–451 PDF WASHINGTON : 2018

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

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

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

KIRSTEN SUTTON MORK, *Staff Director*

SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

STEVAN PEARCE, New Mexico *Chairman*

ROBERT PITTENGER, North Carolina, *Vice Chairman*
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee

ED PERLMUTTER, Colorado, *Ranking Member*
CAROLYN B. MALONEY, New York
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
RUBEN KIHUEN, Nevada
STEPHEN F. LYNCH, Massachusetts

CONTENTS

Page

Hearing held on:
July 18, 2017 1
Appendix:
July 18, 2017 33

WITNESSES

TUESDAY, JULY 18, 2017

Cassara, John, Member, Board of Advisors, Center on Sanctions and Illicit Finance, Foundation for Defense of Democracies 9
DeVille, Duncan, Global Head of Financial Crimes Compliance & US BSA Officer, The Western Union Company 5
Oppenheimer, Matthew, Co–Founder and Chief Executive Officer, Remitly, Inc. 7
Paul, Scott T., Chief Humanitarian Policy Advisor, Oxfam America 10

APPENDIX

Prepared statements:
Cassara, John 34
DeVille, Duncan 51
Oppenheimer, Matthew 58
Paul, Scott T. 62

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Pearce, Hon. Stevan:
Written statement of Bradley S. Lui, on behalf of The Money Services Round Table 73
Ellison, Hon. Keith; and Vargas, Hon. Juan:
Written responses to questions for the record submitted to Duncan DeVille 81
Written responses to questions for the record submitted to Matthew Oppenheimer 89
Written responses to questions for the record submitted to Scott T. Paul .. 93
Perlmutter, Hon. Ed:
Written statement of the Electronic Transactions Association 98
Written statement of various undersigned organizations 99
Letter to Hon. Mike Rogers from Bradley S. Lui, on behalf of The Money Services Round Table, dated May 2, 2017 100
Letter to Hon. Paul Battles from Western Union and MoneyGram, dated February 3, 2017 106

MANAGING TERRORISM FINANCING RISK IN REMITTANCES AND MONEY TRANSFERS

Tuesday, July 18, 2017

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TERRORISM
AND ILLICIT FINANCE,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:40 p.m., in room 2128, Rayburn House Office Building, Hon. Stevan Pearce [chairman of the subcommittee] presiding.

Members present: Representatives Pearce, Pittenger, Rothfus, Messer, Tipton, Williams, Poliquin, Love, Hill, Emmer, Zeldin, Davidson, Budd, Kustoff; Perlmutter, Maloney, Himes, Foster, Sinema, Vargas, Gottheimer, Kihuen, and Lynch.

Ex officio present: Representatives Hensarling and Waters.

Also present: Representatives Heck and Ellison.

Chairman PEARCE. The Subcommittee on Terrorism and Illicit Finance 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 the Subcommittee on Terrorism and Illicit Finance may participate in today's hearing.

Without objection, the gentleman from Washington, Mr. Heck, is permitted to participate in today's subcommittee hearing. Mr. Heck is a member of the Financial Services Committee, and we appreciate his interest in this important topic. Welcome, Mr. Heck.

Today's hearing is entitled, "Managing Terrorism Financing Risk in Remittances and Money Transfers." I now recognize myself for 5 minutes to give an opening statement.

I want to thank everyone for joining us today for this hearing. Today, we are examining the terrorism financing risk for money services, businesses, and remittances. As the Treasury Department noted in its 2015 National Terrorism Financing Risk Assessment, the fight against money laundering and terrorist financing is a pillar of U.S. national security and a strong financial system. It is essential that we work closely together to develop and effectively implement strong, focused, and reasonable laws and regulations to detect, disrupt, deter, and prevent terrorist finance.

The threat from terrorist financing in particular is constantly evolving and requires diligent adaptation by law enforcement, fi-

nancial regulators, intelligence agencies, policymakers, and the financial sector.

This hearing will explore the terrorist illicit financing risks that are inherent in the use of money services business (MSBs), remittance payments, and other value transfer systems, as well as how efforts to combat this activity have unintentionally contributed to the problem of de-risking.

The hearing will explore both formal and informal value transfer systems, including the extent to which de-risking excludes entire groups of customers from the financial system and less transparent underground, unregulated systems which are more difficult to track and easier for bad actors to successfully transfer funds.

The scourge of terrorist finance isn't a new problem, but I hope that today we can shed some new light on this issue and help inform this subcommittee on ways in which we can help disrupt that flow of money. I would like to thank our witnesses for being here today and I look forward to the conversation to come.

I now recognize the ranking member of the subcommittee, the gentleman from Colorado, Mr. Perlmutter, for 2 minutes for an opening statement.

Mr. PERLMUTTER. Thanks, Mr. Chairman. I want to thank all of our witnesses for testifying today, but in particular I want to welcome Duncan DeVille of Western Union, and also my friend, Tim Daly, whom I see sitting behind you. Western Union is the largest money transmitter in the world. It is located in the Denver metropolitan area just outside of my Congressional district. Thank you for being here.

We live in a world of rapidly evolving threats and rapidly evolving technology. The adoption of technology has not only reduced the cost of sending money abroad, but created efficiencies benefiting consumers, markets, and the law enforcement community. But as technology has advanced, so too have the terrorists and criminals.

I am certain we already are and will continue to harness new technologies to stop the flow of funds to the bad guys. Criminals will always search out the unregulated channels to access funding, but if we strike the appropriate balance, we can mitigate the concern of this de-risking phenomena and ensure that companies like Western Union are not at risk of losing their settlement banking relationships. This would drive all activity underground, only exacerbating the national security risks.

So I hope the conclusion we come to today is that we can manage terrorist financing risks associated with remittances and money transfers without destroying the marketplace either through excessive compliance regimes or taxing remittances.

Let me also say at the outset, I strongly oppose H.R. 1834, the Taxing Remittances to Pay for the Border Wall Act, and I look forward to discussing further this subject further with our witnesses. And with that, I yield back.

Chairman PEARCE. The gentleman yields back.

The Chair now recognizes Mr. Pittenger for 1 minute.

Mr. PITTENGER. Thank you, Mr. Chairman. I would like to thank all of our distinguished panelists for lending their expertise to our subcommittee today.

I am particularly glad to see our good friend, John Cassara, on the panel testifying today. I am so grateful for the exceptional partner he has been with us over the last few years, having spoken at a number of our parliamentary security forums for members of parliament.

Mr. Chairman, this hearing is particularly timely and relevant to my interests in reforming financial institution information-sharing mechanisms. As many of you know, I have worked to streamline and improve Sections 314(a) and (b) of the USA PATRIOT Act, which govern bank-to-government and bank-to-bank information-sharing. When we make it easier for banks and money services businesses to talk to each other and better identify money laundering terror financing threats, we not only improve government enforcement, but we also improve institutional compliance with the laws and support our efforts related to privacy.

And in the process of improving compliance, we actually offset many of the concerns related to de-risking and creating financial services vacuums in the very areas where we seek better enforcement. Mr. Chairman, thank you for hosting today's important hearing, and I yield back.

Chairman PEARCE. The gentleman's time has expired. The Chair now recognizes Mr. Emmer for 2 minutes.

Mr. EMMER. Thank you, Mr. Chairman, for yielding, and for organizing this important hearing.

I would also like to thank our witnesses for being here. Your insights and experiences are extremely valuable to this subcommittee and this Congress as we examine the intricate and evolving nature of how terror organizations finance their operations.

The hundreds of billions of dollars in remittances and other value transfer payments sent around the globe each year play an important role in the lives of millions. These transfers can help stabilize an individual's household or even an entire economy's finances, and in many cases serve as an important and vital lifeline among family members and loved ones separated around the globe. That is why today's hearing is so important.

While much of the estimated $575 billion in remittances sent globally in 2016 went to support livelihoods and the well-being of relatives, these transfers were also vulnerable to exploitation by criminal and terror organizations. For decades, our intelligence and terror financing communities have held that without money, there is no terrorism.

I believe this mantra holds true and I am encouraged to see the subcommittee undertake the important challenge of reviewing our Nation's anti-money-laundering and counterterrorist financing laws to ensure our regulatory framework allows for the continued flow of money to friends and family members abroad while eliminating the use of remittances as a means to conduct acts of terror both overseas and here at home.

Striking this important balance, however, is especially relevant, as I represent one of the largest and most diverse refugee populations in the country. Many are surprised to learn that Minnesota has the largest number of refugees per capita in the United States and ranks first in the Nation for secondary migration, or refugees who have resettled in Minnesota from other U.S. States.

The Sixth Congressional District in particular is home to one of the largest populations of Somali-Americans in the country, a population that relies heavily on the use of money services businesses and other forms of transfer to send money to family members abroad. While an estimated $200 million in remittances is sent to Somalia every year, the channels to send these funds are rapidly changing.

The lack of sufficient banking infrastructure and the spread of Al-Shabaab in countries like Somalia have made it difficult for money remittance transmitters and financial institutions to verify their customers and ensure remittances are being used for legitimate purposes.

Although the practice of de-risking is not a new phenomenon that financial institutions have employed to mitigate risk associated with remittances, I am concerned that the continued use of such techniques may have a wider, more detrimental impact to our ability to track the flows of money to finance terror operations globally.

Eliminating funding streams to terrorists and keeping families connected do not have to mutually exclusive, and I have no doubt we can improve our regulatory system to accomplish these goals.

Again, I want to thank the chairman for holding this important hearing today.

Chairman PEARCE. The gentleman's time has expired.

We now welcome the testimony of our witnesses. First, Mr. Duncan DeVille is senior vice president at Western Union where he serves as global head of financial crimes compliance, and as BSA officer. Previously, Mr. DeVille served as head of the Office of Compliance and Enforcement at FinCEN; as a Senior Financial Enforcement Adviser at the U.S. Treasury Department Office of International Affairs; as an Adviser with the Department of Defense in Iraq; and in a series of prosecutorial positions at the Federal, State, and local government levels. Mr. DeVille has earned his law degree from the University of Denver, and other graduate degrees from Harvard University and Oxford University, and his bachelor's degree from the University of Louisiana. Thanks for being here, Mr. DeVille.

Next, we have Mr. John Cassara. Mr. Cassara is a member of the board of advisers for the Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies. Mr. Cassara began his 26-year government career as an intelligence officer during the Cold War. He later served as a Treasury Special Agent in both the U.S. Secret Service and the U.S. Customs Service, where he investigated money laundering, trade fraud, and international smuggling. He was an undercover arms dealer for 2 years. Assigned overseas, he developed expertise in Middle East money laundering, value transfer, and underground financial systems. Mr. Cassara also worked 6 years for Treasury's Financial Crimes Enforcement Network and was detailed to the Department of State's Bureau of International Narcotics and Law Enforcement Affairs.

Mr. Scott T. Paul is the humanitarian policy lead at Oxfam America, where he spearheads the organization's advocacy on a number of crises and cross-cutting humanitarian issues. Mr. Paul previously worked for the Civic, an organization that seeks to make

warring parties more responsible to civilians, where he initiated civics work on the conflict in Somalia and directed its Making Amends campaign. Mr. Paul also serves as deputy director, government relations, at Citizens for Global Solutions, where he led numerous coalition-based campaigns to promote a vision of U.S. foreign policy centered on cooperation, pragmatism, and the rule of law.

Mr. Heck will introduce our next witness, Mr. Oppenheimer. So, Mr. Heck, you are recognized for the introduction.

Mr. HECK. Thank you, Mr. Chairman, very much. I am proud to be able to introduce my friend, Matthew Oppenheimer, the cofounder and CEO of Remitly, which is yet another Seattle-based success story of a company. They provide low-cost remittances to Latin America, India, and the Philippines.

Matthew's resume is impressive, indeed. It combines almost all the issues that make me excited about the opportunity to work together on this committee. He worked for Barclays Bank, where he rose to become head of mobile banking in Kenya. If you understand that, you understand that is quite a success story in and of itself. And he co-founded Remitly to bring fintech innovation to bear on an old problem.

And in dealing day in and day out with Bank Secrecy Act regulation, I know for a fact he has lots of ideas on how these can be made to be more efficient and effective. I look forward to hearing his testimony, and I am sure that if we all do so, we can, indeed, find several opportunities to work across the aisle on mobile banking and fintech regulation and Bank Secrecy Act modernization and strike, as my dear friend, Mr. Perlmutter, says, that appropriate balance.

Welcome to the committee. And thank you for making that trip I make a couple of times of a week.

Chairman PEARCE. Each of you is going to be recognized for 5 minutes to give an oral presentation of your testimony. And without objection, each of your written statements will be made a part of the hearing record.

Mr. DeVille, you are now recognized for 5 minutes.

STATEMENT OF DUNCAN DEVILLE, GLOBAL HEAD OF FINANCIAL CRIMES COMPLIANCE & US BSA OFFICER, THE WESTERN UNION COMPANY

Mr. DEVILLE. Good afternoon, Chairman Pearce, Ranking Member Perlmutter, and members of the subcommittee. Thank you for inviting me here today to discuss ways to detect and combat the use of money services businesses, or MSBs, by terrorist organizations and to talk about Western Union's efforts and how various programs in our compliance umbrella have changed over time.

Western Union's worldwide network includes more than a half million agent locations in over 200 countries and territories. In 2016, across all our products and platforms, Western Union averaged 31 transactions per second and over 900 per second at peak times. For Western Union, a critical part of serving our customers is complying with regulatory requirements. Even though regulatory compliance costs money and inhibits our ability to drive down transaction costs for our customers, we do not view these compli-

ance and customer service goals as conflicting, but as complementary.

Our business model depends upon trust. We cannot build and maintain our business unless we create a safe global environment for the people, families, and businesses who use our services. To that end, Western Union has increased its overall compliance funding by more than 200 percent over the last 5 years and now spends more than $200 million annually on compliance. Approximately 2,400—two thousand, four hundred—full-time employees, over 20 percent of our workforce, are exclusively dedicated to compliance functions.

We have added more employees with banking and legal and law enforcement and regulatory expertise. Our chief compliance officer, Jacqueline Molnar, who is here today, and I are proud to be some of the hundreds of compliance professionals recruited by Western Union in the last few years.

Our compliance program is comprehensive and has 12 components. Today, I will just discuss briefly two of those components, two that are especially relevant to this committee's work: agent oversight; and our financial intelligence unit (FIU.)

Agent oversight is a key component of an MSB's compliance program. In designing our program, we have been cognizant that Western Union's retail money services business operates through company partnerships with our network of agent locations around the world. In addition to regional store chains, convenience stores, small businesses, and other retailers, in most other countries, banks and post offices act as Western Union agents. But for those small businesses, revenue generated through offering Western Union products is very significant, and we are proud to help spur job growth and contribute to the larger economy.

We have established a dedicated compliance team specifically to conduct due diligence on our agents prior to entering the relationship with them, upon renewal of contracts and at other triggering events such as a change of ownership. We also provide training and we do field visits.

We monitor all transactions that flow through agents. In addition to the back-end traditional automated transaction monitoring—which I know other witnesses have spoken to you about—which looks for patterns post-transaction on a weekly or monthly basis, Western Union has something unique. We do upfront monitoring. We call it real-time risk assessments. And these are rules and algorithms that are designed to stop transactions before they go through. This is just one example. We hold 26 patents related to categorizing and identifying data patterns.

The other component of our compliance program I will briefly describe to you is our FIU. Modeled after intelligence programs in the government and law enforcement communities, our FIU, in addition to doing in-depth financial analysis and investigations, develops and maintains collaborative relationships with key law enforcement and other government partners.

For example, within hours of recent European terrorist attacks, our FIU's rapid response team provided actionable intelligence to law enforcement via confidential reports, suspicious activity reports (SARs), and suspicious transaction reports (STRs). Providing this

type of immediate insight into active investigations has in at least one case—and law enforcement told us this—helped identify additional terrorists before they carried out more attacks.

In conclusion, on behalf of Western Union, I thank the members of the subcommittee for having me here today and for your critical work in this area. I will be happy to answer any questions you may have.

[The prepared statement of Mr. DeVille can be found on page 51 of the appendix.]

Chairman PEARCE. Thank you, Mr. DeVille. I now recognize Mr. Oppenheimer for 5 minutes.

STATEMENT OF MATTHEW OPPENHEIMER, CO–FOUNDER AND CHIEF EXECUTIVE OFFICER, REMITLY, INC.

Mr. OPPENHEIMER. Good afternoon. My name is Matt Oppenheimer, and I am the co-founder and CEO of Remitly, an online remittance provider based in Seattle, Washington. I thank the subcommittee for the opportunity to explain why our country has an interest in ensuring that legitimate remittance services are accessible, affordable, and safe.

Remittances matter for the millions who rely on these services, but equally matter as a matter of national security. I founded Remitly in 2011 after living in Kenya and seeing firsthand how difficult it was to send money across borders. Not only that, but it was expensive, costing 8 percent to 10 percent of the total transfer just to send the money.

Looking at the technology available to solve this problem, I knew there had to be a better way. When I moved back, I started Remitly to make remittances easier, faster, and more transparent. By replacing the cash-based brick-and-mortar model with a purely digital one, we sought to build a better, more affordable service for customers.

By focusing on that vision, we have cut the cost of service from 8 percent to under 2 percent, putting hard-earned money back into consumers' pockets, while delivering a better user experience. I am humbled to say that our team of over 400 employees now helps customers send $3 billion a year to recipients in India, Mexico, Latin America, and the Philippines.

While our technology has improved remittances, the basic reasons for sending money have not changed. Our customers send money to pay for basic needs of their family members—housing, food, water, power, medical care, and education—things we take for granted here, but which can be unattainable for millions abroad.

Our customers are heroes. They sacrifice to provide a better life for their families. When they send, it is more than money. It is a lifeline. Paying their family's rent or their child's tuition, if you add up all these transfers, you will find that remittances contribute nearly 4 times the funds provided by all foreign aid.

Beyond the human impact, when remittances are sent through modern, legitimate channels, they strengthen our national security. As a regulated provider, we invest heavily to comply with AML laws and other requirements using the latest technology to detect and report suspicious activity.

Digital providers like Remitly provide an additional security by serving only customers with U.S. bank accounts and by embedding KYC, OFAC screens, and risk features directly into our product. This creates a more secure, lower-risk service compared to the traditional model.

This approach is also a powerful weapon against illegal activity. When our machine-learning systems or our trained staff spot something suspicious, we report it. This provides law enforcement with a high-resolution view into global money flows, an invaluable tool in fighting against illegal activity, money laundering, and terrorism.

Licensed remittance companies keep money in the light by processing legitimate transactions while detecting and reporting those that are not. By contrast, there is an underground market of unlicensed remittance providers that don't comply with these obligations. These informal networks operate without oversight and can be associated with black market activity.

If policies are enacted that raise the cost of legitimate services, money will flow into these shadowy alternatives. That is why I am troubled by recent proposals to tax remittances to fund a border wall. A 2 percent tax would radically increase the cost of sending money, far more than you might expect. Remitly charges less than 2 percent for our service, so this tax would more than double prices.

Do that and money will flow to underground channels, funding the very activities we want to stop. The worst thing Congress could do to our customers and to border security would be to tax remittances to build a wall. It is just bad policy.

Congress should focus on low-risk means to reduce regulatory burdens and enhance competition. While there is no silver bullet to AML reform, a few lead bullets include revisiting SAR reporting thresholds, aligning KYC requirements with international trends and improving OFAC sanctions list to reduce the operational burden posed by false positives.

These improvements would focus private sector and law enforcement resources on higher-risk activities. It makes sense to reality-check our risk-based approach from time to time, so I applaud the subcommittee's focus on these issues.

Making legitimate remittance services more accessible, affordable, and secure benefits consumers and strengthens national security. Smart policies and continued innovation put this goal within reach.

I thank you again for the opportunity to be here. I welcome any questions the Members may have.

[The prepared statement of Mr. Oppenheimer can be found on page 58 of the appendix.]

Chairman PEARCE. Thank you, Mr. Oppenheimer.

I now recognize Mr. Cassara for 5 minutes.

STATEMENT OF JOHN CASSARA, MEMBER, BOARD OF ADVISORS, CENTER ON SANCTIONS AND ILLICIT FINANCE, FOUNDATION FOR DEFENSE OF DEMOCRACIES

Mr. CASSARA. Chairman Pearce, Ranking Member Perlmutter, and members of the subcommittee, thank you for the opportunity to testify today. It is an honor for me to be here.

I am joined by experts from the formal remittance industry, so I will limit my remarks to the informal, underground remittances sometimes known as informal value transfer systems, parallel banking, underground banking, or sometimes just hawala.

There are an estimated 244 million migrant workers around the world. Globalization, demographic shifts, regional conflicts, income disparities, and the instinctive search for a better life continues to encourage more and more workers to cross borders in search of jobs and security. Many countries are dependent on remittances as an economic lifeline.

Although estimates vary, according to the World Bank, global remittances may have reached approximately $575 billion in 2016. That is an estimate of what is officially remitted. Unofficially, nobody knows.

However, using IMF and World Bank assessments, unofficial remittances may be greater than $850 billion per year, with a substantial portion of that originating from the United States. Although diverse alternative remittance systems are found around the world, most share a few common characteristics.

The first is that they all transfer money without physically moving it. Another is that they all offer the three "Cs": they are certain, convenient, and cheap. They are all ethnic-based. They are sophisticated and efficient and, finally, historically and culturally, most alternative remittance systems use trade as a primary mechanism to settle accounts or balance the books between brokers.

In my written testimony, I go into some detail about how they operate. Informal remittance networks are found throughout our country. The overwhelming percentage of money transfers generated by the use of these informal systems is benign. We, of course, do not wish to interfere with migrants sending money back home to support their loved ones.

However, these informal systems are also abused by criminal and terrorist organizations. They avoid our primary anti-money-laundering counterterrorism finance countermeasures. As Osama bin Laden once said, jihadists are aware of the "cracks" in the Western financial system. Informal remittances are not just a crack. They are a Grand Canyon.

There have been many incidents relating to terror finance, both in the United States and overseas. Some examples include the use of hawala in areas our adversaries operate, such as Afghanistan, the Horn of Africa, and ISIS-controlled Syria and Iraq. Hawala was used to help fund the 2010 Times Square bombing in New York City. In 2013, a Federal judge in San Diego sentenced three Somali immigrants for providing support via hawala to Al-Shabaab, a designated terrorist organization.

Hawala is legal in the United States, as long as a service is registered with Treasury's FinCEN and adheres to State licensing

guidelines. Yet our government's own statistics suggest our money services business registration is not successful.

And from an investigative standpoint, it is very hard to penetrate these networks. To use just a few examples, law enforcement does not have many Gujarati, Farsi, Pashtu, or Urdu speakers, and even if we recruited some sources to walk into some of these networks, the question may well be, well, who is your uncle in the village back in the old country? And if you can't answer that question, they are probably not going to have much to do with you.

Because these systems are closed and opaque and based on trust, there are no easy countermeasures. But I do include a number of recommendations in my written statement. These include steps to improve our registration of underground money services businesses using trade transparency as the backdoor into these networks, better exploiting data and advanced analytics, improving financial inclusion by lowering the cost of formal remittances, and improving training and analytics so that compliance and law enforcement officers and analysts can better detect the systems.

I also urge that we begin to pay attention to the worldwide Chinese underground financial systems, sometimes known as Fei-chien or "flying money."

Once again, it is an honor to be here and I am happy to answer any questions you may have.

[The prepared statement of Mr. Cassara can be found on page 34 of the appendix.]

Chairman PEARCE. Thank you, Mr. Cassara. And I now recognize Mr. Paul for 5 minutes.

STATEMENT OF SCOTT T. PAUL, CHIEF HUMANITARIAN POLICY ADVISOR, OXFAM AMERICA

Mr. PAUL. Chairman Pearce, Ranking Member Perlmutter, and members of the subcommittee, on behalf of Oxfam America, I thank you for the opportunity to testify here today.

Oxfam envisions a world without poverty, where all people are able to enjoy the full range of their human rights. Both financial exclusion and terrorism stand in the way of achieving that vision. Therefore, we need to make remittance services accessible, affordable, and accountable, both to law enforcement authorities and to the families sending and receiving money.

As you know, remittances help fight poverty and aid humanitarian response worldwide. But they are particularly crucial in the world's poorest countries and during humanitarian emergencies. Oxfam works in many countries where state institutions and the private sector are very weak or have collapsed. In these countries especially, remittances are a powerful stabilizing force. They help communities build resilience to crises, weather the storm, and then build back better.

Unfortunately, we are witnessing a market failure in the financial sector today that is threatening to reduce and obscure remittance flows. Money transfer operators like Western Union or Remitly, also called MTOs, are the primary providers of remittance services to many migrants, and they typically rely on banks to perform financial services for them, including wiring money. But

banks are closing the accounts of legitimate MTOs at an alarming rate.

Oxfam has commissioned research and conducted extensive outreach to banks, MTOs, community groups, and government agencies to gain a greater understanding of the problem and its possible consequences and solutions. The 9/11 terrorist attacks and 2008 financial crisis created pressure to crack down hard on abuse in the financial sector. In this environment, many banks view MTOs as high risk and are deciding that the benefits of maintaining their accounts just don't justify the costs and consequences that come with it. So rather than manage the AML/CFT risk of their MTO customers, many banks are instead terminating MTO accounts.

It is important to bear in mind that high-risk businesses like some MTOs are not bad actors. They are just viewed as vulnerable to abuse, which means they require more resources and expertise to oversee. Closing MTO accounts may, in fact, be a rational decision for banks, but it likely means a decline in remittances and an increase in the share of remittances transmitted through informal networks, which makes money more difficult for law enforcement officials, regulators, and money senders to trace.

Somalia presents a unique and illustrative case. Remittances make up roughly a third of Somalia's entire economy and are generally spent on basic survival needs. One Somali-American I interviewed told me that without the money we are sending them, he didn't think the entire Somali nation would exist.

Another confessed to me tearfully that the thought of not being able to send money to his sick mother for food and medicine made him consider going back to face drought and conflict. "I can't even eat thinking about it," he told me.

Because of the security situation, most international banks and well-known MTOs are no longer present in Somalia, leaving only lesser-known Somali MTOs operating in the U.S. as a viable option. These MTOs are registered, examined, and regulated. They have collaborated with law enforcement during prosecutions of Al-Shabaab supporters. Nonetheless, banks have closed nearly all of their accounts, forcing them to find alternatives that make remittances more costly and much less secure.

Let's remember, banks will manage risk in the right circumstances. In today's business environment, banks have thought it prudent to participate in multi-billion-dollar money laundering schemes, yet barely offer any service to MTOs whose core business is the transmission of $50 or $100 each month to a migrant who wants to build a better life for her family. It is obvious that the size and profitability of a customer matters a great deal to its bank.

U.S. law and regulation have made the costs and consequences of managing money laundering and terrorist financing a lot steeper, but the revenue potential of MTOs for banks, particularly small MTOs, remains very low. I would urge this subcommittee to work with the Treasury Department, the State Department, USAID, and the Federal banking agencies to refine the risk-based approach in order to encourage more investment in risk management and less risk avoidance, including of MTOs operating in high-risk jurisdictions. That will mean more money in the hands of people looking

to escape poverty and less opportunity for terrorists and other financial criminals to transact business.

I look forward to your questions. Thank you.

[The prepared statement of Mr. Paul can be found on page 62 of the appendix.]

Chairman PEARCE. Thank you, Mr. Paul.

The Chair now recognizes himself for 5 minutes for questions. So without getting too deep into it, last year, about a year ago, I found myself in the middle of Bangladesh, in the middle of the night, needing cash to fill up a small airplane that needed to fly to Muscat, Oman, where I needed cash again. So finding that black and gold logo was somewhat reassuring. I didn't actually use it, but something about hitting the ATM machine in the middle of the night from Bangladesh, then Muscat, Oman, caused some alarm back in the U.S. and caused those cards to be summarily dismissed and turned off.

Again, thanks for what each of you do, because you serve a very real purpose for real people trying to just do things and live lives. So I appreciate that.

So Mr. Oppenheimer mentions three suggestions in his testimony. Mr. Cassara, have you had a chance to—did you pick up those basically, saying that the reporting thresholds for suspicious activity across banks, non-banks should be consistent? And then the travel rule update, and then finally OFAC to build a more complete, updated sanctions list, that sort of—do you have an opinion on those recommendations, something that you would see to be productive? If you don't, it is fine.

Mr. CASSARA. At first hearing, they seem very reasonable to me, but I have not studied them.

Chairman PEARCE. You would like more time to look, but there wasn't anything that said, hey, this is not—it is a track we ought to consider, is what I hear.

Mr. CASSARA. Yes. Nothing there is just outside the pale.

Chairman PEARCE. Okay, fine. Mr. Oppenheimer, you heard Mr. DeVille say that 20 percent of their time is spent on regulations. Do you find that much of your time going into regulations?

Mr. OPPENHEIMER. I certainly spend a lot of my time on regulatory matters, and we have a compliance team that we hired very early. Our second hire was our compliance officer. I think that one advantage of digital channels is because it is centralized, our regulators appreciate everything that a customer enters in. There is no human intervention. We don't have a lot of cash agents.

Chairman PEARCE. Okay, so—

Mr. OPPENHEIMER. So the number of people is less.

Chairman PEARCE. Yes, if I can interrupt here for a second, of that 20 percent, do you find all of it to be very productive, or half of it, or you don't want to say with the IRS watching? I don't know.

Mr. OPPENHEIMER. It is a great question, Congressman. And I think that some of the recommendations that you just mentioned in terms of reducing the number of false positives from OFAC screening, some of that work I think is less productive. And if we expand the number of criteria right now for OFAC matches, for instance, it is name, location, and date of birth. And building the company from day one, those false positives, once they got through

our systems, and then it went through a manual review, I was doing personally, and we basically collect additional information from the customer to make sure that it is not on a terrorist watch list. That is not the individual.

And so I think that some of the recommendations about expanding that criteria, so that can be automated and collected and screened in an automated fashion, so good customers don't go through that false positive experience and we still catch nefarious activity, that is important.

Chairman PEARCE. I appreciate it. I just need to keep moving here. Mr. DeVille, if you want to answer the same question, what percent of your 20 percent do you think is really productive in improving the security of the transfer of money, improving your operations, and improving the security of your customers?

Mr. DEVILLE. In the current regulatory environment, of course, it is a requirement. But your question is somewhat different. There is no doubt that there is a tick-the-box regime on the part of regulators, rather than the things in which I would like to focus, which is like our financial intelligence unit, which as I said provides actionable information to law enforcement.

In fairness to the regulators, however, they are excluded from the law enforcement investigations by definition. So they don't have insight into what is really important to law enforcement.

Chairman PEARCE. Okay, I am just trying to get the big picture. Are the regulations well-directed or are they not well-directed? And we will keep working on that. How many SARs do you file each year?

Mr. DEVILLE. We are actually the largest SAR filer in the country, nearly 200,000 SARs last year and an equivalent number overseas, STRs, we call them generally.

Chairman PEARCE. What is the turnaround time that you get?

Mr. DEVILLE. The turnaround time? We have—it is a complicated regulation, but in simple form, 30 days from the alert to file a SAR. Certainly if it is a terrorist finance SAR, we file it quicker and we pick up the phone to call.

Chairman PEARCE. Do you ever get any responses from FinCEN?

Mr. DEVILLE. We do get occasional responses from FinCEN, I think in large part because I used to work there.

Chairman PEARCE. Would it be more productive if you had a little bit more feedback? Or would that—

Mr. DEVILLE. The feedback has improved. It is easier for me because I used to work there. But I do hear from my counterparts that they wish they had more feedback, but I have been pleased with it. And they have improved it over the last few years.

Chairman PEARCE. My time has expired. I now recognize the gentleman from Colorado, Mr. Perlmutter, for 5 minutes.

Mr. PERLMUTTER. Thanks, Mr. Chairman, and thank you to the panel for your testimony today. Let's get this out of the way. The first questions I have are on H.R. 1834, the border tax, or the remittance tax. So I would like to direct these to you, Mr. DeVille, and to you, Mr. Oppenheimer. And I also want to introduce into the record a letter dated February 3, 2017, from Western Union, and a letter from the Electronic Transactions Association, objecting to the bill dated May 1, 2017, and finally a letter from Morrison

and Foerster on behalf of the Money Services Roundtable, all in objection to the remittance tax.

Chairman PEARCE. Without objection, it is so ordered.

Mr. PERLMUTTER. Mr. DeVille, why don't you go first? Talk to us a little bit. Mr. Oppenheimer gave us a little opening about it. What effect would this tax have in connection with your operations?

Mr. DEVILLE. Thank you, Representative Perlmutter. It is a very good question and timely.

It is especially important to understand how price-sensitive the money transmitter business is. Mr. Oppenheimer and I did not talk beforehand, but my statistic is the same as his, that a 2 percent tax would nearly double in our case the cost of the average transmittal of funds between Western Union clients.

Mr. PERLMUTTER. Do you agree with him that this could drive these transactions underground, which would then make them less transparent to law enforcement—

Mr. DEVILLE. Yes, it almost certainly would drive them underground. There are so many opportunities underground as it is, even without the tax. And the relationship part we have with law enforcement, the SARs I discussed with the chairman, those would not be as readily available, if at all, from an underground money transmitter.

Mr. PERLMUTTER. Thank you. Mr. Oppenheimer?

Mr. OPPENHEIMER. Yes, thank you for the question, Congressman. As I mentioned in my oral testimony, I think that for the reasons that Mr. DeVille mentioned and that we have talked about, funding a border wall with remittance tax would be both bad for our national security and would be harmful for consumers trying to get money back home. So I think regardless of one's views on a border wall, taxing remittances to fund it is just not good policy.

Mr. PERLMUTTER. Okay, thank you. Mr. Cassara, Mr. Paul, I really do want to understand. You gave us an overview, Mr. Cassara, of hawala. And I would like a couple of examples. I know you give them in your written testimony. But for oral testimony today, give me an example of how the money goes underground and how it could get to a terrorist organization. Mr. Pearce said that you had been a gun dealer or an arms dealer at some point in your past—

Chairman PEARCE. That was an underground, legitimate—

Mr. PERLMUTTER. An underground—

Chairman PEARCE. Undercover, excuse me.

Mr. PERLMUTTER. Undercover, pardon me. So explain to me—I understood you were doing it on behalf of all of us, and I appreciate that, all right, thank you—so give us some examples of how this goes underground. And then, Mr. Paul, what I would like you to talk about is, what is the effect to just law-abiding people in Minneapolis or Denver or wherever it may be, if we really tighten down on this stuff?

Mr. CASSARA. Congressman, here in the United States, I believe that underground financial networks, such as hawala, are found throughout the country. So, for example, there could be a Somali—and I am not picking on Somalis; it could just as easily be an Afghan or a Bangladeshi or whomever, it doesn't make any dif-

ference—individual who wants to remit money back to his home country, for example, Somalia. Maybe he wants to help support Al-Shabaab.

There are limitations and real concerns why he would not want to go into a formal financial institution, which I outline in my paper, as well as, for example, a money services business. So he feels comfortable in talking to somebody from his extended family, clan or tribe, somebody that may be called a hawaladar. He gives them some money that he wants transmitted back to Somalia, back to the old country. The money does not physically leave the United States. It stays here in the United States.

The hawaladar here in the United States contacts his counterpart in Somalia. The equivalent of money, less small fees at both ends, is then delivered to the destination that he designates. That destination could be affiliated with, for example, an Al-Shabaab. That money could go for nefarious purposes.

Mr. PERLMUTTER. Okay, so the money is here, but it is like security for the money over there? Like having a certificate of deposit that is on loan to somebody who puts up the money in the old country?

Mr. CASSARA. Correct. It is money transfer without money movement. In a sense, it is what Western Union does.

Mr. PERLMUTTER. Mr. Paul—and I know my time is up—

Mr. PAUL. Yes, I will just quickly agree with Mr. Cassara and just say, on top of the consequences for our national security, consider also the perspective of the individual money sender. Once that money gets out of his pocket and into the hawaladar's pocket, there is no recourse. You can't sue. You can't call someone who has any authority over the person who has just taken your money. That money, for all intents and purposes, is out of his or her hands.

Mr. PERLMUTTER. Thank you. And I yield back.

Chairman PEARCE. The gentleman's time has expired. The Chair now recognizes the gentleman from North Carolina, Mr. Pittenger, for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman.

Mr. DeVille and Mr. Oppenheimer, do your companies share information on terror financing and other illicit financial threats with each other and with other financial institutions?

Mr. DEVILLE. Yes, we participate in 314(b), Congressman.

Mr. PITTENGER. Yes, sir. Is that the same as you, Mr. Oppenheimer?

Mr. OPPENHEIMER. That is correct, yes.

Mr. PITTENGER. Do you have any impediments or challenges there in the respect of that exchange of information?

Mr. DEVILLE. I know my counterparts at other financial institutions have had impediments. We actually have not. It has worked well for us.

Mr. PITTENGER. Okay.

Mr. DEVILLE. Perhaps because we are a bigger player, it could be.

Mr. PITTENGER. Sure. Mr. Cassara, you have testified previously and also written regarding the trade transparency units. And give us some detail, if you would, on how these trade transparency units

can be helpful in identifying illicit financing in remittances, wire transfers, hawalas, and other regard.

Mr. CASSARA. It depends on the geographic location in the world, but historically and culturally, most underground financial systems, particularly hawala and Fei-chien, they settle accounts or balance the books through trade, value transfer, over- and under-invoicing, for example, sometimes called "countervaluation."

I have testified here before on the idea of establishing trade transparency units around the world. There are approximately 16 today. We have one here in the United States in homeland security investigations. The idea is very simple. Looking at one country's targeted imports comparing those with a corresponding country's exports, you can spot anomalies. Those anomalies could be an indication of simple customs fraud. It could also be an indication of some form of underground financial system, like hawala or a black market peso exchange.

Some people have called this a possible backdoor into these networks. I think the trade transparency unit initiative deserves some funding and some more manpower to see if this network could be expanded as a real countermeasure to underground financial systems.

Mr. PITTENGER. Very good. How then, Mr. Cassara, does trade-based money laundering itself—how is it tied into illicit remittance payments or other non-bank means of financing?

Mr. CASSARA. I'm sorry. I did not get that question.

Mr. PITTENGER. The trade-based money laundering, how is it tied into illicit remittance payments or other non-bank?

Mr. CASSARA. Underground banking is tied into trade-based money laundering simply because it is part of the countervaluation process. And if you include things like hawala, like Fei-chien, like the black market peso exchange, like padala in the Philippines, like all these others, as I said, historically and culturally, they all use trade-based value transfer.

So you can't separate them out. All these—

Mr. PITTENGER. Mr. DeVille, would you like to comment? We are looking to try to streamline and try to clarify 314(a) and (b) so as to provide sharing and provide a capacity for financial institutions to be protected, to have a safe harbor in those transfers with each other and with the government. And would you find this helpful, not just in sharing information, but do you believe it would reduce the amount of oversight and engagement that you have to have with multiple SARs, accounts? You could be identifying those individuals so that data that is really relayed to you by the Federal Government or by each other. Would that be a supportive effort for you?

Mr. DEVILLE. Yes, if I may, Congressman, it would be. We certainly, like all financial institutions, receive 314(a) requests. I think the biggest help to us would be is if we could share SARs with our foreign subsidiaries. You have a Western Union license in the U.S., you have a Western Union license in Europe. We cannot share SARs even though they are all Western Union. Now, whether a Congress would put that under 314(a) or something else is another question. But that inhibits our information-sharing.

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

Chairman PEARCE. The gentleman's time has expired. The Chair now recognizes the ranking member of the full Financial Services Committee, the gentlelady from California, Ms. Waters.

Ms. WATERS. Thank you very much, Mr. Chairman. It is very important for all of us that you are holding this hearing today. As a matter of fact, this past weekend, I was in Jamaica and had an opportunity to talk with a number of the parliamentarians and the former prime minister. And they talked about correspondent banking relationships that were not available to them anymore from major banks.

And I had representatives from Saint Vincent's and the Grenadines in my office last week, where they came to tell us they have no bank that will do business with them, and that they can't pay the salaries of the people working in the embassies and pay their bills, and they want us to help them in some way.

And then, of course, they talked about remittances and the important role that it plays in all of these Caribbean countries. And so I want to know, why is the Caribbean being hit so hard? And what suggestions do you have? I certainly don't think that taxing remittances would be a good thing to do. It would be a terrible thing to do. Even for those banks that were—those countries that were able to hold onto some banking relationships, they have increased the charges for providing the services and so, I think taxing would be terrible.

And we should all be appreciative of these remittances and the role that it is playing in these countries to help with poverty problems and education and health and all of that. And so I guess my big question is, can you comment, Mr. Paul, on the effect that this trend is having in terms of the transparency of overall remittance flows? And can you elaborate on the regions where the adverse effects of this trend are more pronounced? For example, you wrote in your testimony that Caribbean governments at the highest levels have raised concerns about the impact of bank closures on remittances flows. What have these adverse effects entailed?

Mr. PAUL. Thank you, Representative Waters. It is an incredibly critical issue, correspondent banking. And the issue of correspondent banking and banks—foreign banks' access to the U.S. financial system is very closely related and in a lot of ways parallel to the issues that MTOs have had accessing the U.S. financial system.

Essentially, the costs and consequences of maintaining correspondent banking relationships are outweighing the profitability of maintaining those relationships. And the cascading effects of the breakdown in correspondent banking is having horrific effects on remittance flows, on the ability of organizations like Oxfam and other nonprofit organizations to move money around the world, also for trade finance. So this is an issue that absolutely demands the subcommittee's attention.

I would say the region that has been hit hardest would be the Caribbean. Belize has come forward to say they may not have any correspondent relationships with the U.S. at all at the moment. Jamaica, you mentioned. The other one that has come out very

strongly is the Pacific. A lot of small island states in the Pacific are finding it more and more difficult to connect to the global financial system. And I would say that is a systemic risk.

Ms. WATERS. Do you have any ideas about what we can do to deal with this? We can't make the banks do what they don't want to do, but they can't say that it is not at all profitable, because actually they can charge and they have been increasing the charges for quite some time. We don't want them to continue to do this, but what I recognize, talking with those in the Caribbean, is that many of these small countries spend a lot of money in the United States. For example, in Florida, whether you are talking about the Bahamas or any of these countries, they come and they do business, they shop, what have you. We should have a good relationship with them.

And we should respect the fact that they have to maintain these embassies, and we want them to do that. Do you have any ideas about what we can do?

Mr. PAUL. Absolutely. Thank you, Representative Waters. There are a few different ways to deal with this—so we have costs and consequences on the one hand, and we have profitability on the other. So one way to do it is to find a way to minimize the cost and consequences.

There are a number of ways to do that. The most simple way is probably just to clarify exactly what banks' responsibilities are when managing risks of correspondent relationships. A second way is to be creative and think about how to create more incentives to bank otherwise unprofitable correspondent banks.

But lastly, and I think maybe the most practical, immediate step that the subcommittee could take is to bring all the stakeholders together to make sure that the right people are in the room, and as concerns the U.S. Government, to bring in some of the voices that are more inclusion-minded. So the International Affairs Directorate at Treasury, parts of the State Department, parts of USAID that have a lot of equities in this issue, but aren't always writing policy.

Ms. WATERS. Thank you very much. I yield back.

Mr. EMMER [presiding]. The gentlewoman's time has expired. The Chair now recognizes the gentleman from Pennsylvania, Mr. Rothfus.

Mr. ROTHFUS. Thank you, Mr. Chairman. Mr. Cassara, can you please explain how charitable organizations fund hawalas? And have you seen U.S.-based charities involved with funding hawalas?

Mr. CASSARA. I personally have not seen U.S. charities use hawala, although there were cases immediately after 9/11 where those charities were alleged to have been involved. Again, it depends on the area of the world that we are talking about. In certain areas in Afghanistan, or Somalia, there are not that many alternatives for regular businesses, for nonprofits. They are almost forced to use these underground systems to transmit funds. So, yes, it is conceivable that this is happening.

Mr. ROTHFUS. On page nine of your testimony, you mentioned Iran's form of hawala is havaleh. On that same page, you mentioned 300,000 Iranians are in Dubai, with reports that billions in capital is invested in Dubai real estate to launder Iranian money.

Are Iranian actors using hawala to launder and integrate this money? Or do they use the Western banking system?

Mr. CASSARA. I believe they are using hawala, havaleh, to transfer funds from Iran into Dubai to purchase properties, et cetera, yes.

Mr. ROTHFUS. How would they use havaleh to launder large sums? How does that work? How much are we talking here?

Mr. CASSARA. I can't give you an estimate. I don't know whether our government, whether the intelligence community and others have studied that issue. I don't know whether those numbers are available.

Mr. ROTHFUS. You also mentioned that the hawala system is based on trust, but that terrorists also use the hawala networks, as ISIS does in Iraq and Syria. The Treasury Department designated the Al-Kauthar money exchange in December 2016 as an ISIS-linked MSB. Is there a network of ISIS-controlled hawalas? Or was this a unique situation where ISIS managed to gain the trust of non-ISIS controlled hawalas?

Mr. CASSARA. I don't have specific intelligence on this one instance. I don't believe there is an ISIS-controlled network. This is my own impression. I think there are hawaladars of opportunity out there that cooperate with ISIS. I also think you have to look at the whole issue of trade-based value transfer in the region. But most definitely, hawala is present in ISIS-controlled territories in Iraq and Syria.

Mr. ROTHFUS. With respect to the unregistered MSBs and hawala brokers here in the United States, is the fact that they are unregistered a function of a lack of Federal agents and resources to enforce compliance? Or are there other factors at play here?

Mr. CASSARA. I was at FinCEN in the late 1990s. At that time, the Director of FinCEN commissioned a study—how many MSBs are there in the United States? This happened right before 9/11. The answer came back approximately 240,000 in the United States. I am sure that number has increased.

I believe that the number of registered MSBs here in this country today is probably in the area of 30,000. So if that original study was correct, there was a missing two-hundred-some-odd thousand. Why aren't more registering? There are a number of reasons. Number one, lack of outreach. There are a lot of communities here that aren't aware of the requirements to register. FinCEN, the IRS is supposed to do much more in that regard.

Second of all, it comes down to enforcement. There should be agents knocking on the doors. Why aren't you registered? Why aren't you licensed? And that is not happening.

Mr. ROTHFUS. Is it a function of insufficient resources? Do we need more agents working on this?

Mr. CASSARA. I think part of it is resources and part of it is priorities.

Mr. ROTHFUS. Can you explain the mechanism of how wealthy Chinese individuals purchase high-end real estate in the United States through their flying money system?

Mr. CASSARA. Thank you for that question. I am very concerned about Fei-chien, flying money, and its use here in the United States. There is a lack of reporting on this issue in our government

and in open source information. But as you well know, in China itself, Chinese citizens are limited to about $50,000 a year they can take out of the country. And even if they use smurfing networks, family members, et cetera, et cetera, there is a massive amount of capital flight leaving China going into the United States, purchasing high-end properties, and I feel that Fei-chien plays a part in this.

The same thing is also happening in places like Canada, in London, in Australia, and elsewhere. And we are not paying any attention to it.

Mr. ROTHFUS. I yield back.

Mr. EMMER. The gentleman's time has expired. The Chair now recognizes the gentlewoman from New York, Mrs. Maloney.

Mrs. MALONEY. Thank you. And I thank so much the Chair and the ranking member for calling this hearing and all of your testimony. Mr. DeVille, your testimony notes that a current area of focus for Western Union's financial intelligence unit is the continued analysis of transaction controls and other risk measures in Iraq, Syria, Turkey, and Libya, to ensure that you appropriately manage risk while at the same time serving the very real humanitarian needs.

But as you know, most other American financial institutions are not operating in these countries. They have pulled out. So why do you think Western Union has been able to continue to serve higher-risk countries such as Syria when so many firms have not continued, have pulled out? You are alone in so many countries. What is the difference? And why are you able to succeed where others are not able to stay and serve? And thank you for doing that, too.

Mr. DEVILLE. Thank you, Congresswoman Maloney. I appreciate that. And you are correct. In many instances, we are the only Western institution in these countries. Take the example of Syria, for instance. We have zoned the country off into zone one and zone two. We shut down the agents in zone one. We apply a lot of due diligence controls in zone two. We don't talk about our specific controls publicly, but limiting thresholds, limiting the velocity.

We also look for individuals who will transmit—do a Western Union transfer on the Turkish side and then go into Syria and vice versa, or go from a western European country. The bottom line is, it takes a lot of resources and a lot of data analysis to allow us to be there.

I will say, in all my conversations with the State Department and the Treasury Department, they are glad we are there, because we are, within the constraints of privacy laws, a source of financial information for them.

Mrs. MALONEY. Well, congratulations, and thank you for your service.

Mr. Paul, as you know, one of the reasons that financial institutions have been de-risking entirely from certain countries rather than trying to manage the risk of doing business in that country is the lack of clarity from the banking regulators about what they need to do to comply with their anti-money-laundering obligations.

And what kind of regulatory action do you think would give financial institutions sufficient clarity on their anti-money-laundering obligations so they can continue to provide essential finan-

cial services and humanitarian support? And could you really—and anybody—talk about this, because this is a problem. How could we clarify it so that they would feel comfortable? Can you expand on it?

Mr. PAUL. Thank you, Congresswoman. As you know, in recent years, the Treasury Department has tried to issue guidance statements, either policy guidance, in some cases blog posts, with the expectation that financial institutions would hear that message and be heartened that they don't have to be infallible, they don't need to know their customer's customer, and that the risk-based approach means taking a proportionate approach in all of these different places, and they should take heart and do business in some of these high-risk jurisdictions.

Unfortunately, I think it is fair to say that for the most part, that hasn't worked. I would encourage regulators to continue the program of outreach that they have begun in general. But specifically, in jurisdictions that are extremely high-risk and at the margins of the formal financial sector, where people are getting pushed out, people might have nonprofit organizations or correspondent banks or remittance services may only have a single bank account and maybe under threat of losing that account, that is where some sort of hybrid risk-sharing approach might be more useful, where you have regulators being willing to promulgate more concrete rules as opposed to a more amorphous risk-based approach and actually take on and share some of that risk by being specific about what is expected.

Mrs. MALONEY. And would anyone else like to clarify in this area, which is a reason why many people are not continuing to serve? Yes?

Mr. DEVILLE. Yes, if I may, thank you. I think we are on the same page. More specifically, if we could have joint guidance from all the regulators on the requirements for banking and MSB, I think that would be helpful. The last time there has been joint guidance was in 2005 on MSBs. That would certainly help.

Mrs. MALONEY. And when you say joint guidance, who all would be part of this joint guidance?

Mr. DEVILLE. It would be—FinCEN did in 2014 guidance on banking MSBs. Maybe that could be a starting point. But you would have to have the OCC, the Fed, the banking regulators involved, as well, for it to carry weight.

Mrs. MALONEY. Maybe that is something we can work on together in a bipartisan way to accomplish. It is a tremendous challenge for our country. And we have to be concerned about it, particularly in our own country, the money laundering taking place. My time has expired. Thank you. Thank you for having the hearing.

Mr. EMMER. The Chair now recognizes himself for 5 minutes.

Mr. Oppenheimer and Mr. DeVille, and I am going to put it in more simplistic terms and give you a little bit of room to run—and I don't care who starts—but can you give the committee a better understanding of the current regulatory environment for money transmitters from an industry perspective?

Mr. DEVILLE. I think it sort of segues from the last question. The current environment is, I think, difficult for the banks in many

ways because there is a lack in some ways of what is a clear guidance on the part of what MSBs have to comply with. So that is a problem from the banks.

Another issue is just divorcing the de-risking argument from this, which we have been talking about, is very often at an MSB we have to extrapolate from banking regulations, because oftentimes there are not specific regulations for MSBs. So more clarity there would certainly be helpful, as well.

I think probably the main point from my perspective at Western Union is the lack of a level playing field in the MSB industry. Mr. Cassara mentioned registered MSBs. As of yesterday, there were 25,939 registered MSBs, but as you said, there are countless unregistered MSBs.

And both the smaller registered MSBs and certainly the unregistered MSBs, frankly, do not get examined. And so there is not a level playing field. And let's forget about Western Union, because I am biased, but there is not a level playing field between them and the PayPal, Xoom, Moneygram, Remitly, those like us.

Mr. EMMER. Mr. Oppenheimer, do you have anything to add?

Mr. OPPENHEIMER. Thank you for the question, Congressman. I think that the environment for registered money services businesses is one that is robust. I think that there is a lot of work in the industry around streamlining the various regulators we have, and I think efforts to do that are welcome. And I think that we are regulated by both State agencies, and then we also, obviously, register with FinCEN. We are also under the purview of the CFPB. So the more streamlining that can happen, partnering between regulators, the States are doing a lot of streamlining between various State agencies I think is welcome.

And I think that the other thing is aligning bank and non-bank regulations. And I mentioned some of that in my written testimony.

Mr. EMMER. By the way, Mr. Oppenheimer, has your company ever had to deal with the issue of de-risking?

Mr. OPPENHEIMER. We have. When I started the company in Boise, Idaho, when I came back from Kenya—I am from Boise originally—I set up a bank account and filled out on the form that I was a money transmitter. It took the bank about 6 months to go through their internal process, but after that point, we had raised about $750,000 in capital to get the business off the ground. We had not processed a single transaction.

But they went through the process, saw we were an MSB, and I got a letter in the mail saying we saw that you are a money transmitter, we are going to be mailing the balance on your account to the registered address. Thanks for being a customer.

And those experiences, I think, happen to a lot of money services businesses. Thankfully, I knew about de-risking, and so I had been working to get a redundant bank account. We transferred it over. And now we have multiple bank accounts. But I think the story that we experienced—there are countless stories out there for MSBs that are not able to get bank accounts and, unfortunately, just have to shut down.

Mr. EMMER. Mr. DeVille, same question. Has Western Union dealt with de-risking?

Mr. DEVILLE. We have. As one of the bigger players, it doesn't perhaps affect us as much, but, Mr. Cassara said earlier that the way Western Union settles up is like a hawala. Well, aside from our—and I know you didn't mean that—huge compliance program, there is a difference.

We require a correspondent bank to settle between us in Denver and our agents overseas, so that is where our de-risking risk comes in. And then for our agents, who are not as big, of course, they certainly face a de-risking risk, as well, if you will.

Mr. EMMER. And I am sorry that I am picking on these two, but I am going to stick with it, because I am interested to know, I asked you about the regulatory environment to start with. So now with de-risking, how much does the regulatory environment actually impact de-risking? Mr. Oppenheimer or Mr. DeVille or the other two witnesses?

Mr. DEVILLE. I will give you an example. Mr. Paul's organization, Oxfam, is obviously a very reputable organization and it is a customer of ours. They have 11 accounts with us. I pulled the numbers, and we had to do 77 investigations on Oxfam last year because of alerts.

We knew Oxfam was good, but you can't just put it aside. A regulator is going to come and look and say, why did you not file a SAR? So that is a perspective from the other side, as opposed to us being de-risked, it is our view into perhaps de-risking a good customer like Oxfam. So it is quite expensive to have a high-risk customer, be it an MSB or a charity.

Mr. EMMER. I see my time has expired. At this point, the Chair will recognize the gentleman from Illinois, Mr. Foster, for 5 minutes.

Mr. FOSTER. Thank you, Mr. Chairman. And thank you to all our witnesses for your testimony today.

Mr. Paul, one thing that I sort of find missing in this discussion is the human element. As you mentioned in your testimony, remittances are particularly important to developing countries. For one thing, remittances have helped lift millions out of poverty, and thereby unquestionably saved hundreds of thousands of lives through access to medical care, et cetera, that would not otherwise be available.

A recent study conducted by the U.N. International Fund for Agricultural Development stated that approximately 200 million migrants globally send more than $445 billion in 2016 as remittances back to their families. And there is a lot of good that is done by that money when it arrives in poor countries.

And in many cases, the majority of this money just helps people meet their most basic needs—food, shelter, education, medical treatment. Remittances also play a crucial role during humanitarian emergencies, particularly in institutions where state institutions and the private sector have unfortunately failed.

However, despite being viewed as, by and large, law-abiding consumers, financial institutions have increasingly moved to de-risk the accounts perceived to be higher risk, often with a sort of broad-brush approach that restricts many consumers from any access to financial services.

And while effective BSA and AML compliance is important, the remittance services, as you stated in your testimony, must be accessible, affordable, and accountable. Can you just talk briefly about the human impact of such wholesale and broad-brush derisking?

Mr. PAUL. Thank you, Congressman Foster. I have had the privilege now in my 5½ years with Oxfam to travel to regions around the world where people have been able to benefit from different kinds of financial inflows, foreign direct investment, remittances, U.S. development and humanitarian assistance. Each has its comparative advantage, but one of the most interesting things about remittances is, it is entirely in the hands of the recipients. It gives people an incredible amount of agency over their lives. It is more insulated from global economic shocks and stresses, not completely insulated, but more insulated, and more insulated also from political shifts than, say, foreign assistance flows.

So really, it is the sort of financial inflow that allows people to identify their most immediate needs. And I have seen that recently in humanitarian emergencies in three countries facing famine—Nigeria, Somalia, and Yemen—where remittances are essentially the firewall from destitution and death. And also in places where remittances enable people to identify their most promising opportunities, be it a college education or a small business, or investment in a family member. So it has been really amazing to see that.

Mr. FOSTER. Well, thank you. Because we have to bear that in mind. My next question I guess is probably directed to Mr. DeVille and Mr. Oppenheimer. What fraction of all of the uncertainties and liabilities that you have to deal with have to do with identity fraud, either at the host country end or the home country end? And would some sort of approach where having a high-quality authenticated digital ID on both ends of the transaction, in exchange for some sort of legal safe harbor, is there a useful arrangement to be made along those lines?

Mr. DEVILLE. Yes, certainly. And I understand it is a controversial issue, a national ID, but we accept—we will view in some cases record an ID. And we do checks. Our templates are designed—if it is a California ID and there are the wrong number of digits, then the transaction will be rejected. But we don't have a means other than that to determine the validity of the ID, at least not in the U.S., so that would be enormously helpful.

Mr. FOSTER. And also, you are talking about how a lot of these are immigrants, immigrants or guest workers here, for which presumably the political resistance to having a very high-quality ID mandated might be a lot smaller. So this might not be a solution for everyone, but might be a significant factor. Especially, it must be more important online than for someone appearing in person.

Mr. OPPENHEIMER. Yes, and just to reiterate that point, I will just add on the systems we have, not only help from a compliance perspective, but we also have similar systems in place, machine learning, rules-based engines, that help us prevent any sort of fraudulent attempts to go through our platform.

Mr. FOSTER. But those have to do with big commercial databases that know everything about you, that are more difficult to use by the Federal Government.

Mr. DEVILLE. Ours is an IBM product, so, yes, similar.

Mr. FOSTER. But it is the big databases from these companies that analyze everything produced by your cellphone and everything else that are different.

Chairman PEARCE. The gentleman's time has expired. The Chair now recognizes the gentleman from North Carolina, Mr. Budd, for 5 minutes.

Mr. BUDD. Thank you, Mr. Chairman, and thank you to the panel.

Mr. Cassara, a question for you. Are these payments in the hawala networks identifiable by law enforcement and our intelligence community on the block chain, thereby breaking the tradition of hawala transfers, not maintaining a record of these transactions?

Mr. CASSARA. Congressman, I wish I could answer your question about the block chain.

Mr. BUDD. Sure.

Mr. CASSARA. I just can't. I just don't have access to that type of information. But one thing I am concerned about is the fact that bitcoins and cyber currency in general in the coming years will be used more and more to settle up between hawaladars.

Mr. BUDD. Okay. Is that valid that there is a tradition of not maintaining a record in hawalas?

Mr. CASSARA. They do maintain temporary records. I have interviewed hawaladars. I have seen their general—they use—again, it depends on the region of the world. Sometimes these are on Excel spreadsheets. Sometimes they are just paper ledgers. But yes, there are records, but it is not like a bank that has to keep these records, say, for 5 years, et cetera, et cetera, et cetera. They use them, then they dispose of them.

Mr. BUDD. Okay, thank you. Is there anything the U.S. can be doing differently to counter this growth without infringing on the largely peaceful users in the network? And that is for you or anyone on the panel. So would you say that we are on the right track?

Mr. CASSARA. Regarding hawala? No. We use this overused expression. There is no silver bullet. This issue is so complex and it involves, again, macroeconomics, microeconomics, literacy rates. That is a huge issue. There are certain areas in the world, for example Pakistan, where about 80 percent of the people are illiterate. So they do not want to go into a bank or a formal money services business simply because they are intimidated. It is hard for them to fill out forms. But they feel very comfortable talking to their local hawaladar, their tea shop owner who doubles as the hawaladar in their village, that type of thing.

So there is a lot of—and the devaluation of currencies and costs, all these things factor in. I wish I could say this is what we need to do, but there is just not that one silver bullet. We have to do a combination of things.

Mr. BUDD. Understood. Thank you. Mr. Chairman, I yield back.

Chairman PEARCE. The gentleman yields back. The Chair now recognizes the gentleman from Massachusetts, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman, and thanks for holding this hearing. I also want to thank our witnesses for your help.

Mr. Paul, with Oxfam, are we seeing a heightened use of bitcoin or alternative currencies in areas where you are doing most of your work?

Mr. PAUL. I couldn't say. I am not aware of any.

Mr. LYNCH. Okay. Let's go back. Mr. Cassara, one of the vulnerabilities that we see on this committee in places like Afghanistan, Pakistan, Iraq, Syria, and Yemen is that, first of all, our folks, our State Department folks are understaffed, number one, but oftentimes there is a mismatch in terms of, we don't have enough FinCEN or Treasury staff onsite. We just did a CODEL to the Gulf, and I think we have one young man who has three or four countries there, Bahrain, Dubai, a couple of others, that he is responsible for.

Do you think it would be helpful either to train up State Department personnel so they would be more tuned into this situation, or do you think it would be better—and I don't want to put you on the spot, I know the funding issues and all—every year, I put an amendment in to hire some more folks for FinCEN and give them a little bit more money to do their job. But do you think we could do a plus-up and help us in some of these tougher areas where we are seeing some illicit finance going on?

Mr. CASSARA. Thank you, Congressman. I think one issue is that there are not enough intelligence reporting requirements for embassies overseas and this whole area of illicit finance. I used to collect intelligence, and it was always helpful if headquarters, if you will, would say, ask these questions. I don't think that is happening enough, not in the area of illicit finance.

I also think there is not enough knowledge and awareness of many of our embassy staff overseas, whether it be State Department officials or others about these areas of illicit finance. Frankly, they are hard, and they are tasked to do many, many, many things.

Regarding FinCEN, let's understand that FinCEN is not law enforcement. They do not have law enforcement capabilities. They have analysts, or they have regulators, but they are not law enforcement. I am all in favor of re-energizing the Department of Treasury's Office of Enforcement, which was decimated at the creation of the Department of Homeland Security. Customs is gone. ATF is gone. Secret Service is gone. This is just me talking as an old-time Treasury Special Agent. I would love to see a revitalization of Treasury law enforcement that could get out overseas and understand these issues. They get the money in the value transfer. That is what they do.

Mr. LYNCH. Thank you. Mr. DeVille, I know you talked about your early efforts at FinCEN. And we actually had a role to play in standing up some of these financial intelligence units (FIUs) in some of these countries. And so are you involved right now in terms of your private business with Western Union, are you involved in Somalia at all or are you completely out of there?

Mr. DEVILLE. No, Congressman, we are in Somalia. I have the numbers here. We are in Somaliland, and it has been difficult to find an agent in Somalia.

Mr. LYNCH. We have just recently been authorized to go into Mogadishu, but are pretty much restricted to the airport and a few

other secure sites. Do you have anything in Mogadishu? Because I understand that the Somali nationals are actually coming over to Kenya, but there are a couple of safe sites, and are doing their business, remittances and all that. But that is less than ideal.

Mr. DEVILLE. It is—and I am sure Mr. Paul can testify—an area that really needs remittance support. We have been able to find an agent with whom we are satisfied in Somaliland, but we have not been able to find a satisfactory agent in Somalia. So we are not there at the moment.

Mr. LYNCH. Okay, great. Mr. Paul, I only have 20 seconds left, but Somalia, any ideas, any answers about how we might better service the people in that area, given the problems with Al-Shabaab?

Mr. PAUL. Yes, thanks for the question, Congressman. There are about a dozen Somali MTOs that operate in the United States. As I said, they are licensed, they are regulated, they are regularly examined, they cooperate with law enforcement. They have now been pushed to the very margins of the banking system. Most of them are unbanked. A few of them have one bank account through which they can transmit some funds.

They are very efficient and trusted by Somali-Americans and by Somalis in the country. But they need more—they need stronger intervention and more assistance to stay within the banking system.

Chairman PEARCE. The gentleman's time has expired.

Mr. LYNCH. Thank you, Mr. Chairman.

Chairman PEARCE. The gentleman's time has expired. The Chair now recognizes the gentleman from Ohio, Mr. Davidson, for 5 minutes.

Mr. DAVIDSON. Mr. Chairman, thank you, and thank you, witnesses, for your testimony. I really appreciate the things I have been able to learn from you today and from previous discussions with some of you.

I am curious, if you go down the line—there are only two who are in the business of moving money. U.S. origin to U.S., we are talking about illicit finance and we are talking generally from a U.S. destination to a non-U.S. destination. And other times from a non-U.S. destination into the United States.

But it mostly flows out. And to talk about a portion of illicit finance it seems to be much easier to get the heroin into the country than it is to get the cash out. That is what they are after. But in a lot of cases, the cash out goes for other purposes.

I am curious about the cash movements between people in the United States to people in the United States. How much of that is happening?

Mr. DEVILLE. I will start. Actually, both by volume and by principal, U.S. to U.S. is—it is the highest in both, at least at Western Union. And U.S. to Mexico is second. And then you can imagine U.S. to China, U.S. to India.

Mr. DAVIDSON. Right. And so do you have a way to track U.S. citizen to U.S. citizen? Or do you track U.S. person, non-U.S. citizen to—

Mr. DEVILLE. We certainly track the transactions, just as we would if they were cross-border transactions, we track them in the

United States. As I mentioned earlier, there are ID thresholds at which review—we are actually stricter than what the law requires. And then we also have an IBM product called Galactic ID, which affixes a number to every customer, and it has these incredibly complex algorithms. But if a customer uses a false ID but the same phone number, it would unite those together. So we try to get—it gives us a unique identifier to every customer, not perfect, but it does.

Mr. DAVIDSON. Thank you. Does your system allow you to discern and differentiate between U.S. citizens and non-U.S. citizens?

Mr. DEVILLE. No, there is no ability to do that, short of requesting a passport. But most—

Mr. DAVIDSON. So you create some form of identity, unique identifier to the citizen. I guess my question is, do you assume that the risk posed by a U.S. citizen is equal to the risk posed by a non-U.S. citizen?

Mr. DEVILLE. In the risk calculation, there is no differentiation made. And of course, when you think of non-U.S. citizens, I know there are certainly illegal aliens here, but then there are also foreigners who are here under visa. So there is no way to distinguish those in terms of risk.

Mr. DAVIDSON. And any other products you are using?

Mr. OPPENHEIMER. The only other thing I would add, as part of the discussion around domestic transfers, we do all international money transmission, but it is really important to understand the benefit of having a digital platform, because when you take out the brick-and-mortar component, customers have already gone through that KYC system to be part of the financial system, and then there is a lot of innovation that is happening to be able to offer customers better solutions.

So the more that I think Congress can encourage innovation and getting people into the formal banking system, the less risky it is.

Mr. DAVIDSON. I guess I am curious about the risk—at the most basic level, do U.S. citizens have an increased confidence of privacy? Citizenship is differentiated in that respect. In terms of risk, if you have somebody who is known to already be illegal, we can say that their respect for the law is at least different from the get-go. And it seems that your current products don't differentiate. I guess the next question I have relates to international.

And so, Mr. Cassara, Mr. Paul, you guys may be able to comment. A lot of the money transfers that are happening outside the United States are moving through mobile telephone networks, particularly in Africa. U.S. persons aren't necessarily involved in that, so some of the current provisions that apply here don't. What best practices are you aware of that are going on there that give us some insight into the illicit transfer of money there?

Mr. PAUL. Thanks for the question, Congressman. Mobile payment systems have been more or less useful in different jurisdictions. And a lot of that has to do with the telecommunications regulation of the jurisdiction and the interoperability of the networks within the jurisdictions. So Mr. Oppenheimer can probably talk a bit more about M-Pesa, which has been increasingly valuable and useful in Kenya.

In Somalia, for example, I have seen a couple of different mobile payout systems, all of which incredibly useful for identifying customers, all of which are incredibly useful for efficient payouts, but aren't interoperable with one another, so they are of limited value.

Mr. DAVIDSON. Thanks. My time has expired. I guess my last question would be, because it is somewhat sensitive, if you who are willing would respond to any gaps that you see in our current system, whether it is inside the United States or with our ability to track outside the United States transfers, that would be terrific. I would much appreciate it.

Mr. Chairman, I yield back the time I no longer have.

Mr. DAVIDSON. The gentleman's time has expired. The Chair now recognizes the gentlelady from Utah, Mrs. Love.

Mrs. LOVE. Thank you all for being here today. I know we have talked a lot about terrorist financing, which is incredibly important. But I would like to focus on a different aspect of illicit financing, namely activities pertaining to human and sex trafficking.

Could you tell me a little bit about the work that Western Union is doing in regards to sex trafficking? In other words, we had somebody from your office come in and talk to us a little bit about how transactions or certain things are set up that raise red flags when it comes to those specific issues. Would you mind telling me a little bit about that?

Mr. DEVILLE. Certainly, Congresswoman Love. And it is one of the things that we take the most seriously. In August of 2013, Western Union partnered with DHS on the Project Blue campaign, which is designed to combat human trafficking. I know you are familiar with it.

We have also, specifically to your question, developed transaction controls that are designed specifically to detect transactions that are possibly related to exploitation of children. I'll give you an example. Again, I will be vague, because we don't like to reveal our—

Mrs. LOVE. Right, you don't want to let it out.

Mr. DEVILLE. —controls, because right away, the bad guys find out.

Mrs. LOVE. I get it.

Mr. DEVILLE. But these RTRA rules I mentioned, the up-front rules in my opening statement, there are three that come to mind in the Philippines. A payee is stopped from receiving more than a certain number, and we have a fixed number of transactions in a rolling period. I won't say the period of time.

We also stop the transaction if a payee is receiving more than a certain number of transactions from senders in a rolling period. And then we also do it by dollar amount and transaction amount.

And there is one example that comes to mind in the Philippines, as well, where information we gave—it wasn't solely us, but it was also two other banks—actually led to the local authorities kicking down a door and rescuing children. It was a photo shop where they were being held, and then people were paying online to view the children, as you can imagine. So that was particularly gratifying. And there was some media on it, as well.

Mrs. LOVE. Is there a way that you interact with law enforcement that is different in the realm of human trafficking than in regards to other, for instance, terrorist activities? When you are re-

acting to law enforcement, do you see specific behaviors and react with the local law enforcement a little differently?

Mr. DEVILLE. We established something—I will briefly describe—it is called our rapid response team within our financial intelligence unit. And within—there are really two categories to which it will respond. One is exactly the two you mentioned, the terrorist attack, and the other is child trafficking, human trafficking.

And as soon as a suspect is identified, within 48 hours the rapid response team will have scrubbed all the transactions in the Western Union system across all our platforms to look for connections. And we also take it out another layer, as well. And those SARs get priority, and we also have a formalized procedure where we will pick up the phone and call law enforcement. DHS is usually the agency involved in child trafficking, and other agencies in terrorist finance. And we will call them to alert them to the information we have found. We don't wait for a subpoena.

Mrs. LOVE. Okay. Do you think that there is anything that we could be doing or doing better to disrupt and stop the money flow that is surrounded around human trafficking?

Mr. DEVILLE. The best thing, Congresswoman, would be—it is similar to on the OFAC side with terrorist names—if law enforcement can get us names and identifying information, we will scan all our transactions. We don't wait for that. It is just like with terrorist financing. You stop and think about it. We certainly have the lists from the government against which we screen and various governments around the world, but we are also—and we accept this burden—we are also expected to find things that law enforcement cannot based upon transaction analysis.

Mrs. LOVE. Right, and you are missing parts of the puzzle, also.

Mr. DEVILLE. Yes, exactly.

Mrs. LOVE. Yes.

Mr. DEVILLE. Even things they can't find. But we readily accept that responsibility.

Mrs. LOVE. Mr. Oppenheimer, I know that Remitly has been doing some work also surrounding that. Can you tell me just briefly if there are any ways or any type of set-ups or transactions that you realize have popped up that put up a red flag for you, also?

Mr. OPPENHEIMER. Yes, I think that we have built our system from day 1 to detect—I am really happy you brought up this issue—all sorts of nefarious activity. And similarly, we try to track that proactively, work with law enforcement if we see anything, such that we are a partner in being part of the solution.

Mrs. LOVE. Okay, thank you so much for being here. At this time, I yield back. Thank you.

Chairman PEARCE. The gentlelady's time has expired. The Chair now recognizes the gentleman from Washington State, Mr. Heck, for 5 minutes.

Mr. HECK. Thank you, Mr. Chairman. So I was sitting here thinking about somebody in my hometown of Olympia, Washington, who goes down to the credit union for a remittance, which they may be doing business with Remitly, who has a correspondent bank relationship that then sends it overseas where it is maybe met by another correspondent bank before it is transferred to a bank. And I just wondered in the spirit I think it was of Mr.

Oppenheimer's streamlining observation, what is the particular value add of requiring multiple SARs for the same transaction?

Elemental question, but I don't really understand, why do we need—in that instance, we would have three domestically. What is it that we really get out of that, that helps us achieve what we are trying to do here? Anybody?

Mr. DEVILLE. Thank you, Congressman. I assume you mean multiple SARs filed by multiple financial institutions?

Mr. HECK. Correct.

Mr. DEVILLE. This is something I have talked to my colleagues about. And there are duplicative SARs certainly being filed on the same individuals. Now, law enforcement would say—and there is certainly some validity to it—that you and the financial institutions don't see the whole picture. There might be a small dollar amount SAR at Western Union, a small one at Citi, a small one at PayPal, but combined together to law enforcement, they do, in fact, have value.

The other thing is that under 314(b), we could share that information, and that is a value of 314(b). So to answer your question, often there probably is no value in duplicative SARs, but there are instances where they are needles in a haystack that law enforcement can bring together.

Mr. HECK. But is it not possible for that data to be rolled up into the single SARs by one of the institution when there are multiple financial institutions involved?

Mr. DEVILLE. There is a consortium that we have recently been invited to that tries to do that very thing, and it has gained permission from FinCEN for a pilot program. Another example is—somewhat related is, we have—are about to start a terminated agent database, where we will—with FTC and FinCEN authority share when a Western Union agent is terminated by us—they could go across the street and become a Moneygram agent or vice versa. We have secured permission to have a database that we can query when signing up a new agent to make sure it is not one that Moneygram has recently suspended. And we thank FinCEN and the FTC for allowing that.

Mr. HECK. So are there other countries that do things better than we do that strike, in Mr. Perlmutter's words, the appropriate balance between the issues of national security and counterterrorism and efficiency? Do we have anything to learn from any other countries' practices in this regard?

Mr. DEVILLE. Honestly, I would say that the information sharing, particularly in terrorist finance in Europe, is far less than in the U.S. We really see duplicative SARs. After the Paris attacks, for instance, and we have spoken about this publicly, so it is okay. And we diagramed it where we receive from a dozen different entities in Europe a duplicative request where it was clear to us they were not talking to each other.

It is much harder to de-conflict in those situations. And you can file a voluntary SAR, for instance, in the United States. In many countries, you cannot. So certainly improvement to be made here, but I find it even more problematic in Europe.

Mr. HECK. Mr. Oppenheimer, you said earlier about considering raising the threshold. I have to tell you, it has been my observation

that once a threshold is enacted, it is the most stubborn thing in the world. I think of CTRs 1972, the index for inflation, holy cow. I also think about SIFIs. And there are a considerable number of voices, myself included, who would argue that what we ought to be doing in the area of SIFIs is looking more qualitatively and not quantitatively, i.e., what is the risky behavior you are engaged in? Is that at all a parallel here? Is it—should we have thresholds at all? Or is this about qualitative risk assessment?

Mr. OPPENHEIMER. I appreciate the question, and I think that the important thing with things like the travel rule, as you mentioned, it has not, I think, with the travel rule been updated since 1995. And so going back and looking at what those thresholds are, in my written testimony, I talk about decreasing the threshold to $1,000. We have to collect right now SSN and passport for any transaction over $3,000, decreasing that to $1,000, but then actually doing KYC on those customers, and doing a more in-depth identification process. I think that certainly those rules can be revisited, which would be a good thing for national security.

Mr. HECK. Thank you. I yield back, and I appreciate the opportunity to participate, Mr. Chairman.

Chairman PEARCE. The gentleman's time has expired. I would like to thank each one of you for your testimony today.

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.

Seeing no other participants, this hearing is adjourned. Thank you.

[Whereupon, at 4:20 p.m., the hearing was adjourned.]

A P P E N D I X

July 18, 2017

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Committee on Financial Services
Terrorism and Illicit Finance Subcommittee

Managing Terrorism Financing Risk in Remittances and Money Transfers

JOHN CASSARA

Board of Advisors Member
Center on Sanctions and Illicit Finance, FDD

Washington, DC
July 18, 2017

John Cassara July 18, 2017

Chairman Pearce, Ranking Member Perlmutter and members of the House Financial Services Subcommittee on Terrorism and Illicit Finance, thank you for the opportunity to testify today. It is an honor for me to be here.

"Without money, there is no terrorism."

This simple truism was recognized early on. A few days after the deadliest terrorist attack in U.S. history, President George W. Bush stated, "Money is the lifeblood of terrorist operations. Today we are asking the world to stop payment."

Almost sixteen years after the September 11 attacks, we are meeting here in part to ask, "Has America and the world stopped payment?"

The answer is not simple, particularly when it comes to both formal and informal remittance systems. Unfortunately, we have seen how successful terrorist and organized criminal groups diversify their funding sources and methods. These include remittance networks. Moreover, our adversaries are creative. They adapt to our countermeasures.

I am joined by colleagues with tremendous expertise in the formal remittance industry. So, I would like to primarily address my remarks to informal remittances sometimes known as informal value transfer systems (IVTS), parallel banking, underground banking, or sometimes just "hawala."

Long before the September 11 terrorist attacks, I was concerned about informal value transfer and remittance systems. I investigated some of these networks in Europe and the Middle East. Through subsequent books and articles I have been trying to draw attention to them. These systems exist here in the United States and though regulated as money services businesses after 9/11,[i] for the most part, continue to operate under the radar screen of many U.S. law enforcement and regulatory bodies.

I would like to briefly discuss the magnitude of the problem; how hawala and similar systems operate; why they are attractive to their customer base; how hawala brokers settle accounts; the futility of our current countermeasures, worrisome links to terror finance and criminality; vulnerabilities; and some suggested steps forward.

Magnitude

There are an estimated 244 million migrant workers around the world.[ii] Globalization, demographic shifts, regional conflicts, income disparities, and the instinctive search for a better life continue to encourage ever more workers to cross borders in search of jobs and security.

Many countries are dependent on remittances as an economic lifeline. Although estimates vary, according to the World Bank global remittances may have reached approximately $575 billion in 2016.[iii] Western Union, Money Gram, Ria Money Transfer, Dahabshill are just a few of the

well-known companies that provide official remittance services for the world's migrants. Of course, banks and non-bank financial institutions are also used. In 2013, some of the top recipients for officially recorded remittances were India (an estimated $71 billion), China ($60 billion), the Philippines ($26 billion), Mexico ($22 billion), Nigeria ($21 billion), and Egypt ($20 billion). Pakistan, Bangladesh, Vietnam, and the Ukraine were other large beneficiaries of remittances. As a percentage of GDP, some of the top recipients were Tajikistan (48 percent), the Kyrgyz Republic (31 percent), Lesotho (25 percent), and Moldova (24 perc$200ent).[iv]

In 2015, approximately $133,552,000,000 in remittances was sent from the United States to other countries. Top recipients include Mexico, China, the Philippines, and Vietnam.[v]

The above are estimates of what is *officially* remitted. Unofficially, nobody knows. However, the International Monetary Fund believes, "Unrecorded flows through informal channels are believed to be at least 50 percent larger than recorded flows."[vi] So, using the above World Bank and IMF estimates, *unofficial* remittances may be greater than $850 billion per year, with a substantial portion of that originating from the United States.

Informal channels operate outside of the ironically labeled "traditional" channels. It's ironic because for most of the migrants involved, the alternatives to Western-style or formal remittances are very traditional for them.

Informal remittances are sometimes touted as a new phenomenon and a symptom of the emerging borderless world. They have also erroneously been labeled "a measure of success" in our efforts to combat international money laundering and terrorist finance due to our crack down on illicit money moving through formal banking channels. Yet diasporas and remittances have existed since ancient times. For example, the Chinese practice of fei-chien, or "flying money," dates back to the T'ang Dynasty (618-907 AD).[vii]

The following is a partial list of worldwide informal remittance systems. The names vary based on a number of factors including geographical locations and ethnic groups:

- Hawala – India, Afghanistan, Africa, the Middle East, Gulf, parts of the Americas
- Hundi – Pakistan, Bangladesh
- Undiyal – Sri Lanka
- Havaleh – Iran
- Door-to-door / padala – the Philippines
- Black market currency exchanges – Nigeria, South America, Iran
- Stash houses / casas de cambio – Latin America
- Phoei kuan – Thailand (Teochew Chinese)
- Hui kuan – China – (Mandarin Chinese)
- Fei-chien – "flying money" China
- Ch'iao hui – overseas remittances – (Mandarin Chinese)

- Chop shop – foreigners sometimes use this term for one of the Chinese systems
- Chiti-banking – (refers to the "chit" used for receipt or proof of claim in transactions; introduced by the British in China)

The two largest underground remittance systems are hawala (and its various sister systems such as hundi and undiyal) and the Chinese fei-chien (and its corollaries). They are both global in scope. While there are no reliable estimates as to the magnitude of these two informal remittance systems, both are probably responsible for hundreds of billions of dollars in unregulated (and non-taxed) money transfers a year.[viii]

Although diverse, alternative remittance systems are found throughout the world, most share a few common characteristics. The first is that they all transfer money without physically moving it. Another is that they all offer the three C's: they are certain, convenient, and cheap. They are all ethnic based. They are sophisticated and efficient. And finally, historically and culturally, most alternative remittance systems use trade as the primary mechanism to settle accounts or balance the books between brokers.

I would like to emphasize that I have the utmost respect for these systems.

The overwhelming percentage of money transfers generated by the use of these informal remittance systems is benign. They are primarily used to remit a portion of migrants' earned wages back to their home countries to support their families. We, of course, do not wish to interfere with this process.

However, because these systems are opaque and based on trust, they avoid our primary anti-money laundering and counter-terrorist finance (AML/CFT) countermeasures. As Osama bin Laden once said, jihadists are aware of the "cracks" in our Western financial system.[ix] Informal remittances are not just a crack but a Grand Canyon. There is no doubt that in addition to remitting wages, they are also abused by criminal and terrorist organizations.

How They Operate [x]

The definition of hawala was concisely expressed during the 1998 U.S. federal trial of Iranian drug trafficker and money launderer, Jafar Pour Jelil Rayhani and his associates. During the trial, prosecutors called hawala "money transfer without money movement." That is, a broker on one side of the transaction accepts money from a client who wishes to send funds to someone else. The first broker then communicates with the second broker at the desired destination who distributes the funds to the intended recipient (less small commissions at both ends). The money does not physically move from Point A to Point B. The key ingredient is trust. Most brokers are of the same ethnic group and many are members of the same family, tribe, or clan.

To illustrate how the hawala remittance process works, we will use a typical example. Ali is an Afghan national, recent immigrant, and a construction worker in Your District. (Note: While in

this example Ali is Afghan, he could just as easily be Pakistani, Iraqi, Syrian, Somali, North African, Lebanese, Indian, Chinese, etc.) Ali emigrated to the United States years ago and earns money that helps support his family. He periodically sends a portion of his salary back to his elderly father, Jafar, who lives in a village outside of Kandahar in southern Afghanistan. To make his monthly transfer - usually about $200 - Ali uses hawala. This is very common in Afghanistan. About 30 percent of its population is externally and internally displaced, and remittances from outside of Afghanistan are received by about 15 percent of the rural population. Hawala has been described as the de facto national banking system of Afghanistan.

If Ali went to a bank in Your District to send the money home to his father, he would have to open an account. He doesn't want to do that for a number of reasons. First, Ali grew up in an area of the world where banks are not common. He is not used to them and doesn't trust them. Next, Ali has little faith in governments and wants to avoid possible scrutiny. Many immigrants believe the government is monitoring their immigration status and/or will make them pay taxes. He also doesn't want the U.S. government to screen his money transfers to Afghanistan. In addition, although Ali has lived in Your District for a few years, he is still a bit intimidated. His English is marginal. He is only semi-literate (the literacy rate in Afghanistan is quite low) and cannot fill out the necessary forms. Moreover, banks charge their customers assorted transfer fees and offer unfavorable exchange rates. If Ali only earns a little money and is sending $200, bank transfer fees of 10 percent or more are quite substantial.

Generally speaking, the average cost of transferring funds through an alternative remittance system such as hawala between major international cities is about 2– 5 percent of the value transferred. (Globally, the cost of sending $200 through formal remittance companies averaged 7.45 percent in the first quarter of 2017, although this was significantly higher than the Sustainable Development Goal (SDG) target of 3 percent.[xi]) The price differential is in large part due to the fact that hawaladars (hawala brokers) generally don't have large brick and mortar businesses. Since they operate in the shadows, taxes and regulatory fees are minimal as well as administrative and personnel costs. Of course, prices in both the formal and informal remittance industries are influenced by a variety of factors. Hawala networks are most competitive when they operate in areas where banking systems and overt money remittance chains find it difficult, expensive, or high risk to operate – particularly in areas where our terrorist adversaries operate.

Delivery of a bank transfer to Jafar would pose additional problems. The number of licensed banks in Afghanistan is still small. They are used by only about ten percent of the population.[xii] Particularly in a poorly secured area such as Kandahar, Jafar does not want to leave his village home and travel a far distance to a bank.

In light of these problems and concerns, Ali uses a hawaladar in Your District who is a member of his extended clan and family. He feels comfortable dealing with him. The hawaladar also owns and operates an "import/export" company in Your District. The hawaladar completes the transaction for a lower commission than banks or money service businesses charge. In addition,

he obtains a much better exchange rate. Delivery direct to Jafar's home in the Kandahar area village is also included in the price. In fact, in certain areas of the world, hawala is advertised as "door-to-door" money remitting.

Ali gives the $200 to the hawaladar in Your District that he wants to transfer. The hawaladar takes his small commission. Ali is not given a receipt because the entire relationship is based on trust. This is a different kind of "know your customer" (KYC) procedure. For purposes of illustration, particularly if this is a first-time transfer, Ali may be given a numerical or other code, which he can then forward to Jafar. The code is used to authenticate the transaction. But in the nature of hawala networks, codes are not always necessary. As opposed to the often-lengthy formal operating requirements of bank-to-bank transfers, this informal transaction can be completed in the time it takes for the hawaladar in Your District to make a few telephone calls or send a fax or e-mail to the corresponding hawaladar in his network that handles Kandahar.

Hawaladars maintain very few records, offering customers near anonymity. They only keep simple accounting records, and even these are often discarded after they settle-up with one another. This means the paper trail is limited or nonexistent, making transactions very difficult to track for law enforcement. Even when records are kept, they are often in a foreign language or code, making them very challenging for Western authorities to decipher.[xiii]

Although some transactions are arranged directly between the two hawaladars involved, many are cleared or pass through regional hawala hubs such as Dubai, Mumbai, Karachi, and Kabul. So generally speaking, money can be delivered directly to Jafar's home within 24 hours and the transaction will not be scrutinized by either U.S. or Afghan authorities.

The above scenario with Ali in Your District could just as easily take place in Minneapolis with its large Somali community, northern Virginia with its large Indian community, or Detroit with its large Arab community.

Similarly, hawala transfers are very common in London, Frankfurt, Dubai, Damascus, Baghdad, Tehran, Karachi, Zanzibar, Durban, the Colon Free Trade Zone in Panama, the Tri-Border region of South America, and many other locations around the world. For example, according to the U.S. State Department 2015 INCSR report in the West African country of Gabon, "There is a large expatriate community engaged in the oil and gas sector, the timber industry, construction, and general trade. Money and value transfer services, such as hawala, and trade-based commodity transfers are often used by these expatriates, particularly the large Lebanese community, to avoid strict controls on the repatriation of corporate profits."[xiv]

Settling Accounts

Hawaladars eventually have to settle their accounts with each other. Frequently, the close relationships between the brokers help facilitate the settlement. Remember, the key ingredient in hawala is trust. So kinship, family and clannish ties often enable the settlement process. For

example, in Afghanistan, intermarriages between the families of hawaladars are common because they help cement confidence between the parties. Brothers, cousins, or other relations often operate in the same hawala network. Lebanese family members that operate in the same hawala networks can be found in Beirut, Dubai, the Colon Free Trade Zone, and various locations in Africa. Yet even though they may have familial or other ties, they are still in business to make money. Somebody is running a surplus and somebody a deficit. Payments go in both directions. For example, remittances may flow into South Asia from the United States and Europe but money and various goods flow back as well. Periodically, accounts must be settled. Generally, money transfers between hawaladars are not settled on a one-to-one basis but are bundled over a period of time after a series of transactions. A variety of methods are used to make payments and settle the accounts.

Trade: From the earliest times - before modern banking and before modern monetary instruments – trade based value transfer was used between hawala brokers to settle accounts and balance their books. The use of trade remains widespread. Settling accounts through import/export clearing is somewhat similar to bilateral clearing using bank transfers, but it uses the import/export of trade goods. That is why many import/export concerns are associated directly or indirectly with hawaladars. If a debt needs to be settled, hawaladar A could simply send goods to hawaladar B such as gold, electronics, or a myriad of other trade items. Or at the end of a reporting period, if an outstanding balance exists between hawaladar A in Somalia and hawaladar B in Dubai, B can use, for example, a Japanese bank account to purchase cars for export to Somalia. Once the cars arrive, they would be transferred to A to settle the debt and/or sell them for profit. The transaction would clear the debt between the two hawaladars.

Invoice fraud and manipulation is also widespread. To move money/value out of a country, a hawaladar or his agent will import goods at overvalued prices or export goods at undervalued prices. To move money/value in, a hawaladar or his agent will import goods at undervalued prices or export goods at overvalued prices. This type of procedure is called counter-valuation. Most other worldwide alternative remittance systems or informal value transfer networks are similarly based on trade. Historically and culturally, trade is still the preferred method of account settlement. [xv]

Banks: Most major hawala networks have access to financial institutions either directly or indirectly. A majority of international hawaladars have at least one or more accounts with formal financial institutions. Bi-lateral wire transfers between brokers to settle accounts are sometimes used. If a direct wire transfer is made between international brokers, hawaladar A would have to wire money directly to hawaladar B's account to clear a debt. This could be problematical because the banks' foreign exchange rate procedures would be triggered. So in this case, hawaladar A might choose to deposit the funds into B's foreign account.

Cash couriers: Direct cash payments are also used to settle debts. This is particularly true in areas of the world that have cash based economies. Sometimes overlooked is that hawala

networks also operate domestically between states and provinces. For example, in Afghanistan, hawala networks are found in each of the 34 provinces. Periodically, the brokers settle accounts and often use cash. Hawala couriers have been identified transporting money within Afghanistan and across the border into Pakistan. Cash couriers representing hawala networks also frequently travel from Karachi to Dubai to settle accounts.

Other methods: Over the last few years, there are indications that new payment products and services (NPPS)[xvi] are being added to the mix: virtual currencies and transfers, mobile payments, and other forms of person to person (P2P) money transfers.

Although open source reporting is very sparse, there is reason to believe that some underground remittance networks are now using virtual currencies, including bitcoins. For example, Indian police raided a money exchanger/hawaladar that allegedly used bitcoins.[xvii] Over time, the use of virtual currencies could potentially have a great impact on the hawala settlement process. Moreover, I can envision how an enterprising hawaladar will acquire bitcoins and use them not only to settle accounts between fellow brokers, but also use them as cash-out service for their clients. Cross border mobile payments network for emerging markets are currently processing air-time top-ups and money transfers in multiple currencies in real-time for duly licensed financial institutions, organizations, and merchants. And since most hawaladars have side businesses, bitcoins could also be used to purchase his product – for example, mobile phone credits.

In many areas of the world, mobile payments or M-Payments – particularly via the use of cell phones - are an increasingly popular vehicle for the remittance of wages. It is also quite possible for M-Payments to be used in the settling of accounts between underground money remitters including hawaladars.[xviii] M-Payments are recognized as a growing money laundering threat – particularly in areas of the world where our terrorist adversaries operate.[xix]

Etisalat Afghanistan, the Afghan telecommunications company, is now offering "M-Hawala." From its website, Etisalat Afghanistan boasts that "M-Hawala is an innovative mobile financial services solution that will enable Etisalat Afghanistan's customers to purchase airtime directly from their handsets, send money from their mobile phones to family and friends, pay their bills via their mobile phones, purchase goods and services from shops and or retail outlets and deposit or withdraw cash from Etisalat authorized M-Hawala distributors or Etisalat partner banks." [xx]

Over the last few years P2P money transfers have grown exponentially. There are many domestic and global services (some are interoperable) that make it easy to transfer money from one party to another via a phone number or email. Parties can send cash from an attached digital wallet account, or a linked debit card, bank account, or credit card. It is also easy to receive money; some services offer payments in brick-and-mortar stores as well.

In many respects, the growing use of P2P could mitigate the widespread use of hawala for traditional remittance purposes. I am not aware if P2P transfers are being used in the hawala

settlement process. If it is occurring, I suspect it is happening overseas and is linked to other forms of M-Payments (see above).

Consequently, one of the challenges to law enforcement is where regulatory regimes have not kept pace with the rapidly evolving business models and payments schemes.

Worrisome Links

Unfortunately, hawala is abused by terrorists. Hawala networks are used by ISIS in war-torn Syria and Iraq.[xxi] Hawala is used in Europe to support terror groups. For example, a network of 250 to 300 shops - such as butchers, supermarkets and phone call centers - run by mostly Pakistani brokers across Spain have supported ISIS and the al-Qaeda-affiliated Nusra Front through their hawala operations.[xxii] There are reports that hawala was used to help finance the 2015 ISIS attacks in Paris.[xxiii]

Hawala is widespread in South Asia and is heavily used by drug warlords and both the Afghan and Pakistani Taliban. Hawala networks exist in other troublesome spots where our adversaries operate such as the Horn of Africa.[xxiv] Hawala is "central" to Libya's underground economy.[xxv]

Boko Haram's funding is likely to withstand most restrictions on accessing the banking sector, as it uses hawala and cash couriers to move funds, some of which originates from supporters outside Nigeria.[xxvi]

Media reports indicate a surge in hawala funding from charity organizations in the Persian Gulf to madrassas and seminaries in the Kashmir Valley used to indoctrinate local youth.[xxvii]

Iran, a U.S. designated state sponsor of terror, also uses hawala —locally known as *havaleh*. The underground money transfer system has also been used to circumvent sanctions. [xxviii] Reportedly some financial exchanges between Iran and Pakistan are routed through hawala instead of the legal channels of the Asian Clearing Union. [xxix]

Iran's merchant community makes active use of money and value transfer systems, including hawala and moneylenders. Many hawaladars and traditional bazaari are linked directly to the regional hawala hub in Dubai. Over 300,000 Iranians reside in Dubai, with approximately 8,200 Iranian-owned companies based there. The trading companies are instrumental in settling accounts between hawaladars (see above). There are reports that billions of dollars in Iranian capital have been invested in the United Arab Emirates, particularly in Dubai real estate. Iran's real estate market is also used to launder money. [xxx]

The United States is not immune. Hawala has repeatedly been used to finance terror attacks against the U.S., including the 1998 bombing against our embassy in Nairobi, attacks against our troops in Afghanistan and Iraq, and the 2010 Times Square bombing in New York City. [xxxi] In 2013, a federal judge in San Diego sentenced three Somali immigrants for providing financial

support to al-Shabaab—a designated terrorist organization. Evidence presented during trial showed that the defendants conspired to transfer funds to Somalia via hawala to wage jihad.[xxxii]

Hawala is often used in other criminal activity. For example, in 2013 a naturalized U.S. citizen and his wife were indicted for medical billing fraud in Texas, and for sending the illicit proceeds to Iran via hawala.[xxxiii] In November, 2015, authorities in Los Angeles announced they had broken up an international hawala network with ties between Canada, India, the United States and other locations that moved millions of dollars for the Sinaloa drug cartel and other criminal groups.[xxxiv] And international criminal organizations from sex traffickers in Nigeria, fraudsters in Eastern Europe, to drug traffickers in Southeast Asia use hawala. Many of these criminal networks impact the U.S.

Countermeasures and Steps Forward

Registration

Similar to Western Union, Pay-Pal, casas de cambio, and "Mom and Pop" check cashing services, Treasury's Financial Crimes Enforcement Network (FinCEN) classifies hawala as a money services business or MSB.

As a result, hawala and similar money transfer systems are legal as long as the operation is registered with FinCEN and meets individual state licensing requirements. Unfortunately, the regulatory response hasn't worked. According to the 2007 National Money Laundering Strategy, "While the exact number of money service providers in the United States is difficult to determine, estimates suggest that fewer than 20 percent of MSBs are registered with FinCEN. It is not known what percentage of unregistered MSBs are exempt from registration, due for example to their low business volumes or agent status. Regardless, the result is that the vast majority of MSBs operate without direct Federal regulatory supervision."[xxxv]

Hawaladars are also supposed to file Suspicious Activity Reports (SARs). I believe very few do. Should we be surprised? Hawala is based on trust. Why would a hawaladar file a suspicious activity report on an extended family, tribe, clan, or ethnic group member?

The IRS/Criminal Investigation Division has the law enforcement mandate to ensure MSB compliance. Unfortunately, due to budget cuts and manpower constraints the IRS has been unable to conduct necessary assessments or compel MSBs to register. Mandated "outreach" programs that are designed to advise informal remittance networks of their registration and reporting responsibilities have also fallen short.

Before a strategy for enhanced MSB registration can be formulated I suggest this committee request the following information from FinCEN:

1. Over the last five years, how many hawaladars, fei-chien brokers, and other similar informal remittance operators have actually registered with FinCEN? Please ask that the registration totals be listed by year.
2. Of those that have registered, how many SARs have been filed? Per year?
3. A FinCEN request should be made to the Egmont Group of Financial Intelligence Units (FIUs) to poll its international members regarding questions 1 and 2 above. For the Egmont FIUs, a precursor question will be whether or not registration is required for hawala in their jurisdiction and, if so, under what authority.
4. Request that FinCEN estimate the number of informal unregistered money remitting entities currently in operation in all 50 states.
5. For the last five years, have FinCEN and the IRS detail their "outreach" programs to ethnic communities throughout the United States regarding the obligation to register and license money remitters.
6. Ask IRS/CI what it would need in additional budget and personnel to launch an aggressive campaign that targets unregistered and unlicensed money remitters.
7. Ask the FinCEN Intelligence Group to provide, on a classified basis as required, information related to the instance of emerging payments such as bitcoin and other virtual currencies used as hawala systems or financing.
8. Request that FinCEN provide any statistics or case examples related to its 314 program regarding inquiries related to hawala and terrorist financing, on a classified bases, as required.

Accountability

The U.S. government's *2007* Inter-Departmental *National Money Laundering Strategy* report's goal #2 is to "Enhance Financial Transparency in Money Service Businesses." The laudable goal contains eight "action items;" most are pertinent to this hearing. I urge Congress to exercise its oversight responsibilities and determine whether or not the action items were fulfilled and hold the departments, offices, and bureaus involved responsible if they have not.

Examine the "back door" of Trade

Hawaladars are most vulnerable to law enforcement, customs, and intelligence agencies when they settle accounts. As discussed above, historically and culturally, in many parts of the world settling accounts via trade-based value transfer is the preferred technique. One does not understand hawala and underground remittance systems unless one understands this concept.

Particularly in areas where our adversaries operate, examining trading records for signs of "counter-valuation" or a method of settling accounts between hawala traders could be the backdoor into their operations. Systematically cracking down on associated trade fraud could also be a boon to revenue strapped governments. (Sometimes offering the "carrot" of increased

revenues to cash-strapped governments is often more effective than the "stick" of heavy handed enforcement.)

In 2003 I proposed the creation of Trade Transparency Units or TTUs to spot trade anomalies that could be indicative of customs fraud, money laundering, or even underground financial systems such as hawala.[xxxvi] The concept is now part of our national anti-money laundering strategy. To date there are approximately 16 international TTUs. Many additional countries have expressed interest in joining the TTU network. Congress should create a specific line item that funds the expansion of the U.S. TTU to include additional dedicated personnel and advanced analytics.

Over the last few years, there has been an explosion in trade and related data. Advanced analytic programs are available. Trade anomalies can be identified such as over-and-under invoicing by making a comparison to market norms. [xxxvii] We could specifically risk-score the probability of informal value transfer /counter-valuation. Analytics are available to help over worked analysts and investigators prioritize trade-based money laundering (TBML)-related investigations and help with investigative decision making. For example, we can apply subjective logic analytics to the high levels of uncertainty inherent in hawala networks. Potentially models could be built to help prioritize which cases of potential TBML should be pursued.

Funds should also be provided to the U.S. TTU and the State Department's Bureau of International and Narcotics Affairs (INL) that will assist with the creation of additional foreign TTUs. Any funds expended will be more than made up by enhanced revenue collected by cracking down on associated customs fraud.

Examine Fei-Chien

While hawala gets attention because of its links to terror finance, the Chinese equivalent fei-chien or "flying money" is undoubtedly as large and pervasive. As I outline in my book *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement,*[xxxviii] fei-chien is ancient; it operates in the same manner as hawala; Chinese flying money is international in scope; it relies on trade to settle accounts between brokers; and while used primarily for remittances, the underground system has also been linked to criminal organizations and capital flight.

I believe flying money is used by wealthy Chinese to help purchase high-end residential real estate (including in the United States [xxxix]) in probable violation of China's own capital controls. FinCEN is currently studying the purchase of high-end real estate and its links with money laundering in specific geographic areas. [xxxix]

Unfortunately, our law enforcement, intelligence, and regulatory communities have little knowledge or interest in fei-chien and other forms of underground Chinese remittance systems.

Open source information on fei-chien is limited and I fear there is little classified information as well. I suggest this Committee task FinCEN to develop a strategic study on the prevalence of Chinese flying money and how it impacts the United States.

Data and Analysis

Since many hawaladars and similar underground financial networks often use financial institutions, advanced analytics should be employed to provide the transparency that the hidden systems seek to deny. AML/CFT compliance software could be coded to provide red-flag alerts and/or risk scoring specifically for informal remittance systems such as hawala. Diverse data sets (financial, social media, etc.) could be examined and suspicious activity indicators installed for transfers to/from suspect locations, suspect businesses, individuals on designated lists, etc. Applicable overseas data sets could be analyzed and cross-referenced against suspect remittance service providers in the United States.

The same should be done with financial institutions that deal heavily in trade finance. AML/CFT compliance software should be engineered to flag alerts for indications of trade-based money laundering which, per the above, could be the back door into underground remittance networks.

Inclusion

One of the primary reasons immigrants use informal remittances is cost. As a result, the formal financial system—banks and remittance services— should improve their services and reduce charges and fees for remittances. This will attract more customers into the formal and transparent banking and remittance sectors. Lower cost structures are currently one of the major marketing features of M-payments in emerging markets.

Training

In my opinion, a staggering amount of compliance officers and those involved with trade finance do not understand informal remittance systems and how to recognize them. Only with specific insight into hawala and other similar systems will AML/CFT compliance staff responsible for risk monitoring be able to properly react to flagged transactions or adjust risk exposure. Financial institutions and MSBs that are exposed to informal remittance systems and TBML should do more to provide training and assistance to staff. Training in this area should be part of AML/CFT compliance review.

I have firsthand knowledge that law enforcement personnel at the federal, state, and local levels as well as intelligence officers, regulators, analysts, etc. similarly do not understand informal remittance systems and TBML and do not know how to recognize them in their area of operations.

Even though I can demonstrate how informal remittances and TBML affects state and local law enforcement, most often the consensus opinion is, "This is a federal issue and doesn't concern us."

Yet it is precisely because law enforcement officers are on the front lines in their communities and know their operating environment well that they should notice if a local business or commercial activity does not make market or economic sense. For example, a normal business should not remain in operation for long with sporadic commercial activity or when consistently selling goods far above or below market norms. Numerous businesses in the U.S. and elsewhere are involved at the local level in TBML schemes and deal with goods that are frequently manipulated to transfer value. Underground remittance networks such as hawala and fei-chien are found in local communities throughout our country and they often depend on trade and local business networks.

Accordingly, I urge my state and local law enforcement colleagues to become more familiar with issues surrounding TBML and informal remittance schemes and how they affect the local community. Where appropriate, trade fraud and associated crimes should be part of their financial investigations education. The State and Local Anti-Terrorism Training (SLATT) program[xl] funded by the U.S. Department of Justice, Bureau of Justice Assistance (BJA) is an excellent starting point. The SLATT program is dedicated to providing specialized multiagency antiterrorism detection, investigation, and interdiction training and related services at no cost to our nation's law enforcement officers, who face the challenges presented by the terrorist and violent criminal extremist threat – including the detection of opaque underground financial systems sometimes employed by terrorists.

It is of paramount importance the SLATT program continues to be offered in the field.

John A. Cassara is a former U.S. intelligence officer and Treasury Special Agent. More information is available at www.JohnCassara.com

---

[i] Section 359 of the USA PATRIOT Act expanded the definition of "financial institution" to include not only a licensed sender of money but any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside the conventional financial institution system. See 31 U.S.C.5312(a)(2)(R)

[ii] United Nations; available online at http://www.un.org/sustainabledevelopment/blog/2016/01/244-million-international-migrants-living-abroad-worldwide-new-un-statistics-reveal/

[iii] The World Bank; available online at: http://www.worldbank.org/en/news/press-release/2017/04/21/remittances-to-developing-countries-decline-for-second-consecutive-year

[iv] The World Bank; available online at: http://www.worldbank.org/en/news/press-release/2013/10/02/developing-countries-remittances-2013-world-bank

[v] The World Bank; available online at http://www.pewglobal.org/interactives/remittance-map/

[vi] Dilip Ratha, "Remittances, Funds for the Folks Back Home," International Monetary Fund; available online: http://www.imf.org/external/pubs/ft/fandd/basics/remitt.htm

[vii] Leonides Buencamino and Sergei Gorbunov, "Informal Money Transfer Systems: Opportunities and Challenges for Development Finance," November, 2002, United Nations; available online: http://www.un.org/esa/esa02dp26.pdf

[viii] Estimates vary as to how much money is pumped annually through the global hawala network but according to Gretchen Peters research in *Seeds of Terror*, St. Martins Press, 2009, p. 170, economists put the total figure at about $100 billion per year. Others estimate hawala transfers approach $400 billion annually; see Jack Moore, Hawala, The Ancient Banking Practice Used to Finance Terror Groups, *Newsweek*, February 24, 2015; available online at: http://www.newsweek.com/underground-european-hawala-network-financing-middle-eastern-terror-groups-307984. Because the global nature of the Chinese diaspora, I believe "flying money" is at least equal to or surpasses the magnitude of hawala.

[ix] Chairman Evan Bayh, "Hearing on "Hawala and Underground Terrorist Financing Mechanism," November 14, 2001; available online: https://www.banking.senate.gov/01_11hrg/111401/bayh.htm

[x] The information in this section is taken from John Cassara, *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement*, Wiley, 2015; see chapter on Hawala: An Alternative Remittance System, pages 49 – 69 and original references.

[xi] The World Bank; available online at: http://www.worldbank.org/en/news/press-release/2017/04/21/remittances-to-developing-countries-decline-for-second-consecutive-year

[xii] International Narcotics Strategy Report Volume II on Money Laundering, State Department, 2015, see Afghanistan country report; available online at: https://www.state.gov/j/inl/rls/nrcrpt/2015/supplemental/239124.htm

[xiii] Financial Crimes Enforcement Network (FinCEN) # 33, March, 2003; available online at: https://www.fincen.gov/sites/default/files/advisory/advis33.pdf

[xiv] International Narcotics Control Strategy Report, Volume II, Money Laundering, Department of State, 2015; available online at: https://www.state.gov/j/inl/rls/nrcrpt/2015/vol2/index.htm See Gabon country report.

[xv] Trade-based money laundering being used as counter valuation for hawala and other informal value transfer systems is described in detail in my book *Trade-Based Money Laundering;* see ix

[xvi] See Guidance for a Risk-Based Approach: PREPAID CARDS, MOBILE PAYMENTS AND INTERNET-BASED PAYMENT SERVICES, Financial Action Task Force (FATF), June, 2013.

[xvii] "Bitcoins May be Used by Hawala Traders: Official," The Times of India, December 29, 2013; available online (http://timesofindia.indiatimes.com/city/ahmedabad/Bitcoin-may-be-used-by-hawala-traders-Officials/articleshow/28067184.cms)

[xviii] For an overview of Mobile Payments see John A. Cassara , Written Statement for the Hearing On "The Next Terrorist Financiers: Stopping Them before They Start" Before the Task Force to Investigate Terrorism Financing Of the House Financial Services Committee, June 23, 2016; available online at: https://financialservices.house.gov/uploadedfiles/hhrg-114-ba00-wstate-jcassara-20160623.pdf

[xix] Ibid

[xx] See Etisalat press release; available online: http://www.etisalat.af/about-us/press-releases/183-etisalat-launches-mhawala-mobile-financial-services-in-afghanistan and the Mhawala website; http://mhawala.af/

[xxi] See Yaya J. Fanusie and Alex Entz," Islamic State - Financial Assessment," Foundation for the Defense of Democracies, March 2017; available online at: http://www.defenddemocracy.org/content/uploads/documents/CSIF_ISIS_Finance.pdf

[xxii] Jack Moore, Hawala, The Ancient Banking Practice Used to Finance Terror Groups, *Newsweek*, February 24, 2015; available online at: http://www.newsweek.com/underground-european-hawala-network-financing-middle-eastern-terror-groups-307984

[xxiii] Rukmini Callimachi, Alissa J Rubin, Laure Fouquet, Paris attacks: terrifyingly fatal layers of resources and tactics, *The Irish Times*, March 20, 2016; available online at: http://www.irishtimes.com/news/world/europe/paris-attacks-terrifyingly-fatal-layers-of-resources-and-tactics-1.2580749

[xxiv] See Yaya J. Fanusie and Alex Entz," Al-Shabaab - Financial Assessment," Foundation for the Defense of Democracies, May, 2017; available online at: http://www.defenddemocracy.org/content/uploads/documents/CSIF_TFBB_Al-Shabaab_v05_web.pdf

[xxv] Yaya Fanusie and Landon Heid, *Foreign Affairs*, June 17, 2016; available online at; https://www.forbes.com/sites/realspin/2016/06/17/what-isis-is-banking-on/#50fe1cc11651

[xxvi] See Yaya J. Fanusie and Alex Entz, "Boko Haram Financial Assessment," Foundation for the Defense of Democracies, May, 2017; available online at: http://www.defenddemocracy.org/content/uploads/documents/CSIF_Boko_Haram.pdf and Kathleen Caulderwood, "Fake Charities, Drug Cartels, Ransom and Extortion: Where Islamist Group Boko Haram Gets Its Cash," International Business Times, May 16, 2014; available online at: http:// www.ibtimes.com/fake-charities-drug-cartels-ransom-extortionwhere-islamist-group-boko-haram-gets-its-1585743

[xxvii] "Gulf funds being used to radicalize Kashmir youth", *Daily Excelsior*, 24 April 2016; available online at: http://www.dailyexcelsior.com/gulf-funds-used-radicalise-kashmir-youth/

[xxviii] Rick Gladstone, "Iran Finding Some Ways to Evade Sanctions, Treasury Department Says," *New York Times,* January 10, 2013; available online at: http://www.nytimes.com/2013/01/11/world/middleeast/iran-finding-ways-to-circumvent-sanctions-treasury-department-says.html

[xxix] Reschikov, Oleg, "Iran: Opposition to Western Sanctions in the Banking Sector", *New Eastern Outlook*, January 30, 2015 available online at: http://journal-neo.org/2015/01/30/rus-iran-protivodejstvie-zapadny-m-sanktsiyam-v-bankovskoj-sfere/

[xxx] International Narcotics Control Strategy Report, Volume II on Money Laundering, U.S. Department of State, 2015, See Iran country report; available online: https://www.state.gov/j/inl/rls/nrcrpt/2015/supplemental/239219.htm

[xxxi] "Manhattan U.S. Attorney Charges Long Island Man with Engaging in Hawala Activity That Funded Attempted Times Square Bombing," FBI Press Release, September 15, 2010; available online at: https://archives.fbi.gov/archives/newyork/press-releases/2010/nyfo091510a.htm

[xxxii] "Three Somali Immigrants Sentenced for Providing Support to Foreign Terrorists," FBI Press Release, November 18, 2013; available online at: https://archives.fbi.gov/archives/sandiego/press-releases/2013/three-somali-immigrants-sentenced-for-providing-support-to-foreign-terrorists

[xxxiii] "Healthcare Fraudsters Sent $1.1 Million to Iran," *Money Jihad*, March 26, 2013; available online at: https://moneyjihad.wordpress.com/2013/03/26/health-care-fraudsters-sent-1-1-million-to-iran/

[xxxiv] Joel Rubin, "Drug cartel money-laundering indictment is first major effort against hawala tactics," *Los Angeles Times,* October 2, 2015, available online at: http://www.latimes.com/local/crime/la-me-hawala-drug-money-20151003-story.html

[xxxv] 2007 National Money Laundering Strategy Report; available online at: https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf

[xxxvi] See my February 3, 2016 testimony before the Task Force to Investigate Terrorism Financing of the House Financial Services Committee available online at: https://financialservices.house.gov/uploadedfiles/hhrg-114-ba00-wstate-jcassara-20160203.pdf; Also, see John Cassara, *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement*, 2016 John Wiley & Sons, Hoboken, New Jersey; see chapter 9 page 145 on "Monitoring Trade."

[xxxvii] Ibid

[xxxviii] Ibid, Cassara TBML; see chapter 5 on "Chinese Flying Money."

[xxxix] John Cassara, "Flying money" may land in U.S. - Is Chinese money laundering "flying" into real estate?" February 21, 2016, *Banking Exchange;* available online at: http://www.bankingexchange.com/news-feed/item/6079-flying-money-may-land-in-u-s

[xxxix] See https://www.fincen.gov/news/news-releases/fincen-expands-reach-real-estate-geographic-targeting-orders-beyond-manhattan FinCEN recently expanded its Real Estate Geographic targeting orders beyond

Manhattan and Miami to identify natural persons behind shell companies used to pay for high end real estate in six major metropolitan areas.

[xl] The Institute for Intergovernmental Research (IIR) serves as the technical service provider for ongoing training, research, and analysis services to the SLATT Program through the support of grant awards received from the Bureau of Justice Assistance. IIR supports the SLATT Program by providing project coordination activities, training assessment, and meeting coordination. See the IIR/SLATT website for additional information; (https://www.iir.com/WhatWeDo/Criminal_Justice_Training/SLATT/)



Testimony of
Mr. Duncan DeVille
Global Head of Financial Crimes Compliance &
US BSA Officer

The Western Union Company

Submitted to the

United States House of Representatives
Financial Services Subcommittee on
Terrorism and Illicit Finance

"Managing Terrorism Financing Risk in Remittances and Money Transfers"

July 18, 2017

Introduction and Background

Good afternoon Chairman Pearce, Ranking Member Perlmutter, and members of the Subcommittee. My name is Duncan DeVille, and I am Global Head of Financial Crimes Compliance and US Bank Secrecy Act Officer for Western Union, based in our Colorado headquarters. Prior to joining Western Union in 2013, I headed the Office of Compliance and Enforcement at the Financial Crimes Enforcement Network (FinCEN) in the US Department of Treasury; before this I was with the consulting firm Booz Allen Hamilton, and prior to this an Assistant US Attorney in Los Angeles. In each position I worked on Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) matters. I am also an adjunct professor at Georgetown Law School. Thank you for the opportunity to be here today to discuss Western Union's efforts to detect and combat the use of money services businesses (MSBs) by terrorist organizations.

The Western Union Company is a global leader in innovative, cross-border and cross-currency money transmission services. Western Union moves money for better, enabling individuals and families to transfer money safely around the world in increasingly easier, faster ways. Western Union's worldwide network includes more than a half-million agent locations in over 200 countries and territories, as well as more than 100,000 ATMs and kiosks, with the ability to send money to billions of accounts. In addition to person-to-person money transfers and other primary services such as money orders and bill payment options, the company offers a full suite of payment solutions and cash management strategies for global companies, small businesses, charities, non-governmental organizations, and universities through Western Union Business Solutions. We also own two international banks. In 2016, across all products and platforms, Western Union averaged 31 transactions per second, and over 900 per second at peak times.

At Western Union, we strive to provide ease of transaction and convenience to our customers. As our customers move to digital platforms, we continue to connect with them through online applications and mobile services. This is a critical area of focus for the company. Over 50% of Western Union's digital transactions originate from a smart phone.

Commitment to Compliance, Critical Component of Western Union's Identity and Organizational Structure

For Western Union, a critical part of serving our customers is complying with regulatory requirements. Even though regulatory compliance costs money and inhibits our ability to drive down transaction costs for our customers, we do not view the two goals as conflicting, but as complementary. This is because we value our customers' confidence and trust, and we think that they in turn value dealing with a reputable company that conducts business in accordance with the spirit and letter of the law.

As a money transmitter, Western Union is subject to regulation and examination by 48 states, the District of Columbia, and multiple territories, as well as by the federal government and numerous financial regulators overseas. We are subject to the Bank

Secrecy Act (BSA), the USA PATRIOT Act, and sanctions laws administered by Treasury's Office of Foreign Assets Control (OFAC). We register with FinCEN and are subject to examination by the Consumer Financial Protection Bureau (CFPB). In addition to regulator examinations, each year Western Union's compliance program is reviewed by banking partners, audited internally and externally, and provides detailed license and registration information.

I am here today to talk about Western Union's anti-money laundering and counter-terrorist financing efforts, and how various programs under our compliance umbrella have changed over time. This evolution can be attributed to many factors including the changing nature of the threats posed by bad actors, the introduction of new products and delivery platforms, increased regulator expectations, and other key events that have presented opportunities for Western Union to grow as a company.

Earlier this year, Western Union entered into settlement agreements with the Department of Justice (DOJ), Federal Trade Commission, FinCEN and 51 state attorneys general to resolve previously disclosed investigations focused primarily on oversight of certain agents and whether our employees' actions in connection with the maintenance of our anti-fraud program and anti-money laundering controls failed to prevent misconduct by those agents and third parties. The conduct at issue mainly occurred from 2004 to 2012. As detailed in the deferred prosecution agreement, "Since at least September 2012, Western Union took remedial measures and implemented compliance enhancements to improve its anti-fraud and anti-money laundering programs." These remedial measures and compliance enhancements, many of which will be outlined in my testimony today and as acknowledged in the deferred prosecution agreement, reflect Western Union's "...ongoing commitment to enhance compliance policies and procedures." These efforts will be reviewed by an independent compliance auditor for three years.

Western Union's business model depends upon trust. We cannot build and maintain our business unless we create a safe global environment for the people, families, and businesses who use our services. To that end, Western Union has increased its overall compliance funding by more than 200 percent over the past five years, and now spends more than 200 million dollars annually on compliance. Approximately 2,400 full-time employees, over 20 percent of our workforce, are exclusively dedicated to compliance functions. We have added more employees with law enforcement, national security and regulatory expertise, strengthened consumer education and agent training, and bolstered technology-driven controls. I am proud to have been one of the people recruited with a specific background in this area, and we have added many other experts with similar experience. The cumulative impact of these changes has been enormous in terms of strengthening compliance safeguard capabilities at the company and ensuring that our workforce understands the top-down commitment Western Union is making to regulatory compliance.

In fact, Western Union today is a recognized leader in the fight against many types of illicit activity including fraud, human smuggling, sex trafficking, child

exploitation, transnational criminal organizations, gang activity, counterfeit goods, and narcotics. While Western Union has a global scope and our Compliance Department targets latent and emerging threats in a wide variety of areas, my testimony today will focus on terrorist finance and Western Union's work with US law enforcement to provide actionable, forward-looking intelligence analysis.

As a global company, in addition to following US laws and regulations including FinCEN guidance,Western Union has adopted AML/CFT standards established by the Financial Action Task Force (FATF) and the Wolfsberg Group of international financial institutions. In many cases we apply global standards and targeted risk mitigation that are more restrictive than FATF recommendations or those required by the countries in which we operate.

We have established an AML Risk Assessment Framework to detect, deter, prevent, and report illicit transactions with dedicated teams of employees who are responsible for risk assessment, risk modeling, and ongoing analysis. This framework requires a multifaceted approach to assessing and managing risk including but not limited to analysis such as:

- Consumer-level monitoring, investigation, and assessment
- Agent-level due diligence, monitoring, investigation, and assessment
- Product risk assessment
- Country and regional level risk assessments
- Emerging risk and strategic intelligence analysis
- Control testing, audit, and assessments

This framework establishes a process for Western Union to address its risk and implement appropriate controls.

Primary compliance risks for terrorist finance generally derive from two sources: our agent network and our customers. Accordingly, as a company we are particularly focused on these areas. In addition, our compliance program has specific components dedicated to identifying geographic and emerging risks in order to proactively identify and respond to latent threats before they become widespread.

In designing our compliance program, we have been cognizant that Western Union's retail money service business operates through company partnerships with our network of agent locations around the world. Agent relationships with Western Union are defined by how the agent operates its retail locations. Some agents act as program managers that oversee many sub-agents. Others are independent or have multiple retail locations within the same company. In addition to regional store chains, convenience stores, small businesses, and other retailers, in many cases banks and post offices act as Western Union agents. For the small businesses, revenue generated through offering Western Union products is very significant and we are proud to help spur job growth and contribute to the larger economy.

We have established a dedicated team specifically to conduct research on our agents prior to entering a relationship with them, upon renewal of contracts, and at other triggering events such as a change of ownership. Agent due diligence includes criminal background checks, screens against the US Treasury's Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons lists and other appropriate government sanctions lists. Agents are trained through initial and ongoing AML/CFT and consumer fraud modules that cover applicable laws and regulations as well as Western Union's own policies, and common criminal typologies that we want our agents to monitor. Western Union has also built and patented the Comprehensive Model to Prioritize Strategy (CMPS), a statistical-indexing model that combines and enhances various risk indices and is used to measure agent risk across many categories. Risk scores are determined by factors such as transaction volume, transaction corridors, fraud data, and suspicious activity reports (SAR) data. The CMPS model helps guide agent compliance visits and program reviews for AML/CFT and consumer fraud purposes.

To assess and manage risk posed by our customers, Western Union has developed patented systematic and automated controls to detect and prevent suspicious and illicit payments, including transaction thresholds at which additional information, identification or supporting documentation is required from the consumer. In some cases, telephone interviews are prompted so that the purpose of the transaction, nature of the relationship between sender and receiver, and source of funds for the transaction can be determined. Examples of transaction limit controls include single and aggregate transaction limits, corridor specific limits, and currency or foreign exchange limits. As a company, we have the proven ability to use data analytics in many areas and have leveraged this to track and/or stop transactions and ensure that those initiated outside of established parameters receive heightened due diligence. In addition to CMPS described above, Western Union holds 26 patents related to categorizing and identifying data patterns that allow us to make more informed decisions about agent and consumer oversight.

In addition to the traditional back-end automated transaction monitoring rules/algorithms that banks have which look for patterns on a weekly or monthly basis *post-transaction*, we have something unique: up-front monitoring (Real Time Risk Assessment [RTRA]) rules/algorithms that can be designed to stop transactions with indicia of crime before they go through.

While it is not the primary focus of today's hearing, I want to bring to the subcommittee's attention another key program Western Union has established to help detect scam-related fraud and protect consumers at the point-of-sale. Our Courtesy Callback Program places some high-risk transfers on hold pending an interview with the sender, and resulted in $300 million in customer refunds in 2016. This program has grown exponentially since its inception in 2006 and today covers over 300 transaction corridors and has a staff of nearly 200 people. I have listened to the recordings of some of these calls and customers can be quite irate, insisting that they are not fraud victims and demanding that their transactions go through. Nonetheless, if the evidence shows that they are in fact victims of fraud, we will not process the transactions.

Western Union also has a program specific to sanctions compliance where OFAC and other applicable government lists are uploaded daily so that a person whose name appears on these lists will be blocked from conducting transactions anywhere around the world.

Working with Law Enforcement to Combat Terror Finance, Western Union's Financial Intelligence Unit

Identification, reporting and mitigation of terrorist finance risk is a top priority for Western Union's Financial Intelligence Unit (FIU). Modeled after intelligence programs in the government and law enforcement community, our FIU is another part of our Compliance Department and helps inform strategic decision making. The FIU develops and maintains collaborative, trust-based relationships with key law enforcement and other government partners to ensure that intelligence and information necessary to combat terrorism and terrorist finance can flow to the right people at the right time. For example, within hours of recent European terrorist attacks our FIU's Rapid Response team provided actionable intelligence to law enforcement via confidential reports – both Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs). Providing this type of immediate insight into active investigations has in at least once case helped identify additional terrorists before they carried out more attacks.

Western Union recognizes and supports the bipartisan work of Subcommittee Vice Chairman Robert Pittenger (R-NC) and full Committee Ranking Member Maxine Waters (D-CA) and others to enhance safe harbor provisions for the sharing of SAR information. Of particular interest to Western Union is one day having the legal authority to share these reports with our own overseas subsidiaries. As the largest SAR/STR filer in the world, with nearly 200,000 filed in the US and an additional 200,000 filed abroad last year alone, Western Union is committed to maximizing the potential impact of these important reports. In fact, we have established a structured system that allows us to formally identify SARs that may be related to terrorism. We immediately share these reports with law enforcement so they can prioritize them at their discretion. The ultimate goal of our FIU is to "see around the corner", i.e., to proactively identify bad actors not otherwise visible from internal detection systems and external referrals, and to provide advance warning and risk mitigation options for potential threats.

Despite Western Union's cooperation with law enforcement and commitment of resources to combatting terror finance, the fact remains that identifying terrorists and facilitators is extremely difficult. There is no distinctive profile for a terrorist based solely on an individual's consumer activity, and we are not aware that any financial institution has yet been able to develop effective predictive analytical capacity to identify terrorists through their transactional activity. On the contrary, it is most often the case that the volume, frequency and other characteristics associated with terrorists' transactions are consistent with routine patterns the company sees for legitimate purposes such as humanitarian aid, charitable giving, and sending money to family and friends. This underscores the importance of identifying terrorist finance activity through collaborative public-private partnerships where information flows back and forth in real time. It also

underscores the importance of both the public and private sector looking beyond raw transaction data and combing other sources such as social media to paint a more complete picture of subjects that may be moving money for illicit purposes.

Key current areas of focus for Western Union's Financial Intelligence Unit include:

- Analysis of Turkey and Lebanon as transit areas for people and funds ultimately intended to support ISIS.

- Focus on potential ISIS "provinces" and/or affiliated groups such as those in Libya, Egypt, Tunisia, Philippines, Bangladesh and elsewhere.

- Continued analysis and adjustments to transactions controls and other risk mitigation measures in Iraq, Syria, Turkey, Libya, and Lebanon to ensure that we are appropriately managing risk while still serving the great humanitarian need in these challenging areas.

The deep, ongoing relationships Western Union has with law enforcement are a critical part of what we do. Terrorists and global criminal organizations threaten the individuals, families and businesses we serve. They also threaten our own agents and the foundation of our business. It is in our interest to keep our services out of the hands of those who would use them to do harm, and we remain committed to that effort. Western Union has proved to be a valuable and trusted government partner in protecting US national security, and we consider this to be a paramount responsibility and core aspect of our mission. We believe that we are helping, as evidenced by the recognition that we have received from law enforcement, in the form of dozens of thank you letters for our work; as well as formal, written recognition by regulators for SARs that have helped with critical cases. Our best strategy to successfully combat an evolving and increasing complex threat landscape is to do so together.

In conclusion, I want to recognize *The Money Remittances Improvement Act of 2014* signed into law during the 113th Congress with the help of many of the members here today. This legislation provided much-needed streamlining of the examination process for Western Union and other money transmitters, and freed up resources for the Treasury Department to focus on anti-money laundering and counter-terrorist financing efforts. I would also like to acknowledge the work of the Conference of State Bank Supervisors in aiding many of these streamlining efforts including joint examinations where appropriate. We will continue to work with members of the subcommittee on legislative efforts to combat the financing of terrorism and other illicit activities – and to help stop the many bad actors who operate today.

On behalf of Western Union, I thank the members of this subcommittee for having me today and for your work in this area. I would be happy to answer any questions you may have.

Statement for the Record
House Financial Services Committee - Subcommittee on Terrorism and Illicit Finance
Matthew Oppenheimer - Co-Founder & CEO, Remitly, Inc.
July 18, 2017

Good afternoon. My name is Matthew Oppenheimer and I am the Co-Founder and CEO of Remitly, an online remittance provider based in Seattle, Washington.

Remitly thanks the Subcommittee for the opportunity to explain why our country has a strong interest in making sure that remittance services are accessible, affordable, and secure. The availability of legitimate, licensed remittance services matters, both to the millions who rely on these services, but equally as a matter of national security.

I founded Remitly in 2011 after living in Kenya and seeing firsthand how difficult it was to transfer money across borders. Not only that, but it was expensive -- costing 8 to 10% of the total transfer just to send the funds. Looking at the technology that was becoming increasingly available to solve this problem, I knew there had to be a better way. And with over $600 billion in remittances sent around the world annually, I knew that this was a problem that affected a lot of people.

When I moved back, I started Remitly to make sending money abroad easier, faster, and more transparent. By replacing the traditional cash-based brick-and-mortar model with a purely digital one we sought to deliver a better, more affordable remittance service to customers.

By focusing on that vision, we have cut the cost of service by more than half -- from 8 to 10% to under 2% -- putting hard-earned money back into customers' pockets while delivering a better overall user experience. I am humbled to say that our team of over 400 employees around the world now helps customers in the United States, Canada, and the U.K. send $3 billion a year to recipients located in India, Mexico, Latin America, and the Philippines.

While our technology has improved remittances, the basic reasons for sending haven't changed. A recent survey of Remitly's customers revealed that nearly all are using our service to send money intended to pay for the basic needs of their family members - housing, food, water, electricity, medical care, and education - basic things we take for granted in the United States but can be unattainable for millions living abroad.

I see our customers as heroes. They sacrifice and save to provide a better life for their families. When they send, it's not just money, it's a lifeline - paying for their family's rent or their child's tuition.

The simple act of sending money abroad is how these unsung heroes deliver on their promises to loved ones. Consider Dalia Maldonado, a Remitly customer who lives and works in California. Dalia sends $250 a month from her real estate job to help pay for her father's knee surgery and a friend's leukemia treatment, in addition to providing regular assistance for staples like food and utilities. Hers is one of

countless stories of the immensely personal reasons people use remittances and the true reliance that people all over the world have on money sent from the United States.

Add all of these individual transfers up and you would find that remittances alone contribute nearly four times the funds provided by all foreign aid globally -- and more than all foreign direct investment if you exclude China.[1] In some nations, remittance inflows are a substantial component of the country's GDP.[2] Remittances provide a foundation of stability and opportunity not just for individual recipients, but for entire countries.

Beyond the human impact, when remittances are sent through modern, legitimate channels, they strengthen our national security. As a licensed money transmitter operating in all 50 States, we are registered with the Treasury Department's FINCEN Bureau and maintain a strict compliance program. We invest heavily to comply with anti-money laundering (AML) requirements, the Bank Secrecy Act, OFAC regulations, and other requirements, using the latest technology to detect suspicious activity and report it to the authorities.

Digital remittance providers like Remitly provide an additional layer of security against consumer fraud and money laundering risks by not accepting cash and by providing services directly to the end customer without relying upon the use of an agent network or other intermediary. As a digital-only provider, Remitly provides service to customers who currently have a bank account or a debit or credit card. This approach eliminates placement risk, the first stage in the money laundering process. In addition to being subject to our own Know Your Customer process that independently verifies the customer's identity with high confidence, our customers have also already been identified and verified by a U.S. bank or credit card issuer.

By offering services directly to customers, Remitly's product is built with consumer protection and AML, OFAC screening, and Bank Secrecy Act compliance features incorporated by design. This eliminates the vagaries and variance in compliance inherent in a distributed agent network, while also providing regulators with a direct end-to-end means to confirm the compliance of every transaction. Further, by accessing our service through digital means, the customer's device, location, and other digital metadata is available to us, providing additional data points that enable us to confirm or refute the customer's KYC information. The cumulative effect of these factors makes our digital approach a more secure and lower risk product compared to traditional remittance services.

This approach also turns our technology to protect our customers' identities and fight fraud into a powerful weapon to fight illegal activity. When our machine-learning systems or trained staff spot something suspicious, we say something; reporting this activity to authorities as required by our BSA obligations. This reporting provides law enforcement with a high resolution view into global money

---

[1] World Bank, Migration and Remittances Factbook 2016 at pg. 34. *See also* NPR, *Who Gives More To The Developing World: Aid Donors Or Migrant Workers?* (Apr. 13, 2016).

[2] *Id. See also* Meyer & Shera, Economia, *The Impact of Remittances on Economic Growth: An Econometric Model* (2016).

flows, an invaluable tool in the fight against illegal activity, money laundering, and terrorism. Licensed money transmitters like Remitly keep the money "in the light" by efficiently processing legitimate transactions, while detecting and deterring those that may not be.

By contrast, there exists an underground market of unlicensed remittances providers who do not comply with any of these obligations.[3] These informal networks operate without oversight and can be associated with black market activity. If policies are enacted that drive up the costs of legitimate remittance services or clear the field of healthy competition, money will be pushed towards these shadowy alternatives.

That is why Remitly is particularly troubled by recent proposals that would tax remittances to fund a Border Wall. This "2%" tax would actually increase the costs of sending money through legitimate channels dramatically, far more than might be initially expected. In our industry, the entire revenue opportunity for companies like ours is a combination of fee and foreign exchange revenue against the balance of the transaction. Historically, fees in our industry have been in the range of 8%, meaning that a 2% tax on the balance would effectively raise prices by 25% up to 10%. For Remitly, a company that charges less 2% of the amount sent, a 2% tax would more than double the prices experienced by consumers. A pricing increase of this magnitude would lead customers to abandon licensed, regulated service options like Remitly and engage in black market alternatives. By pushing this money underground we would be funding the very illicit activities that we want to stop.[4] It would be harmful to our customers and to border security to tax remittances to pay for a wall.

We submit that Congress, and this Committee in particular, should focus on reducing regulatory burdens and enhancing competition without creating additional risk. While there is no single policy solution to an issue as complex as AML and BSA reform, there are several areas of low hanging fruit that the Subcommittee should consider. We present the following suggestions:

- Congress should align the reporting thresholds for suspicious activity across banks and non-bank providers and update the reporting thresholds which have not been updated for over 15 years.[5] This would reduce regulatory burdens and focus both private sector and government resources on higher risk behavior and law enforcement priorities.

- Congress should update the so-called "Travel Rule" recordkeeping requirement for the first time since 1995. We suggest replacing the rule with an explicit safe harbor on customer data verification for transactions under $1,000 for bank account or card-funded transfers. Over $1,000

---

3 FinCEN, *Report on Informal Value Transfer Systems* (2002).

4 World Bank, Economist Blog, *Why Taxing Remittances is a Bad Idea* (March 24, 2017), available at the World Bank website. *See also* Catalina Amuedo-Dorantes, Cynthia Bansak, and Susan Pozo, "On the Remitting Patterns of Immigrants: Evidence from Mexican Survey Data," Economic Review, Federal Reserve Bank of Atlanta, vol. 90, no. 1 (2005); and Raúl Hernández-Coss, "The U.S.–Mexico Remittance Corridor: Lessons on Shifting from Informal to Formal Transfer Systems" (working paper, Series No. 47, Washington, D.C.: 2005).

5 31 U.S.C. § 5318(g); as transposed into 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System) (Federal Reserve); 12 CFR 353 (Federal Deposit Insurance Corporation)(FDIC); 12 CFR 748 (National Credit Union Administration)(NCUA); 12 CFR 21.11 and 12 CFR 163.180 (Office of the Comptroller of the Currency)(OCC); and 31 CFR 1020.320 (FinCEN).

threshold would require customer data collection and verification, an assumption in the risk-based approach that should be made more explicit. This would streamline low risk transactions that are already within the financial system, while simultaneously maintaining the flexibility of a risk-based approach that is the hallmark of our anti-money laundering regulations. This would also provide regulatory clarity regarding KYC obligations which are in line with global AML trends without being overly prescriptive.

- Congress should work with OFAC to build more complete and updated sanctions lists to reduce the significant operational burden created by false positive matches that cannot be dismissed due to incomplete or vague entries on name, location, and date of birth.

These improvements would focus private sector and law enforcement efforts on activities and transactions that pose greater risks. Given that the underlying assumptions of the above requirements have changed with the introduction of increasingly advanced technologies and recognizing the dollar thresholds have not changed in many years, it is time to revisit these assumptions and adjust our risk-based approach accordingly. Remitly is encouraged by the Subcommittee's focus on these important issues.

Making legitimate money transfers more accessible, affordable, and secure benefits consumers and strengthens national security. While innovation can solve part of this problem, a more comprehensive solution requires the attention of Congress. However, with sound policy and continued innovation, Remitly is confident that this goal is within reach.



OXFAM

Statement of Scott T. Paul, Humanitarian Policy Lead, Oxfam America

U.S. House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance
Hearing on: Managing Terrorism Financing Risk in Remittances and Money Transfers
July 18, 2017

Chairman Pearce, Ranking Member Perlmutter, Members of the Subcommittee:

I greatly appreciate the opportunity to testify before the Subcommittee on the critical and timely issue of managing terrorism risk in remittances and money transfers. I am testifying in my capacity as the Humanitarian Policy Lead for Oxfam America. As part of the global Oxfam confederation, we and our local partners work in more than 90 countries around the world to tackle the root causes of poverty and save lives in humanitarian crises. In order to be independent advocates for effective US foreign assistance and foreign policy, Oxfam America does not accept US government funding.

Oxfam first became concerned about the subject of today's hearing during the 2011-12 humanitarian emergency in Somalia. At the time, a large part of the country was experiencing a catastrophic famine that ultimately claimed the lives of approximately 258,000 people, most of them children under five years of age.[1] Oxfam was working with local partners to help Somalis, particularly women and children, access food, procure clean and safe water, and prevent disease. We also endeavored, as we do in each emergency, to raise the voices of the most vulnerable. In this instance, vulnerable Somalis told us that, more than any other operational or policy issue affecting them, the most important threat to their lives was the possibility of a disruption in remittance flows from the United States to Somalia. Oxfam took their concerns very seriously. With partner agencies, we subsequently published two reports on remittances to Somalia[2] and an additional study on the broader, global phenomenon of banks' exiting or limiting relationships with MTOs among other types of bank customers.[3]

---

[1] "Mortality among populations of southern and central Somalia affected by severe food insecurity and famine during 2010-2012." May, 2013; Food and Agriculture Organization and the Famine Early Warning Systems Network (FEWS NET), available online at http://www.fsnau.org/downloads/Somalia_Mortality_Estimates_Final_Report_8May2013_upload.pdf.

[2] See Orozco, Manuel and Yansura, Julia. "Keeping the Lifeline Open: Remittances and Markets in Somalia." July, 2013; Oxfam and Adeso, available at https://www.oxfamamerica.org/static/media/files/somalia-remittance-report-web.pdf; "Hanging By

Both financial exclusion and terrorism stand in the way of achieving Oxfam's vision of a world without poverty where all people are able to enjoy the full range of their human rights. In many places where we work, remittances represent a community's collective effort toward a better life, as well as its only firewall against destitution. We also see terrorist groups trap many of those same communities in poverty, insecurity, and horrific cycles of violence. In my travels through Somalia, Yemen, El Salvador, and Nigeria, I have seen firsthand the dreadful effects of indiscriminate violence and attacks on civilians. Any coherent, principled, prudent, and compassionate approach to the financial sector must aim to both enable *bona fide* remittances and reduce financing for extremist violence.

In my view, a strategy that aims to maximize remittances, keep them within the formal financial system, and curb illicit financial flows will achieve the twin aims of poverty alleviation and combating the financing of terrorism. To do this, remittance services must be accessible, affordable, and accountable – both to law enforcement authorities and to the families sending and receiving money.

Remittances Fight Poverty and Aid Humanitarian Response

In 2016, migrants sent $575 billion in remittances to their countries of origin, including $429 billion to developing countries.[4] In the world's poorest countries, remittances are particularly crucial. At the household level, remittances may be used to put children through school, pay rent, access medical treatments, or as start-up costs for a business. Remittances received by women and in woman-headed households have been shown to increase women's economic empowerment and investment in social capital.[5] At the national level, particularly in low-income countries, remittances are often drivers of the economy. Remittances accounted for more than 10 per cent of GDP in at least 28 countries and more than 20 per cent in at least nine of them.[6]

---

a Thread: The Ongoing Threat to Somalia's Remittance Lifeline." February, 2015; Oxfam, Adeso, & Global Center on Cooperative Security, available at https://www.oxfam.org/en/research/somalia-remittances-hanging-by-thread.

[3] Shetret, Liat and Durner, Tracey. "Understanding Bank De-Risking and Its Effects on Financial Inclusion." November, 2015; Oxfam & Global Center on Cooperative Security, available at https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/rr-bank-de-risking-181115-en_0.pdf.

[4] "Migration and Development Brief 27," April, 2017; World Bank, available at http://pubdocs.worldbank.org/en/992371492706371662/MigrationandDevelopmentBrief27.pdf.

[5] "Gender, Migration and Remittances," International Organization for Migration (IOM), available at https://www.iom.int/sites/default/files/about-iom/Gender-migration-remittances-infosheet.pdf.

[6] See "Migration and Remittances Data as of October 2015," World Bank, in "Report to the G20 on Actions Taken to Assess and Address the Decline in Correspondent Banking," note 1;

Remittances play a particularly crucial role in humanitarian emergencies, especially when state institutions and the private sector have collapsed. In Somalia and Yemen – two countries that face the threat of famine in the midst of complex humanitarian emergencies – remittances have been a relatively stable financial inflow. In Yemen, businesses have been decimated by fighting and a *de facto* blockade on the country's Red Sea ports, and public sector salaries on which a quarter of all Yemenis depend have not been paid for nearly a year.[7] In Somalia, government-provided social services are nearly nonexistent, and 26 years of civil war have undermined essentially all domestic industry other than subsistence farming, herding, and fishing, which themselves have been threatened by climate change and illegal, unreported and unregulated (IUU) fishing. In both countries – as well as for the surrounding region – money transfers from migrants abroad have been a stabilizing force. They have been more consistent than aid, investment, or social welfare programs. In Somalia, famine would have been declared long ago if not for money from the diaspora. At every phase of an emergency – the pre-crisis phase, the crisis phase, and the recovery phase – remittances help families and communities survive. They build resilience to crises, help communities weather the storm, and then help them build back better.[8]

Remittances are transmitted in a variety of ways – through banks, fintech enterprises, cash couriers, trust-based networks – known primarily in the United States by their Arabic name, *hawalas* – and non-bank money transfer operators (MTOs). MTOs are often the only remittance option for many poor migrants and their families who have no other point of access to the formal financial sector. MTOs themselves typically rely on banks to provide financial services, such as check collection, deposit services, payroll services, and most critically, wire transfers, as well as for their typically more robust anti-money laundering/combating the financing of terrorism (AML/CFT) information technology infrastructure. MTOs rely on cross-border wires in order to settle its accounts. If an MTO is unable to access this service in a country where it sends or receives money, it will be forced to identify another way to move money in or out of the jurisdiction, and otherwise may shut down its operations there.

Banks are Closing MTO Accounts

November, 2015; Financial Stability Board, available at http://www.fsb.org/wp-content/uploads/Correspondent-banking-report-to-G20-Summit.pdf.

[7] For more information on remittances and Yemen's financial sector in the context of its current humanitarian crisis, see Salisbury, Peter. "Bickering While Yemen Burns: Poverty, War, and Political Indifference." June, 2017; Arab Gulf States Institute in Washington, available at http://www.agsiw.org/wp-content/uploads/2017/06/Salisbury_Yemen_ONLINE.pdf.

[8] Savage, Kevin and Harvey, Paul. "Remittances during crises: implications for humanitarian response." May, 2007; Overseas Development Institute, available at https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/317.pdf.

Unfortunately, MTOs are one of a number of types of customers losing access to banking services, both in the United States and globally. A 2015 World Bank study that interviewed representatives of governments, MTOs, and banks in G20 countries reported that 46 per cent of MTO respondents had experienced bank account closures.[9] 28 per cent reported that they could no longer access banking services, with a staggering 45 per cent reporting that some of their agents were unable to use banks.[10] Neither banks nor MTOs interviewed for the study cited money laundering or terrorist financing-related violations or sanctions as one of the top five reasons for account closures. In short, MTOs are losing their bank accounts despite being viewed as law-abiding customers.

MTOs are not alone. MTOs are just one of a number of segments of the banking customer base losing financial services without regard to their AML/CFT compliance records. Other segments of the customer base include nonprofit organizations, respondent banks, foreign embassies and diplomatic missions, fintech enterprises, payday lenders, and other merchant categories viewed as high-risk.[11] The most widely used term for these practices is "bank de-risking," which former U.S. Under Secretary of the Treasury Adam Szubin defined as, "instances in which a financial institution seeks to avoid perceived regulatory risk by indiscriminately terminating, restricting, or denying services to broad classes of clients, without case-by-case analysis or consideration of mitigation options."[12] I prefer not to use this term, for two reasons. First, the term "de-risking" masks the fact that pushing law abiding customers out of the formal financial system actually increases, rather than decreases, money laundering/terrorist financing (ML/TF) risk. Second, "de-risking," as defined by Mr. Szubin and others, is concerned only with the indiscriminate denial of services to broad classes of clients. We should be equally concerned when any financial flow is forced to the margins of formal banking system, even if it is the result of careful, case-by-case analysis by each bank. Instead, I will discuss these practices as a decline in access to financial services.

All of the customer types experiencing this decline in access have a trait in common: they are all viewed widely in the financial sector as inherently "high-risk." It is important to note in this context that the level of risk associated with a customer does not describe the likelihood that

---

[9] "Report on the G20 Survey on De-Risking Activities in the Remittance Market." October, 2015; World Bank, available at http://documents.worldbank.org/curated/en/679881467993185572/pdf/101071-WP-PUBLIC-GPFI-DWG-Remittances-De-risking-Report-2015-Final-2.pdf.

[10] *Ibid.*

[11] Shetret and Durner.

[12] "Remarks by Acting Under Secretary Adam Szubin at the ABA/ABA Money Laundering Enforcement Conference," November, 2015, available at https://www.treasury.gov/press-center/press-releases/Pages/jl0275.aspx.

the customer will violate the law. Rather, it connotes the likelihood of the customer's being exploited for the purposes of terrorist financing, money laundering, or other financial crimes. Even the most stringent AML/CFT controls may not save a customer from being perceived or rated as high-risk, depending on the nature of its business, the jurisdictions in which it operates, or other factors.

The decline in financial access for customers perceived as high-risk appears to stem from the less tolerant political environment in which banks have operated following the 9/11 terrorist attacks and the 2008 financial crisis. We see this in number of ways, including:

- High fines for Bank Secrecy Act (BSA) noncompliance, particularly related to AML/CFT failings;
- Reputational risk for association with AML/CFT failings;
- Higher capital requirements and liquidity thresholds;
- Compliance costs related to BSA compliance;
- Shift from corporate to individual liability, including criminal liability;
- Risk of private civil litigation related to AML/CFT failings; and
- Pressure from bank examiners related to the maintenance of high-risk accounts, particularly in the wake of the 2008 financial crisis.

These factors have combined to dramatically reduce banks' risk appetites.[13] Consequently, banks are deciding that it is easier and more profitable to avoid any risk associated with customers like MTOs than to manage that risk.

There is little agreement over the relative importance of each of these factors, but from my experience and conversations with bank representatives, banks of different sizes have different rationales. Large banks tend to be more concerned with reputational risk, but at the same time more willing to maintain relationships with large MTOs. The UK legal dispute between Barclays Bank and Dahabshiil, a Somali MTO, provides fascinating insight into the decision-making

[13] See Shetret and Durner. See also "Unintended Consequences of Anti-Money Laundering Policies for Poor Countries," November, 2015; Center for Global Development, available at https://www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf.

process on account retention of one large bank. The judgment publishes the "Minimum Standards" used by Barclays for MTOs customers, which include a minimum revenue requirement and a high net tangible assets requirement.[14] In other words, Barclays had decided that no small MTO could be account-worthy, no matter how strong its AML/CFT compliance program.

On the other hand, small banks appear to withdraw accounts immediately following examinations. On occasion, banks have told me that examiners explicitly discourage banking MTO customers. More commonly, I hear examiners appropriately asking to see details and asking probing questions about MTO accounts at the beginning of examinations, which simply makes examiners nervous about maintaining these accounts. It is possible that many small banks simply do not have the capacity to conduct effective due diligence on complex MTO customers, but the likely alternative – pushing the compliant MTO and its remittance flows out of the banking sector altogether – seems much worse.

Pressures on Correspondent Banking Are Compounding and Globalizing the Challenges to MTO Financial Access

As I mentioned earlier, correspondent banks are one of the types of customers viewed as high-risk that are experiencing rapid account closures.[15] Foreign banks in particular rely on correspondent banking to access the US financial system and currency. For many, losing the ability to conduct transactions in US dollars is a death sentence.

Like MTOs, correspondent banks have been targeted as vulnerable to money laundering and terrorist financing (ML/TF) abuse.[16] And as with MTOs, banks are deciding that the costs and consequences of managing these interbank relationships outweigh the benefits (one representative of a large bank told me that the cost of onboarding a new respondent customer exceeded $60,000). Like MTOs, however, not all correspondent bank accounts are equal when it comes to account maintenance and retention. Large banks with lower risk profiles are viewed as more attractive customers than small banks with higher risk profiles. In 2015, the World Bank

---

[14] Dahabshiil Transfer Services Ltd vs. Barclays Bank Plc, judgment of Henderson, J. [2013] EWHC 3379 (Ch), Available at http://www.bailii.org/ew/cases/EWHC/Ch/2013/3379.html.

[15] Correspondent banks provide services for and on behalf of other banks, often to provide access to different jurisdictions. Those services include foreign exchange, wire transfers, business transactions, and settlement of accounts.

[16] See, e.g., "Money Laundering: A Banker's Guide to Avoiding Problems," December, 2002; Office of the Comptroller of the Currency (OCC), available at https://www.occ.gov/topics/bank-operations/financial-crime/money-laundering/money-laundering-2002.pdf.

concluded that roughly half of the emerging market and developing economy jurisdictions surveyed have experienced a decline in correspondent banking systems.[17]

For customers that depend on banking services in both wealthy and developing countries alike – including MTOs and charities such as Oxfam – this decline compounds the financial access problem in two ways. First, fewer interbank connections means more difficulty routing cross-border transactions, particularly to high-risk jurisdictions. Second, banks are desperate to make themselves more attractive customers for larger correspondent banks. This is especially true for foreign banks looking to maintain correspondent relationships with US financial institutions, which are insisting that their respondent banks reduce their risk profiles. Cutting MTO accounts, appears to be an easy way to do that, at least superficially.

The impacts of MTO account closures on remittances are unclear

It is certain that MTOs are experiencing bank account closures at an alarming rate. What is less clear is what effect this is having on actual remittance flows – the extent to which they are declining or moving outside of the formal financial system.

The evidence is mixed. Here's what we do know:

- An investigation into MTO bank account closures in Australia showed that the account closures had forced a number of MTOs to go out of business, but also showed that overall financial outflows from Australia remained constant.[18]

- Global remittances declined in 2016 from an all-time high of 2015, the first decline since the 2008 financial crisis, despite predictions that they would continue to increase.[19]

- In a number of instances, governments have raised concern at the highest levels about the impacts of bank account closures on remittance flows, particularly in the Caribbean region.[20]

---

[17] "Report to the G20 on Actions Taken to Assess and Address the Decline in Correspondent Banking."
[18] "Bank De-Risking of Remittances Businesses," November, 2015; AUSTRAC, available at http://www.austrac.gov.au/bank-de-risking-remittance-businesses.
[19] "Migration and Development Brief 27."
[20] Torbati, Yeganeh. "Caribbean Countries Caught in U.S. Crackdown on Illicit Money." 12 July 2016; Reuters, available at http://www.reuters.com/investigates/special-report/usa-banking-caribbean/; The Hon. Audley Shaw CD, MP. Presentation at 2016 IMF/World Bank Annual Meetings, available at

- Even in the absence of more convincing evidence that remittance flows are declining or going underground, the World Bank MTO study shows that MTOs are coping with account closures by employing other MTOs' bank accounts, cash couriers, or personal bank accounts.[21] This means higher costs and less transparency in money flows.

Remittances to Somalia: a case for more aggressive intervention

As I mentioned at the beginning of my testimony, I first became aware of these problems following an outcry from our partners in Somalia during the last famine in 2011-12. Somalia presents a unique case:

- Somalia is one of the most remittance-dependent countries in the world, with money from the diaspora comprising roughly a third of its entire economy. At more than $1.3 billion annually, the flow of remittances to Somalia is greater than the humanitarian aid, development assistance, and foreign direct investment it receives – combined.[22]

- Most of this money helps people meet their most basic needs, such as food, shelter, school fees, and basic medical expenses.[23]

- Most international banks and MTOs that are well-known in the US are almost entirely absent from Somalia. The only realistic channel through which to send money to Somalia are a set of Somali-owned MTOs offering low fees and an impressive ability to deliver throughout the country.[24]

- With the internationally designated terrorist group al-Shabaab present throughout much of South and Central Somalia and only the most nascent oversight of the financial sector, Somalia is viewed as an extremely high-risk destination for cross-border transactions.

One Somali-American I interviewed two years ago told me: "Without the money we're sending them, I don't think the Somali nation would exist." Another confessed to me tearfully that the thought of not being able to send money to his sick mother for food and medicine made him consider going back to face drought and conflict. "I can't even eat thinking about it," he told me.

---

http://www.mof.gov.jm/downloads/speeches/presentations/2016_annual_meetings_small_states_form_speech.pdf.

[21] "Report on the G20 Survey on De-Risking Activities in the Remittance Market."

[22] Orozco and Yansura.

[23] *Ibid.*

[24] *Ibid.*

Many people have expressed a concern that they were being targeted by the U.S. government because of their nationality or religion.[25]

Somali MTOs operating in the United States are registered with the Financial Crimes Enforcement Network (FinCEN) and are regularly examined by state authorities and the Internal Revenue Service. I am not aware of any Somali MTO that has been subject to civil or criminal penalties. I am aware of a number of instances in which Somali MTOs have provided information that has been used in the prosecution of individuals accused of sending money to al Shabaab. I should note here that in Somali, these companies are known as *hawalas*, which simply means money transfer. In English, *hawala* is used to designate money value transfer systems as informal and unregulated. For that reason, Somali MTO professionals forcefully reject this label.

No large bank has agreed to a relationship with a Somali MTO in at least six years. In response to community pressure, one large bank publicly announced in 2014 that it was considering opening an account for the largest Somali MTO. This MTO told me that the bank requested two costly audits and then declined to provide an account.

Small banks, for one reason or another, have almost all closed their Somali MTO accounts over the past five years. In official communications, they simply said they had decided to exit the relationships without providing any reasons,[26] but Oxfam and the MTOs opened lines of communication with a number of them following the account closures. One community development bank said it was concerned about criminal liability. A few banks claimed that recent examinations demonstrated to them that they did not have the capacity to conduct due diligence over the accounts. The last bank serving many of the MTOs, a bank that holds itself out as a specialist bank for MTO and other money service business customers, felt unable to maintaining the accounts while operating under a Consent Agreement with the U.S. Office of the Comptroller of the Currency.

The effect of these account closures is difficult to ascertain without better evidence. One survey conducted by the Food Security, Nutrition, and Analysis Unit (FSNAU) of the World Food Programme found that in the period following Somali MTOs' last major bank account closure, 35 per cent of urban Somalis outside the capital of Mogadishu reported receiving less money than before.[27] It is difficult to draw other strong conclusions from the survey due to its methodology

---

[25] *Ibid.*

[26] *Ibid.*

[27] "Assessment of External Remittances in Selected Urban Areas and Among Displaced Populations Across Somalia," September, 2015; FSNAU, available at http://www.fsnau.org/downloads/FSNAU-Assessment-of-Remittance-Flows-in-Selected-Urban-Areas-of-Somalia-October-2015.pdf.

and coincidental timing with other disruptions, but in my opinion, it indicates a connection between bank account closures and a decline in life-saving income for many Somali households. The consultations I have done with communities in Somalia and in Somali diaspora communities in the United States support that conclusion.

Somalia's banking system, financial oversight, and mobile-based remittance systems are all developing, but it will take years before we know whether these will give rise to a reliable remittance system and a stable economy in Somalia. Today, as parts of Somalia teeter on the verge of famine and al-Shabaab continues to assert itself throughout South-Central Somalia, remittances from the United States to Somalia remain on the precipice of a serious disruption. With many Somali MTOs remaining unbanked, some have resorted to carrying cash abroad to settle accounts – a legal option that has the blessing of the Treasury Department, but one that puts people and funds in great jeopardy.[28] In 2017, I'm convinced we can come up with options preferable to suitcases full of cash when it comes to our national security and the Somali people's lifeline.

Our goal is a fully inclusive and transparent financial system

We're witnessing a market failure in the financial sector today. In a perfectly functioning market, some banks would be providing service to MTOs, correspondent banks, nonprofit organizations, and others that are associated with high risk and low revenue potential. Those banks would be conducting better due diligence and potentially charging higher fees for MTOs and be in regular dialogue with MTOs on improving their AML/CFT controls. The reduced profit margins and additional costs passed on to individuals sending money aren't ideal, but they're preferable to the alternative that we're watching unfold. Market, regulatory, and political incentives are pushing banks to drop MTOs altogether, especially small MTOs specializing in money transfers to high-risk jurisdictions. If these MTOs aren't banked, we're not only likely to see a decline in remittances, but also an increase in the share of remittances being transmitted though informal networks – where law enforcement officials, regulators, and money senders can't trace it. That means less money in the hands of people looking to escape poverty and more opportunity for designated terrorists and other financial criminals to transact business.

A better approach would be to affirmatively encourage access to financial services for all regulated MTOs, including those at the high-risk end of the market. Government should be the first mover. In that regard, I would like to offer a few recommendations to the Committee.

---

[28] Trindle, Jamila. "Money Keeps Moving Toward Somalia, Sometimes in Suitcases." 15 May 2015, *Foreign Policy*. Available at http://foreignpolicy.com/2015/05/15/money-keeps-moving-toward-somalia-sometimes-in-suitcases.

Recommendations

1. **Get more and better data**. The GAO is currently undertaking four interrelated studies related to this issue which should make an important contribution to our understanding of the topic. I would encourage the Committee to more regularly request information on remittance outflows from the United States and, to the extent practicable, to follow up on these information requests to determine the causes and consequences of any disruptions.
2. **Urge the Treasury and State Departments to increase technical assistance for improved financial controls in high-risk countries**. Both Treasury and State have initiated this process with the Government of Somalia. Similar processes should be replicated and supported where there is an interested government partner whose weak financial governance contributes to its perception by banks as a high-risk jurisdiction.
3. **Request input from government agencies and offices concerned with financial inclusion**. As concerns terrorist financing, Treasury's Office of Terrorist Financing and Financial Crime (TFFC) and the federal banking agencies tend to play the leading roles in policymaking. Officials in these agencies have done an incredible job in recent years reaching out to and soliciting input from interested parties over the past few years. Still, I believe that officials at the State Department, USAID, and officials at Treasury more focused on financial inclusion should have a stronger role in the policymaking process and informing public debate around these issues.
4. **When there is a strong public interest, support public-private partnerships to maintain money flows at the periphery of the banking system**. These could take many forms. As an example, Section 271 of the Countering Iran's Destabilizing Activities Act, currently under consideration in by the House of Representatives would require a feasibility study to determine whether the Treasury Department could assist private banks or credit unions wishing to facilitate remittances to Somalia. Another approach would be for the Federal Reserve Banks to utilize Fedwire to transmit funds on behalf of certain unbanked customers. I don't advocate these options in all cases, but in circumstances such as Somalia's remittance corridor, or for unbanked organizations delivering life-saving assistance in Syria, these options are worthy of consideration.

MORRISON | FOERSTER

Written Statement of
Bradley S. Lui
on behalf of The Money Services Round Table

Submitted to the

United States House of Representatives
Financial Services Subcommittee on
Terrorism and Illicit Finance

Hearing on Managing Terrorism Financing Risk in Remittances and Money Transfers

July 18, 2017

I am Bradley Lui, a Partner with the law firm of Morrison & Foerster LLP and counsel to The Money Services Round Table ("TMSRT"). On behalf of TMSRT, I am pleased to have the opportunity to submit these remarks for the record on the role of money transmitters in detecting and combatting money laundering and countering the financing of terrorism.

TMSRT was founded in 1988 as an information-sharing and advocacy group for the nation's leading non-bank money transmitters. Its current members are American Express Travel Related Services Company, Inc., MoneyGram Payment Systems, Inc., RIA Financial Services, Sigue Corporation, Viamericas Corporation, and Western Union Financial Services, Inc. These companies offer services including bill payments and funds transfers (domestic and international) through retail points of sale, the Internet, and mobile phones, as well as the sale and reloading of stored value products and other money transmission services. They are licensed in all states that have nonbank licensing laws currently in effect[1] —48 states plus the District of Columbia—and are Money Services Businesses ("MSBs") as defined in the regulations implementing the Bank Secrecy Act, 31 USC § 5311 *et seq.* and 31 C.F.R. Chapter X (collectively, the "BSA").

Since its founding, TMSRT has been active in the passage and implementation of more than 27 state licensing laws, and participates in the Treasury's Bank Secrecy Act Advisory Group. TMSRT comments on pertinent state and federal legislation and regulations involving safety and soundness and/or anti-money laundering/terrorist financing issues. TMSRT also for many years has worked closely with the Money Transmitters Regulators Association, the leading national organization of state non-bank money transmitter regulators, and the Conference of State Bank Supervisors. TMSRT has also participated with the Financial Action Task Force on international anti-money laundering standards.

Money Transmitter Services

Licensed money transmitters provide a diverse array of valuable services to consumers throughout the world. They provide a safe, reliable and affordable way to send money to family and friends, to pay bills and to obtain other financial services. In recent years, consumers have increasingly begun to rely on money transmitters for a diverse array of services including bill payment, online and app-based peer-to-peer transfers, domestic and international remittances, and stored value (i.e., prepaid) cards and other devices. In many cases, consumers have foregone or reduced the use of traditional banking services because of the ability of money transmitters to offer affordable, prompt and convenient services.

TMSRT members, like many other licensed money transmitters, primarily serve their customers through agents at physical locations throughout the United States, such as drugstores and convenience stores, large grocery chains and small corner markets, and many businesses in between. Many agents are small business owners that offer money

[1] With the exception of one member that has a license application pending in New York State.

transmission services as part of their overall business operations. These businesses, by operating as agent locations, benefit from the revenues generated directly from offering the services of the licensed money transmitter and also indirectly because of the general business traffic they can generate by offering the services.

TMSRT members, like many other licensed money transmitters, provide services valued by consumers and other businesses alike. It is important to note, however, that funds transfer activity that takes place through licensed money transmitters—such as those operated by TMSRT members—also provides significant benefits to law enforcement. As discussed further below, money transmitter licensees, as MSBs under the BSA, are required to implement comprehensive anti-money laundering programs that include substantial recordkeeping and reporting obligations. This information, as well as other steps taken by MSBs discussed below, facilitates law enforcement efforts to combat money laundering, crime, and the financing of terrorism.

The Current Regulatory Environment

The collective purposes of the regulatory regimes under which TMSRT members operate is twofold: (1) to develop, implement and maintain effective anti-money laundering programs; and (2) to ensure the safety and soundness of money transmitters to protect consumers. TMSRT members operate in a complex regulatory environment, with multiple regulators at the state and federal level.

As MSBs, non-bank money transmitters are subject to regulation under the BSA. MSBs are required to have, and all TMSRT members have in place, anti-money laundering programs reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[2] These so-called "BSA/AML" programs must be in writing, and must include what are known as the "four pillars":

(1) Policies, procedures, and controls reasonably designed to assure compliance with the requirements of the BSA, including its transaction monitoring, recordkeeping, and reporting requirements;
(2) A designated person to oversee the BSA/AML program and assure its compliance (i.e., a "compliance officer");
(3) Training of appropriate personnel on their responsibilities under the program; and
(4) Independent review of the program.[3]

The Financial Crimes Enforcement Network ("FinCEN") implements and interprets the BSA, and facilitates the reporting obligations of licensees under the BSA. Licensees, and all MSBs, are subject to examination by the Internal Revenue Service ("IRS") for BSA compliance pursuant to the regulations established by FinCEN. Many state money transmission licensing laws incorporate the requirements of the BSA by reference or

[2] 31 C.F.R. § 1022.210(a).
[3] *See id.* at § 1022.210(d)

otherwise impose obligations on licensees under state law with respect to aspects of BSA compliance, and state examinations (discussed further below) include assessments of BSA compliance. In addition, licensees are also subject to examination by the Consumer Financial Protection Bureau for compliance with the Remittance Transfer Rule, which imposes specific requirements including disclosures and error resolutions on international consumer remittances.[4]

In addition, money transmitters currently are required to be licensed in each of the individual states in which they do business (except Montana and South Carolina). Because TMSRT members have licenses and offer services to residents throughout the United States (both through physical in-state agent locations and through the Internet), they are subject to examinations by regulators in 48 different states and the District of Columbia. While there is some variance among state money transmission laws, each of the laws contains robust requirements to ensure safety and soundness of the licensees. The state regulatory framework for licensees typically provides safeguards including permissible investments, bonding, net worth, examinations, reporting protocols, and other mechanisms for oversight so that users of their services have reasonable assurance regarding the funds entrusted to the money transmitter.

To monitor and enforce compliance with licensing requirements, state banking departments conduct regular on-site examinations of money transmitter licensees to review their financial condition, monitor financial reserves, assess their funds transfer activities and, as noted above, examine for BSA and anti-money laundering compliance. These examinations are similar in scope and purpose to the examinations conducted at state-chartered banks though, as noted, money transmitters generally must be licensed in all states in which they do business, including through agent locations.

Simply put, money transmitters are very heavily regulated and closely scrutinized by multiple regulators at the state and federal level.

The Role of Money Transmitters in the Fight against Money Laundering

As part of their BSA/AML programs, MSBs are subject to significant transaction monitoring, recordkeeping and reporting obligations. These obligations include:

- Monitoring transactions and filing with FinCEN Suspicious Activity Reports ("SARs") if a transaction is conducted or attempted, at or through the money transmitter, which involves or aggregates funds or assets of at least $2,000 and the money transmitter knows, suspects or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part) is suspicious[5];

[4] Subpart B of Regulation E, at 12 CFR § 1005.30 *et seq.*
[5] *See* 31 C.F.R. § 1022.320

- Filing Currency Transaction Reports ("CTRs") for transactions involving more than $10,000 (inclusive of fees) in cash[6]; and

- Maintaining records of a customer's identity (including name, address, date of birth and Social Security number) for certain funds transfers of $3,000 or more, as well as beneficiary information, though we note that many industry participants, including TMSRT members, collect and verify customer identifying information for transactions at thresholds lower than $3,000.[7]

Like banks, money transmitters may be targeted by money launderers and other illicit actors who seek to exploit the world's financial system to facilitate criminal activities. TMSRT members have made it a priority to prevent their services from being used as conduits for illicit activity. Our members have spent many years and hundreds of millions of dollars in the aggregate on building and maintaining comprehensive AML programs to enable them to identify and report suspicious activity to FinCEN, and they continue to increase their spend on technology and personnel. Their efforts including building, implementing, and refining robust monitoring programs that include the use of sophisticated software systems to help identify and monitor high-risk customers and transactions and to block such transaction as appropriate.[8] TMSRT members have also heavily invested in the personnel necessary to run their compliance programs; for some TMSRT members more than 20% of their workforce is dedicated to compliance functions. And, as part of their programs, TMSRT members also educate and oversee their agent locations with respect to their BSA/AML obligations, including by conducting due diligence on potential agents, visiting agent locations (including unannounced "mystery shopping" visits), and reviewing and monitoring transactions.

Money transmitters' BSA/AML programs provide tremendous value to law enforcement. The terabytes of transaction data that MSBs collect, parse, and report facilitate law enforcement investigations and the fight against money laundering and terrorism financing. In addition, TMSRT members have also forged strong, direct relationships with law enforcement officials in the United States and throughout the world.

In short, compliance costs and regulatory overhead are significant for TMSRT members. Nevertheless, our members appreciate the value that their efforts provide to law

---

[6] *See id.* at § 1010.330.

[7] *See id.* at § 1010.410(e). As FinCEN recently noted, some money transmitters implement standards that go beyond BSA requirements. *See* GAO Report, *International Remittances: Money Laundering Risks and Views on Enhanced Customer Verification and Recordkeeping Requirements*, at p. 22 (GAO -16-65, January 2016) ("GAO Remittance Report").

[8] As part of their BSA/AML compliance programs, money transmitters have in place risk-based policies and procedures to comply with the sanctions programs administered by the Office of Foreign Asset Control of the United States Department of the Treasury ("OFAC"). The sanctions laws enforced by OFAC bar engaging in trade or financial transactions with certain specified countries and/or "specially designated nationals," and thus TMSRT members monitor transactions they process to ensure to the extent reasonably possible that transactions prohibited by OFAC sanctions occur.

enforcement and are proud to play a role in effort to detect and prevent financial crimes and illicit activities including money laundering and the financing of terrorism.

De-Risking and Similar Challenges

Although money transmitters face a very heavy regulatory burden, TMSRT members take their regulatory obligations very seriously. In particular, TMSRT members—like their customers and regulators—appreciate the importance of formal, well-regulated money transfer networks. Not only does the provision of funds transfer services through regulated channels enable law enforcement to have visibility into the movement of funds, but it also ensures that consumers are protected when they entrust their funds to an intermediary.

The industry, however, faces significant challenges due to a phenomenon known as "de-risking" as well as efforts to impose taxes on remittances. De-risking is generally understood to be the practice of banks eliminating, or significantly curtailing, their relationships with MSBs and related entities such as agents and foreign correspondent banks. Banks have done so apparently due to concerns about their own BSA/AML risks posed by such customer relationships. Indeed, the Office of the Comptroller of the Currency ("OCC") affirmed in its most recent risk perspective that businesses including money transmitters and foreign correspondent banks may be experiencing termination or restriction of banking relationships.[9] And, as FinCEN previously elaborated,

> [MSBs], including money transmitters important to the global flow of remittances, are losing access to banking services, which may in part be a result of concerns about regulatory scrutiny, the perceived risks presented by money services business accounts, and the costs and burdens associated with maintaining such accounts.[10]

De-risking directly impacts access to banking resources for large MSBs, including TMSRT members, as well as their agents and foreign correspondents. TMSRT also understands that smaller MSBs, as well as MSBs that seek to serve specific international corridors, have faced challenges with obtaining and maintaining banking relationships that enable them to provide funds transfer services. TMSRT also understands that these challenges are especially acute in border states, and that the inability to access banking resources is also affecting cross-border business activity.

De-risking is, therefore, a significant concern to the industry from a business perspective. It is also, however, a very significant problem from a law enforcement perspective. To the extent that de-risking makes it more difficult for money transmitters to provide their services to consumers, such individuals may turn to informal or underground

---

[9] *See* Office of the Comptroller of the Currency, *Semiannual Risk Perspective* at 19 (Spring 2017), *available at*: https://www.ots.treas.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2017.pdf ("OCC Risk Perspective").

[10] *FinCEN Statement on Providing Banking Services to Money Services Businesses* (Nov. 10, 2014), *available at*: https://www.fincen.gov/sites/default/files/news_release/20141110.pdf.

networks to transmit their money.[11] The OCC, for example, observed that the consequences of de-risking "may include potentially negative effects on financial inclusion internationally or the movement of transactions out of the regulated financial system."[12] FinCEN has similarly noted that MSBs play an "important role in a transparent financial system" in particular because they "often provide financial services to people less likely to use traditional banking services."[13] De-risking threatens this role. If transactions do not take place through regulated networks, there will be no visibility into this activity, and thus efforts by both money transmission licensees and law enforcement to detect and prevent money laundering and terrorist financing will be severely hampered. As the OCC put it, "***Such transactions then may not be appropriately monitored and reported for potential suspicious activity***."[14] (Emphasis added.)

In addition, while a discrete policy issue, recent legislative efforts to impose taxes on funds transfers at both the state and federal level would have the same types of negative impacts on the money transmission industry as de-risking, although on a broader scale. One prominent example of such an effort is H.R. 1813, which would impose a tax of 2% on each funds transmission transaction defined as a "remittance transfer" under the Electronic Funds Transfer Act.[15] TMSRT opposes this tax as well as similar efforts to impose remittance taxes in individual states. Money transmission taxes will discourage and distort economic activity and therefore harm American businesses and consumers. In addition, by increasing the cost of using regulated money transmission services, these taxes would discourage the use of affordable, reliable, and readily available regulated funds transfer services and would result in more individuals turning to informal networks.[16] As is the case with de-risking, if funds are driven out of regulated and monitored channels by remittance taxes, U.S. law

[11] For example, as the GAO has explained, one common type of such an informal transfer system is a "hawala." Under this system, "a customer hands cash to a person known as a 'hawaladar' and requests that an equivalent amount be delivered in local currency to a recipient in a different country. The hawaladar then contacts a hawaladar in the receiving country and asks that the funds be disbursed to the recipient." *See* GAO Remittance Report at p.10.

[12] OCC Risk Perspective at 19.

[13] *See id.* This point has been echoed by others, including the then-Deputy Director of FinCEN, Jamal El-Hindi, in a 2016 speech, and the former Comptroller of the Currency Thomas J. Curry, who noted in a recent speech that as a result of regulated entities losing their banking relationships "[t]ransactions that would have taken place legally and transparently may be driven underground." *Remarks by Thomas J. Curry, Comptroller of the Currency, Before the Institute of International Bankers* (March 7, 2016).

[14] OCC Risk Perspective at 19.

[15] 15 U.S.C. § 1693o-1.

[16] As the GAO observed in a recent study, imposing a tax or fine on money transmission activity "could result in a decrease in remittances in the regulated market and an increase in remittances through informal methods of money transfer." United States Government Accountability Office, *International Remittances: Actions Needed to Address Unreliable Official U.S. Estimate*, GAO-16-60 (February 2016). The GAO also noted that money transmission providers experienced a decrease in transaction volume after Oklahoma imposed a tax on certain types of remittances.

enforcement will be deprived of valuable insight into flows of money within and across America's borders.[17]

On behalf of TMSRT, I would like to thank Chairman Pearce, Ranking Member Perlmutter, and the members of the subcommittee for examining these issues and inviting TMSRT to provide these comments for the record. TMSRT would be happy to continue to be a resource for the subcommittee and its members.

dc-891017

[17] Though it is not relevant to state remittance tax proposals, we also note that while H.R. 1813 is intended to fund a border wall, the actual funds likely to be raised by the proposed tax would not come close to meeting the projected cost of any actual border wall.



September 7, 2017

Duncan Deville
Global Head of Financial Crimes Compliance
Western Union

Questions for the Record

"Managing Terrorism Financing Risk in Remittances and Money Transfers"

Questions submitted by Mr. Ellison and Mr. Vargas

1. To what extent are money transmitters (principal organization and its agents) experiencing account terminations by banks or reductions in services offered? For those that have their accounts terminated, to what extent are they able to find new accounts and what kinds of challenges do they face?

   Accounts terminations by banks can pose a serious risk to Money Service Businesses (MSBs), their agents, and the consumers they serve. As a principal organization, Western Union has not been immune to de-risking challenges particularly given the cross-border nature of our business. Regulation and risk tolerance will inevitably change, and we believe the response by the banking industry should be due diligence and assessment of individual BSA/AML programs for risk as opposed to wholesale elimination of entire categories of businesses. Furthermore, financial institutions that elect to meet the needs of underserved communities through MSBs should be recognized by examining agencies. As a global financial company, Western Union has relationships with over 200 banks from large settlement banks to correspondent banks that carry out financial transactions on behalf of the company. When Western Union encounters account terminations at the correspondent banking level it is usually on an industry basis, a geographical basis, or combination of industry and geographical issues. Generally speaking, account termination has been particularly difficult for Western Union agent locations, many of which are small businesses. This is especially true in underserved areas where banking options may be limited.

2. What are the factors driving account terminations? Are all money transmitters affected equally?

   Financial institutions are not required to provide Western Union with feedback or factors specific to account termination. This makes it difficult to understand what may or may

not have contributed to an account closure and if other MSBs are encountering account terminations for the same or different reasons. For the same reason, is also difficult to fully understand the frequency of account terminations.

3. To what extent is the ability of money transmitters to facilitate money transfers affected by correspondent banks restricting or terminating relations with respondent banks? If there are differences among how correspondent banks serve money transmitters, please explain.

   Most MSBs transmit funds and information through proprietary systems. This enables many money transmitters to deliver funds faster and more efficiently than the traditional banking system. In many cases, MSBs use correspondent banks help enable back end settlement. As described above, when Western Union encounters account terminations at the correspondent banking level it is usually on an industry basis, a geographical basis, or combination of industry and geographical factors. In the case of Western Union's business, for example, we have encountered such issues in the Caribbean and North Africa. Due to the restriction of information that is given when a correspondent bank terminates a relationship with a respondent bank, it is difficult to discern how correspondent banks may serve various money transmitters differently.

4. Does the technology and expertise exist for money transmitters to build effective BSA/AML compliance programs that would allow them to manage the risk associated with terrorist financing? Please discuss. Can smaller money transmitters build effective programs?

   Western Union believes technology and expertise are vital components to building BSA/AML compliance programs. While some smaller MSBs may have limited products serving a limited number of areas, building an effective BSA/AML program inevitably takes a substantial amount of time, money and expertise. MSBs that offer simple and limited purpose products will have to make compliance investments, but for those MSBs operating in more complex cross-border environments investments will be more significant. These investments are ongoing as regulatory and business environments are in a constant state of evolution.

   As discussed in my written testimony, over the past five years Western Union's compliance program has grown significantly in terms of funding, workforce, and targeted decision making. Regarding expertise to manage risk associated with terrorist financing, the company has made a concentrated effort to add employees with strong law enforcement, national security and regulatory backgrounds. Technology also plays a key role in how Western Union's compliance systems work and compliment human capital.

   Western Union holds 26 patents related to categorizing and identifying data patterns that allow the company to make more informed decisions about agent and consumer oversight. As a company, we have the proven ability to use data analytics in many areas and have leveraged this to track and/or stop transactions and ensure that those initiated outside of established parameters receive heightened due diligence.

Western Union has also built and patented the Comprehensive Model to Prioritize Strategy (CMPS), a statistical-indexing model that combines and enhances various risk indices and is used to measure agent risk across many categories. Risk scores are determined by factors such as transaction volume, transaction corridors, fraud data, and suspicious activity reports (SAR) data. The CMPS model helps guide agent compliance visits and program reviews for AML/CFT and consumer fraud purposes.

5. To what extent do current BSA/AML regulations and guidance as well as the implementation and enforcement of the regulations and guidance for both banks and money transmitters promote the effective management of associated terrorist financing risks?

As a money transmitter, Western Union is subject to regulation and examination by 48 states, the District of Columbia, and multiple territories, as well as by the federal government and numerous financial regulators overseas. Western Union is subject to the Bank Secrecy Act (BSA), the USA PATRIOT Act, and sanctions laws administered by Treasury's Office of Foreign Assets Control (OFAC). Western Union registers with FinCEN and is subject to examination by the Consumer Financial Protection Bureau (CFPB). In addition to regulator examinations, each year Western Union's compliance program is reviewed by banking partners, audited internally and externally, and provides detailed license and registration information.

Effectively managing terrorist financing risk is a shared goal of Western Union, Western Union's regulators, and the law enforcement community. Clear, concise guidance coupled with communication efforts by both parties and a mechanism for covered entities to receive feedback during the implementation phase allows market participants to best understand regulatory expectations and comply. MSB specific regulation would also be helpful. Oftentimes MSBs are lumped in with all types financial institutions without the uniqueness of a different business model being taken into consideration or MSBs are dependent on deriving regulatory expectations based on guidance written for banks. We have seen regulators use standards set in the OCC model validation process or regarding account based transaction monitoring to apply to non-account based person-to-person transactions.

Western Union supports the idea of ensuring there is a level playing field among money transmitters which is an important part of creating a fair marketplace that protects consumers and meets regulatory requirements. With over 26,000 registered MSBs, it is a very fragmented marketplace. To create a level playing field that truly protects consumers, enforcement of laws and regulations should be applied equally across market participants.

6. What challenges exist in trying to balance the need to meet BSA/AML compliance requirements while recognizing the needs of individuals, charities, and businesses to transmit funds to high risk areas? How can these be overcome?

Western Union moves money for better, enabling individuals and families to transfer money safely around the world in increasingly easier, faster ways. As described in your question, Western Union operates in many challenging areas of the world where the company partners with many non-governmental organizations (NGOs) to deliver humanitarian assistance.

Challenges do exist as, despite Western Union's cooperation with law enforcement and commitment of resources to combatting terror finance, the fact remains that identifying terrorists and facilitators is extremely difficult. There is no distinctive profile for a terrorist based solely on an individual's consumer activity, and we are not aware that any financial institution has yet been able to develop effective predictive analytical capacity to identify terrorists through their transactional activity. On the contrary, it is most often the case that the volume, frequency and other characteristics associated with terrorists' transactions are consistent with routine patterns the company sees for legitimate purposes such as humanitarian aid, charitable giving, and sending money to family and friends.

Western Union helps address these challenges, in part, by supplementing traditional back-end automated transaction monitoring rules/algorithms that banks have with unique up-front monitoring (Real Time Risk Assessment [RTRA]) rules/algorithms that can be designed to stop transactions with indicia of crime before they go through. For example, in Haiti, Western Union partners with many NGOs including Haitian Education & Leadership Program (HELP), UNICEF, Mercy Corps, Save the Children, the Red Cross, and Partners in Health. In other parts of the world we work with Oxfam International and a long list of additional NGOs to address poverty and basic needs.

Western Union has implemented specific RTRA controls concerning inbound transactions of a certain threshold to Haiti that will be stopped before funds are sent if certain consumer identifying information is not adequately presented to the agent at the point of sale. In many cases, Western Union's RTRA rules and algorithms go above and beyond what is required by any law or regulation.

   a. For example, how can regulators ensure a balance between BSA/AML compliance and transparent financial flows between countries? Are there processes that could keep financial flows, especially remittances, from being driven to informal and less transparent means?

As discussed above, effectively managing terrorist financing risk is a shared goal of Western Union, Western Union's regulators, and the law enforcement community. Clear, concise guidance coupled with communication efforts by both parties and a mechanism for covered entities to receive feedback during the implementation phase allows market participants to best understand regulatory expectations and comply. Robust communication about how regulations work in practice and may impact consumers can

help strike the balance regarding effective AML regulations and preventing unintended consequences that could drive consumers to underground, less transparent markets. Western Union also supports the idea of ensuring there is a level playing field among money transmitters which is an important part of creating a fair marketplace that protects consumers and meets regulatory requirements. Having this type of level playing field among money transmitters could also be a positive first step in ensuring that the flow of remittances stays in the formal, regulated system. It is this kind of transparency that helps money transmitters and law enforcement develop relationships and work toward the shared goal of stopping terrorist finance.

One specific area that would promote transparency would be the adoption of FinCEN's longstanding proposal for financial institutions to report cross-border electronic funds transmissions at a certain threshold. Having this centralized government database could certainly provide the government with additional transparency.

b. Have you provided any input on this issue to federal agencies? Which agencies and what was the outcome?

Western Union routinely participates in the open comment process by which federal agencies develop and issues regulations as described in The Administrative Procedure Act. As the largest MSB, we want to serve as a resource to both regulators and lawmakers as various public policy issues are explored. We hope that many of the themes discussed at the subcommittee hearing will continue to develop.

7. Money transmitters are subject to regulation and supervision, including regular examinations, by state banking supervisors and also to examination by the IRS. To what extent is state/IRS supervision of money transmitters leveraged by banks when conducting risk assessments of money transmitters and by bank examiners when evaluating banks' risk assessments?

In most cases, examination results for MSBs, banks, and other financial institutions would be treated as confidential supervisory information and therefore unavailable to banks conducting due diligence and examiners. If confidential supervisory information were made available to financial institution examiners, all regulatory bodies should be able to share this information.

8. Do you have any knowledge of how much BSA/AML compliance cost is passed on to money transmitters, and how much of those costs get passed on to customers who send money abroad? What other effects has BSA/AML compliance had on the money transmitter industry?

While these figures are difficult to quantify there clearly is a cost to the government to regulate money transmitters, a cost to money transmitters to comply with government regulation, and as these costs impact Western Union's total operating budget, have some impact on the cost to consumers to use Western Union's system. At a very basic level,

BSA/AML compliance can be burdensome on MSBs and consumers, but communication between regulators and impacted entities can help streamline processes and keep systems and consumers safe while minimizing costs. In the case of Western Union, BSA/AML compliance has provided a framework that the company must work within to help combat terrorist financing and has allowed Western Union's compliance program the flexibility to evolve and go beyond regulatory requirements as warranted.

At the same time, BSA/AML compliance costs can also be viewed from a bank's perspective for having MSB account holders and the associated costs. This type of question may be best suited for the banking industry. In 2016, Western Union had over 30 in-person bank visits, and about 400 requests to provide information on the many levels of compliance it applies to its own customers.

9. Last year, the Conference of State Banking Supervisors and the Money Transmitter Regulators Association released a report, *The State of Money Services Business Regulation & Supervision*. It highlighted the coordinated enforcement and supervision of MSBs by state banking regulators. Below is a list of all the regulations that Money Services Businesses follow:

The State of Money Services Business Regulation & Supervision
Conference of State Banking Supervisors & Money Transmitter Regulators Association

BSA/AML compliance is a substantial portion of money transmitter exams. During an exam, state examiners review the following:

- Registration with FinCEN
- Agent Monitoring
- BSA/AML Risk Assessment
- Anti-Money Laundering Programs
- Currency Transaction Reporting
- Foreign Bank and Financial Accounts Reporting
- Suspicious Activity Reporting
- Purchase and Sale of Monetary Instruments Record Keeping
- Funds Transfers Record Keeping
- Voluntary Information Sharing
- Internal Controls
- Training
- Independent Review of BSA/AML Program
- Information Systems Adequacy
- Office of Foreign Assets Control Requirements
- Personal Information Safeguards
- Procedures for mitigating money laundering and terrorist financing from foreign agent or counterparty relationships
- International Transportation of Currency of Monetary Instruments Reporting

Shouldn't a bank or credit union be able to provide a checking account, safe deposit box, or wire transfer services to an MSB as long as that money transmitter is legally operational with appropriate compliance paperwork, etc.? If an MSB is legally operating, should a financial institution assume it is fine to serve them?

All banks and credit unions can provide the above services to MSBs; still, many choose not to. Financial institutions are not required to provide Western Union, or any other MSB, with feedback or factors specific to account termination. This makes it difficult to understand why financial institutions may choose not to serve an MSB. As described above, the MSB marketplace is highly fragmented. While Western Union is subject to a high level of scrutiny, clearer more robust examination of all market participants may give financial institutions additional ease as they evaluate partnering with an MSB. For example, the IRS has a limited number of examiners delegated to MSBs yet there are over 26,000 registered MSBs.

10. Please explain how a financial institution can assess legality and compliance of MSBs? Are they able to have access to state banking or IRS supervision information? If not, would it help them feel more comfortable providing services if they could?

We are aware that under the National Mortgage Licensing System, some state regulators allow MSBs to submit a Call Report to help facilitate the regulatory examination process. This was recently developed with the goal of enhancing and standardizing the information available to state regulators concerning the activities of MSB licensees on a quarterly basis. Still, in most cases, information resulting from regulatory examinations would be treated as confidential supervisory information and therefore unavailable to banks that may be conducting risk assessments. Additionally, other types of financial institutions regulatory examinations are also confidential supervisory information and therefore unavailable to third parties.

In 2016, Western Union had over 30 in-person bank visits, and about 400 requests to provide information on the many levels of compliance it applies to its own customers.

Western Union believes that clear guidance, perhaps jointly issued by the federal financial regulators, could help create the kind of consistency needed so lawful compliant businesses and the consumers they serve can effectively participate in the banking system. In particular, it would be helpful for such guidance to recognize that it is appropriate and acceptable, under a risk-based approach, for a bank to provide services to an MSB that itself has a sophisticated AML program that has been approved by its own regulators.

11. To what extent is the ability of money transmitters to facilitate money transfers affected by correspondent banks restricting or terminating relations with respondent banks?

The extent of MSB's ability to facilitate money transfers can absolutely be affected by correspondent banks restricting or terminating relations with a respondent bank. The extent of the impact is usually felt by MSBs on an industry basis, a regional basis, or

through a combination of industry and geographical factors. Due to the restriction of information that is given when a correspondent bank terminates a relationship with a respondent bank, it is difficult to discern the extent of this problem or how it may vary among market participants.

Remitly
Promises Delivered
1111 Third Avenue, Suite 2100
Seattle, WA 98101 USA

September 11, 2017

United States House of Representatives
Committee on Financial Services
Washington, DC 20515

Re: Responses to Questions for the Record
"Managing Terrorism Financing Risk in Remittances and Money Transfers, July 18, 2017

Dear Mr. Ellison, Mr. Vargas, and Members of the House Subcommittee on Terrorism and Illicit Finance:

Below please find responses to your questions posed to Remitly following our testimony before the Subcommittee on July 18, 2017. We have restated the question and presented our response in bold.

1. To what extent are money transmitters (principal organization and its agents) experiencing account terminations by banks or reductions in services offered? For those that have their accounts terminated, to what extent are they able to find new accounts and what kinds of challenges do they face?

While Remitly has not experienced a termination of its bank relationship as an operating entity, we are well aware of the challenges that money service businesses ("MSBs") experience in obtaining and maintaining reliable banking services. When Remitly began as a startup in 2012 one of its most significant initial challenges was to obtain the banking relationship necessary to deliver a remittance service. It required almost a year of solicitation, negotiation and on-site examination before a large national bank agreed to provide us the necessary banking services. In many ways, this exercise was as difficult as obtaining our initial State money transmitter licenses. Incidentally, Remitly now operates in jurisdictions around the world and we have found that our experience abroad in obtaining banking services is just as great in other countries as it is in the U.S.

2. What are the factors driving account terminations? Are all money transmitters affected equally?

Much of what we know on this topic is anecdotal but it appears the primary issue stems from regulatory scrutiny of banks that provide necessary services to MSB's like Remitly. Because MSBs are considered to be "high risk", regulators hold banks overly responsible for all activity of their MSB customers. The result is that banks avoid being in a relationship with MSB's that creates real compliance risk to the bank without the ability to exercise day to day control. Terminations are felt most acutely by licensed MSBs who self-disclose their intended operations and are therefore easily identified, while unlicensed MSBs -- entities with that present AML and terrorist financing risk -- operate within bank merchant portfolios until they are detected.

3. To what extent is the ability of money transmitters to facilitate money transfers affected by correspondent banks restricting or terminating relations with respondent banks? If there are differences among how correspondent banks serve money transmitters, please explain.

As an MSB operating within the jurisdictions that we currently serve we have not directly experienced this issue. However, as a general statement we believe that it is clear that the lack of available banking services restricts

the ability of new and innovative money transmitters to enter the industry. As a result, consumers pay a higher price for money transfers and have fewer competitive choices, especially when they want to send to "high risk" jurisdictions.

4. Does the technology and expertise exist for money transmitters to build effective BSA/AML compliance programs that would allow them to manage the risk associated with terrorist financing? Please discuss. Can smaller money transmitters build effective programs?

Yes, technology and vendors are available to smaller or emerging money transmitters to manage the risk of terrorist financing. We believe the most effective way to manage terrorist financing risk is perform robust KYC of our customer base and take full advantage of available OFAC and other sanctions lists to screen and identify terrorists and supporters of terrorism. For transfers to certain high risk areas, MSBs can also perform enhanced due diligence of customers. Finally, MSBs must work closely with their disbursement partners to ensure that appropriate KYC procedures are carried out at the point of payment receipt. These procedures are available to be implemented by all MSBs, regardless of their size.

5. To what extent do current BSA/AML regulations and guidance as well as the implementation and enforcement of the regulations and guidance for both banks and money transmitters promote the effective management of associated terrorist financing risks?

Regulatory guidance regarding what constitutes an "effective" anti-terrorist financing program is not as readily available as what generally exists for anti-money laundering programs. While BSA requirements and objectives are complementary to the efforts to detect and deter terrorist financing there are few specific references beyond OFAC screening and cautions about facilitating payments to charitable organizations.

6. What challenges exist in trying to balance the need to meet BSA/AML compliance requirements while recognizing the needs of individuals, charities, and businesses to transmit funds to high risk areas? How can these be overcome?

a. For example, how can regulators ensure a balance between BSA/AML compliance and transparent financial flows between countries? Are there processes that could keep financial flows, especially remittances, from being driven to informal and less transparent means?

It would be helpful if the federal and state bank regulatory agencies made a strong statement in support of the need to provide services to money service businesses, including money transmitters. The goal should be to encourage banks to assess MSB risk on a case by case basis, as opposed to making an across the board judgment about our industry.

b. Have you provided any input on this issue to federal agencies? Which agencies and what was the outcome?

The topic of de-risking and the relative scarcity of bank services to MSBs is discussed in nearly every industry meeting, including those involving regulators. When included, the state regulators usually comment that they have shared the concern with their federal counterparts and received assurance that banks are being encouraged not to treat the money transmitter industry as extraordinarily high risk. To date, we do not see evidence that this message has taken root among banking institutions.

7. Money transmitters are subject to regulation and supervision, including regular examinations, by state banking supervisors and also to examination by the IRS. To what extent is state/IRS supervision of money transmitters leveraged by banks when conducting risk assessments of money transmitters and by bank examiners when evaluating banks' risk assessments?

We do not believe that state agency reports of examination have been used by bank or bank examiners to assess the risk associated with any specific money transmitter. Typically, these reports are considered to be property of the issuing state regulatory agency and therefore cannot be shared with third parties.

8. Do you have any knowledge of how much BSA/AML compliance cost is passed on to money transmitters, and how much of those costs get passed on to customers who send money abroad? What other effects has BSA/AML compliance had on the money transmitter industry?

The cost of compliance in our industry is considerable. We estimate that an amount equal to several percentage points of total revenue is spent on complying with applicable state and federal requirements. As any compliance-related fine, infraction, or finding could potentially translate into a MSB losing its license or its access to banking services, these investments are not optional. As a result, these costs are necessarily passed on in the form of higher prices paid by customers. In addition to the financial costs, the compliance burden creates a negative customer service experience for those offering a regulated, compliant product, which in turn likely drives customers into informal money transfer alternatives which carry no such compliance obligations or associated costs.

9. Last year, the Conference of State Banking Supervisors and the Money Transmitter Regulators Association released a report, *The State of Money Services Business Regulation & Supervision*. It highlighted the coordinated enforcement and supervision of MSBs by state banking regulators. Below is a list of all the regulations that Money Services Businesses follow:

The State of Money Services Business Regulation & Supervision
Conference of State Banking Supervisors & Money Transmitter Regulators Association

BSA/AML compliance is a substantial portion of money transmitter exams. During an exam, state examiners review the following:

- Registration with FinCEN
- Agent Monitoring
- BSA/AML Risk Assessment
- Anti-Money Laundering Programs
- Currency Transaction Reporting
- Foreign Bank and Financial Accounts Reporting
- Suspicious Activity Reporting
- Purchase and Sale of Monetary Instruments Record Keeping
- Funds Transfers Record Keeping
- Voluntary Information Sharing
- Internal Controls
- Training
- Independent Review of BSA/AML Program

- Information Systems Adequacy
- Office of Foreign Assets Control Requirements
- Personal Information Safeguards
- Procedures for mitigating money laundering and terrorist financing from foreign agent or counterparty relationships
- International Transportation of Currency of Monetary Instruments Reporting

Shouldn't a bank or credit union be able to provide a checking account, safe deposit box, or wire transfer services to an MSB as long as that money transmitter is legally operational with appropriate compliance paperwork, etc.? If an MSB is legally operating, should a financial institution assume it is fine to serve them?

We generally agree. As an MSB we are regulated by 47 state agencies and the federal government. As a result we are required to operate in compliance with a multitude of regulations, especially those related to anti-money laundering and consumer protections. Accordingly, in some respects we are lower risk than many other industries. Realistically, we would simply encourage banks to complete appropriate due diligence and risk underwriting. Assuming it's an appropriate and complete effort, banking examiners should give deference to the bank's underwriting rather than second guess it based on a judgement or pre-existing prejudice about the perceived riskiness of the industry.

10. Please explain how a financial institution can assess legality and compliance of MSBs? Are they able to have access to state banking or IRS supervision information? If not, would it help them feel more comfortable providing services if they could?

Banks are capable of assessing the adequacy of an MSB's compliance program. In many respects they are familiar with the AML/TF risks of an MSB, given that they are subject to many of the same rules and regulations. Some of the information readily available to banks for their review are: 1) AML policy and procedures, 2) Independent Review reports, 3) copies of periodic reports sent to state agencies, and 4) custom reports with metrics regarding suspicious activity reports, payment exceptions, occurrence of state examinations and fraud. It would be more efficient if banks were able to rely upon the findings of State regulatory agencies or upon the fact that an MSB is licensed, leaving the assessment of legality and compliance to the applicable regulatory body.

11. To what extent is the ability of money transmitters to facilitate money transfers affected by correspondent banks restricting or terminating relations with respondent banks?

Again, given the nature of our business and our experience to date we are not sure how the difference between respondent and correspondent banks affects MBSs. However, we can state with certainty that the reluctance of banks to provide financial services to money transmitters is harmful to consumers. It creates a significant barrier to entry, limits innovation and raises costs that must passed to on customers.

* * *

Please feel free to reach out to Aaron Gregory, VP of Legal, with any additional questions or follow-up you may have.

Respectfully submitted,

Remitly, Inc.

Responses by Scott T. Paul, Humanitarian Policy Lead, Oxfam America, to Questions for the Record submitted by Mr. Ellison and Mr. Vargas

Questions:

1. To what extent are money transmitters (principal organization and its agents) experiencing account terminations by banks or reductions in services offered? For those that have their accounts terminated, to what extent are they able to find new accounts and what kinds of challenges do they face?

As I mentioned in my written testimony, MTOs are one of a number of types of customers losing access to banking services, both in the United States and globally. A 2015 World Bank study that interviewed representatives of governments, money transmitters, and banks in G20 countries reported that 46 per cent of money transmitter respondents had experienced bank account closures.[1] 28 per cent reported that they could no longer access banking services, with a staggering 45 per cent reporting that some of their agents were unable to use banks.[2]

In the United States, I am not aware of any study that has analyzed a statistically significant sample of money transmitters to determine the extent to which they are losing access to the financial services that banks provide. However, there is overwhelming anecdotal evidence that this is a serious problem. Somali-American money transmitters, with which I have had the most extensive contact on the subject, have almost entirely lost access to banking services. This has left them to use a combination of coping mechanisms, including sending large volumes of physical cash abroad, that are less secure, transparent, and affordable than wire transfers. Representatives of many other money transmitters have also told me that maintaining bank account access and wire services are some of the most significant operational challenges that they face.

2. What are the factors driving account terminations? Are all money transmitters affected equally?

The reasons behind account terminations are numerous, complex, interrelated, and vary depending on the type and size of the bank and the type and size of the money transmitter. In general, regulatory and market changes have resulted in a decline in banks' risk appetites and an increase in the perceived risk associated with money transmitters. Those regulatory and market changes include higher fines for Bank Secrecy Act noncompliance; higher capital requirements and liquidity thresholds; a shift from corporate to individual liability, including criminal liability; an increase in private civil litigation for anti-money laundering/countering the financing of terrorism (AML/CFT) failings; and increased pressure from bank examiners related to the maintenance of high-risk accounts, particularly in the wake of the 2008 financial crisis. These

---

[1] "Report on the G20 Survey on De-Risking Activities in the Remittance Market." October, 2015; World Bank, available at http://documents.worldbank.org/curated/en/679881467993185572/pdf/101071-WP-PUBLIC-GPFI-DWG-Remittances-De-risking-Report-2015-Final-2.pdf.

[2] *Ibid.*

factors have made banks more conscious of the legal and reputational consequences of their various business lines and, in some cases, have increased the costs of compliance.

The revenue potential of money transmitter accounts has not increased to keep pace with the rising costs and consequences of maintaining them. I have found that small money transmitters have a more difficult time maintaining and opening bank accounts than large money transmitters.

3. To what extent is the ability of money transmitters to facilitate money transfers affected by correspondent banks restricting or terminating relations with respondent banks? If there are differences among how correspondent banks serve money transmitters, please explain.

Correspondent banking is a critical enabler for remittance flows. The decline in correspondent banking, which has taken place for similar reasons as the decline in banking for money transmitters, hurts money transmitters in two ways. First, banks are under tremendous pressure to reduce their risk profiles in order to maintain their correspondent relationships. In some instances, they terminate the accounts of money transmitters in order to do this. Second, some countries' banks have lost or almost lost all of their correspondent accounts with banks in the U.S. This leaves money transmitters working in and serving those countries unable to settle remittances paid in US dollars and paid out in local currencies.

4. Does the technology and expertise exist for money transmitters to build effective BSA/AML compliance programs that would allow them to manage the risk associated with terrorist financing? Please discuss. Can smaller money transmitters build effective programs?

I am not enough of an expert in BSA/AML compliance mechanisms or technologies to offer an informed opinion on this issue.

5. To what extent do current BSA/AML regulations and guidance as well as the implementation and enforcement of the regulations and guidance for both banks and money transmitters promote the effective management of associated terrorist financing risks?

In general, BSA/AML regulations, guidance, and enforcement over the past fifteen years appear to have resulted in much greater investment by banks in compliance and money transmitters. This may have resulted in better risk management as concerns most high-profit or low-risk customers and transactions.

However, the rising costs and consequences of managing customers viewed as high risk has pushed banks to end relationships with those customers, and sometimes entire classes of customers and business lines viewed as high risk. This seems particularly true of large banks, which have the best capacity to invest in compliance and risk management mechanisms. The result appears to be less and worse management of risk when it comes to low-profit, high-risk customers and transactions.

6. What challenges exist in trying to balance the need to meet BSA/AML compliance requirements while recognizing the needs of individuals, charities, and businesses to transmit funds to high risk areas? How can these be overcome?

    a. For example, how can regulators ensure a balance between BSA/AML compliance and transparent financial flows between countries? Are there processes that could keep financial flows, especially remittances, from being driven to informal and less transparent means?

    b. Have you provided any input on this issue to federal agencies? Which agencies and what was the outcome?

I believe that there are a few steps that regulators could take to effectuate stronger risk management and better service for individuals, charities, and businesses looking to transmit funds to high-risk areas. I will emphasize two suggestions that my organization, along with a number of coalition partners, has made directly to the Treasury Department and federal banking agencies.

First, federal banking agencies should take steps to emphasize the importance of maintaining accounts and managing the risk associated with individuals, charities, and businesses transmitting funds to high-risk areas. Presently, the examination process recognizes only the negatives of banking these customers. On occasion, banks have told me that examiners explicitly discourage banking these types of customers, which are viewed as high-risk. More commonly, I hear examiners asking probing questions and seeking details about money transmitters accounts at the beginning of examinations. This is consistent with what the agencies view as best practice, but it understandably makes examiners nervous about maintaining these accounts. I would suggest that the bank examination manual be reviewed and revised. The revision should state that banks are not required to know their customer's customer and that not all money transmitters, charities, and foreign financial institutions are high-risk. Most importantly, it should emphasize that even for the accounts presenting the highest risk, risk management and account maintenance are preferable to risk avoidance and account termination.

A revision of the manual is currently underway. I have provided this input to federal banking agencies and the Treasury Department, which have taken it under advisement.

Second, in extraordinary cases when there is a strong public interest in maintaining financial flows that are being pushed out of the formal system, the Treasury Department should enter into public-private partnerships to keep those flows secure and transparent. This could take many forms, including a joint effort between FinCEN or another Treasury office and a private bank to manage critical accounts that banks believe would otherwise be unprofitable or unmanageable. Oxfam has advocated for such an initiative to be put in place for Somali-American money transmitters since 2014 and for Syrian-American charities since 2016, but the Treasury Department is not receptive to this suggestion.

7. Money transmitters are subject to regulation and supervision, including regular examinations, by state banking supervisors and also to examination by the IRS. To what extent is state/IRS supervision of money transmitters leveraged by banks when conducting risk assessments of money transmitters and by bank examiners when evaluating banks' risk assessments?

I do not have sufficient information to answer this question.

8. Do you have any knowledge of how much BSA/AML compliance cost is passed on to money transmitters, and how much of those costs get passed on to customers who send money abroad? What other effects has BSA/AML compliance had on the money transmitter industry?

I do not have any insight to offer on this question.

9. Last year, the Conference of State Banking Supervisors and the Money Transmitter Regulators Association released a report, *The State of Money Services Business Regulation & Supervision*. It highlighted the coordinated enforcement and supervision of MSBs by state banking regulators. Below is a list of all the regulations that Money Services Businesses follow:

The State of Money Services Business Regulation & Supervision
Conference of State Banking Supervisors & Money Transmitter Regulators Association

BSA/AML compliance is a substantial portion of money transmitter exams. During an exam, state examiners review the following:

- Registration with FinCEN
- Agent Monitoring
- BSA/AML Risk Assessment
- Anti-Money Laundering Programs
- Currency Transaction Reporting
- Foreign Bank and Financial Accounts Reporting
- Suspicious Activity Reporting
- Purchase and Sale of Monetary Instruments Record Keeping
- Funds Transfers Record Keeping
- Voluntary Information Sharing
- Internal Controls
- Training
- Independent Review of BSA/AML Program
- Information Systems Adequacy
- Office of Foreign Assets Control Requirements
- Personal Information Safeguards

- Procedures for mitigating money laundering and terrorist financing from foreign agent or counterparty relationships
- International Transportation of Currency of Monetary Instruments Reporting

> Shouldn't a bank or credit union be able to provide a checking account, safe deposit box, or wire transfer services to an MSB as long as that money transmitter is legally operational with appropriate compliance paperwork, etc.? If an MSB is legally operating, should a financial institution assume it is fine to serve them?

Banks should conduct their own review of an MSB's compliance systems and determine whether they have the capacity to manage their accounts. However, it is distressing to see many banks arrive at the conclusion, largely aided by public pronouncements by regulators over the past 15 years and communicated directly by bank examiners, that they should be wary of MSBs. At a minimum, passing the extensive examination that MSBs undergo at the state level should at a minimum create a presumption that an MSB is responsibly managing AML/CFT risk.

10. Please explain how a financial institution can assess legality and compliance of MSBs? Are they able to have access to state banking or IRS supervision information? If not, would it help them feel more comfortable providing services if they could?

I do not have sufficient information to answer this question. However, allowing banks to access information about an MSB collected during supervision and examination should give them more information about the MSB's business model and compliance practices, and enhance banks' confidence in their ability to manage the MSB account.

11. To what extent is the ability of money transmitters to facilitate money transfers affected by correspondent banks restricting or terminating relations with respondent banks?

As I mentioned in my written testimony, customers that depend on banking services in both wealthy and developing countries alike – including MTOs and charities such as Oxfam – are affected by the decline of correspondent banking in two ways. First, fewer interbank connections means more difficulty routing cross-border transactions, particularly to high-risk jurisdictions. Second, banks are desperate to make themselves more attractive customers for larger correspondent banks. This is especially true for foreign banks looking to maintain correspondent relationships with US financial institutions, which are insisting that their respondent banks reduce their risk profiles. Cutting MTO accounts, appears to be an easy way to do that, at least superficially.

In addition, in certain jurisdictions without any correspondent links to provide them access to the US financial system, the cost of remittances appears to be skyrocketing. More data is needed to determine the damage that the decline of correspondent banking is inflicting on families relying on remittances, but it appears to be substantial.

ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW
Suite 1020
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

The Honorable Mike Rogers
United States House of Representatives
2184 Rayburn HOB
Washington, DC 20515

May 1, 2017

Dear Congressman Rogers:

On behalf of the Electronic Transactions Association (ETA), I write to oppose H.R. 1813, which would amend the Electronic Fund Transfer Act (EFTA) to impose a 2 percent tax on remittance transfers to certain countries.

ETA opposes this proposed tax on remittance transfers, and therefore H.R.1813, for several reasons.

First, imposing a tax on remittance transfers will distort the marketplace and ultimately harm consumers and businesses by driving up the cost of doing business and limiting products and service offerings. The market should be consumer-driven, where the development of products and services is based upon demand from consumers. For example, the ability to remit money digitally has provided many benefits for users. Digital remittances can cost almost half of what traditional channels charge, and can be done easily with little to no friction for the parties in the process. Imposing a tax will negatively impact this market and limit the availability of these types of beneficial services for customers.

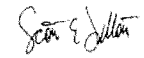
Second, imposing an additional tax on consumers and therefore increasing the cost of using a transfer service will drive traffic to alternative, likely unregulated channels. For example, Americans sent roughly $25 billion dollars to Mexico in 2015 – if an additional tax or fee was implemented for these transfers at the expense of the sender, the sender will be incentivized to find cheaper alternatives, such as illegal or black-market channels. Driving traffic to a black-market economy has important consequences for our nation's security, including law enforcement's ability to track money that is sent overseas and to ensure that money is not being used for illegal and dangerous activities such as: money-laundering, terrorist activities, and drug trafficking.

ETA urges you to reconsider the implications that H.R. 1813 would have for American businesses and consumers.

ETA is the leading international trade association for the payments industry, representing more than 500 companies that offer electronic transaction processing products and services. ETA's members include financial institutions, payment processors, and licensed money transmitters.

Please let me know if ETA can ever be of assistance on issues related to payments or financial services.

Respectfully,



Scott Talbott, Senior Vice President, Government Affairs
Electronic Transactions Association
Stalbott@electran.org

May 17, 2017

To: Members of the U.S. House of Representatives

Re: Opposition to H.R. 1813, the Border Wall Funding Act of 2017

On behalf of our member companies, many of which engage in the facilitation of remittance transfers, we write to express our concern with H.R. 1813, the Border Wall Funding Act of 2017. This legislation, which would subject remittance transfers from the U.S. to certain countries to a 2% user fee, is an ill-advised consumer tax on a legal and heavily regulated financial product used by millions of Americans.

As a matter of principle, taxes on consumer financial products and services are bad policy, no matter what the stated goal. The consumer tax in H.R. 1813 would increase the cost of remittance transfers, driving consumers out of regulated financial services and forcing these money flows underground.

When consumers utilize banks and other regulated financial institutions for remittance transfers – firms that have robust anti-money laundering programs – it provides law enforcement and financial regulators visibility into potentially illegal activities. Policies that encourage alternative channels reduce transparency and the ability to properly monitor transactions.

For these reasons, we urge opposition to H.R. 1813.

Sincerely,

American Bankers Association

Consumer Bankers Association

Electronic Transactions Association

Financial Services Roundtable

Independent Community Bankers of America

Money Services Business Association

Money Services Round Table

National Money Transmitters Association

MORRISON | FOERSTER

2000 PENNSYLVANIA AVE., NW
WASHINGTON, D.C.
20006-1888

TELEPHONE: 202.887.1500
FACSIMILE: 202.887.0763

WWW.MOFO.COM

MORRISON FOERSTER LLP
BEIJING, BERLIN, BRUSSELS, DENVER, HONG KONG, LONDON, LOS ANGELES, NEW YORK, NORTHERN VIRGINIA, PALO ALTO, SACRAMENTO, SAN DIEGO, SAN FRANCISCO, SHANGHAI, SINGAPORE, TOKYO, WASHINGTON, D.C.

May 2, 2017

Writer's Direct Contact
+1 (202) 887.8766
BLui@mofo.com

Via Overnight Delivery and FAX

The Honorable Mike Rogers
United States House of Representatives
2184 Rayburn HOB
Washington, DC 20515
FAX (202) 226-8485

Re: Remittance Transfer Tax (H.R. 1813)

Dear Congressman Rogers:

I write on behalf of The Money Services Round Table ("TMSRT")[1] to oppose H.R. 1813, which would impose a tax of 2% on each funds transmission transaction defined as a "remittance transfer" under the Electronic Funds Transfer Act ("EFTA"). As explained herein, TMSRT opposes this tax for a number of reasons. It will discourage and distort economic activity and therefore harm American businesses and consumers. In addition, by increasing the cost of using regulated channels for funds transfer services, H.R. 1813 will harm American national security by driving these transactions to informal or other unregulated and unmonitored channels, which will deprive U.S. law enforcement of valuable insight into flows of money across America's borders. Finally, while the ostensible purpose of H.R. 1813 is to fund a border wall, the actual funds likely to be raised by the proposed tax would not come close to meeting the projected cost of any actual border wall.

Background

As the General Accounting Office ("GAO") noted in a recent study[2] (the "GAO Study"), there are a number of ways that individuals can transfer funds abroad, including through cash payments to individuals and bank accounts, using prepaid cards, or transfers initiated online

[1] TMSRT is comprised of leading national non-bank money transmitters including RIA Financial Services, Sigue Corporation, Viamericas Corporation, Western Union Financial Services, Inc., and MoneyGram Payment Systems, Inc. These companies offer a variety of funds transmission services including bill payments and funds transfers (domestic and international) through retail points of sale, the internet, and mobile phones, as well as the sale and reloading of stored value products and other money transmission services. With the exception of one member company whose license application is pending in New York, each of these companies is licensed in all U.S. states that have non-bank licensing laws and is a Money Services Business as defined in the regulations implementing the Bank Secrecy Act, 31 USC § 5311 *et seq.* and 31 C.F.R. Chapter X (collectively, the "BSA").

and through mobile devices. These types of transactions are generally subject to federal oversight under the Bank Secrecy Act, and in many cases (including for money transmitters) to state regulation and oversight as well. Alternatively, as the GAO noted, individuals can use informal, unregulated channels to transfer money, including the use of "hand-carried cash, courier services, and agents known as hawalas."[3] Transactions through these channels are not subject to any oversight.[4]

H.R. 1813 would impose a tax of 2% on funds transfers that meet the definition of a "remittance transfer" and that are sent to the countries of Central America, South America, and the Caribbean Islands, and other island nations in the Atlantic Ocean. The EFTA defines a "remittance transfer" as an electronic transfer of funds initiated by a remittance transfer provider that is sent for personal, family, or household purposes from the United States to a "designated recipient," which is a person located in a foreign country identified by the sender of the funds as the authorized recipient of the funds.[5] And, a "remittance transfer provider" is defined as "any person or financial institution that provides remittance transfers for a consumer in the normal course of its business."[6]

Therefore, regardless of the means by which a consumer initiates a funds transfer to a recipient in any of these designated countries—whether online, at a brick-and-mortar retail location, at a bank branch, and so on—the transaction would be subject to the tax. Thus this tax will be imposed on a diverse array of consumer financial products and services, and on consumers that frequent a diverse array of businesses including large banks and credit unions, online payments companies, and traditional money transmission businesses that offer their services through physical locations such as grocery store chains and other major retailers as well as through smaller convenience stores and other local American businesses.

As discussed below, the breadth of this tax will have a detrimental impact on American businesses and consumers, and on law enforcement efforts to detect and counter money laundering and the financing of terrorism. And, perhaps most importantly, for all of these burdens on the economy and national security, the tax will likely raise far less revenue than H.R. 1813's proponents may be hoping for.

---

[2] United States Government Accountability Office, *International Remittances: Actions Needed to Address Unreliable Official U.S. Estimate*, GAO-16-60 (February 2016).
[3] *Id.* at 7.
[4] In addition, in light of recent innovations, it is possible that the use of virtual currency as a means to initiate remittances will become significantly more appealing. Currently, attempting to move money in this fashion is generally not competitive with the safe and efficient services offered by licensed money transmitters. But, if a tax were imposed on licensed money transmission services, the tax would likely make virtual currency services—which offer much less transparency and receive much less oversight—more economically appealing to U.S. consumers.
[5] *See* 15 U.S.C. § 1963o-1(g)(1), (2), (4).
[6] *Id.* at § 1963o-1(g)(3).

TMSRT therefore opposes H.R. 1813 and a tax on remittance transfers.

Regulated Money Transmission Activity Benefits Law Enforcement

A remittance tax will be detrimental to national security. Imposition of the proposed tax will increase the costs of using formal, licensed money transmission networks to transmit remittances. This, in turn, will create significant incentives for remitters to discontinue using these networks to transmit funds and instead turn to unregulated, informal networks for their money transmission needs.

Licensed money transmission networks are heavily regulated and monitored. In particular, money transmitter licensees must comply with detailed transaction recordkeeping and reporting requirements, and strict anti-terrorism and anti-money laundering laws and regulations under the BSA and under state laws as well. The records and reports that licensed money transmitters maintain enable regulators and law enforcement to have visibility into the money transmission transactions conducted by licensees, and enable licensees to work with law enforcement at all levels to help detect and prevent illegal or criminal activities from being facilitated by the use of money transmitters.

More specifically, the BSA requires that money transmitters register with the Financial Crimes Enforcement Network ("FinCEN"), have an effective anti-money laundering compliance program in place, and, among other things: (1) file Suspicious Activity Reports ("SARs") for certain types of transactions that are considered suspicious[7]; (2) file Currency Transaction Reports ("CTRs") for transactions involving more than $10,000 in cash[8]; and (3) maintain records of a customer's identity (including Social Security number) for certain funds transfers of $3,000 or more.[9] State money transmission laws also require licensed money transmitters to maintain transaction records including customer identifying information.

By taxing all remittance transfers to designated countries, H.R. 1813 is likely to discourage senders from using formal, regulated channels including licensed money transmitters.[10] Instead, as the GAO Study noted, imposing a tax or fine on international remittances "could result in a decrease in remittances in the regulated market and an increase in remittances through informal methods of money transfer."[11] Transactions driven to informal or underground networks will not be tracked, monitored, and regulated. Consequently, H.R. 1813 is likely to hamper law enforcement efforts to detect and prevent money laundering and terrorist financing. In addition, increasing the volume of transactions sent

[7] *See* 31 C.F.R. § 1022.320
[8] *See id.* at § 1010.330.
[9] *See id.* at § 1010.410(e).
[10] The GAO Study notes that money transmission providers experience a decrease in transaction volume after Oklahoma imposed a tax on certain types of remittances.
[11] *See GAO Study* at 10.

through informal networks is also likely to encourage the development and strengthening of such networks because it increases the attractiveness of these types of businesses.

Harm to Businesses

As noted above, and as indicated by the GAO Study, a remittance tax is likely to discourage senders from using regulated channels such as licensed money transmitters for their remittance transfer needs. Of course discouraging economic activity is generally harmful to any enterprise, but TMSRT members and the businesses they partner with to offer money transmission services will face particular challenges. This is because TMSRT members, and many other licensed money transmitters, primarily serve their customers through agents at physical locations throughout the United States, such as grocers, markets, etc. Many agents are small business owners that offer money transmission services as part of their overall business operations.

The tax will discourage consumers from using money transmission services. This, in turn, will lead to a loss of revenues to these small business agents both in terms of their money transmission business and their other businesses as overall consumer visits are reduced. In other words, this fee, like any other significant tax increase, will depress consumption and directly affect American businesses.

TMSRT members (as well as other remittance transfer providers) also will face significant costs in connection with collecting the tax. As the GAO Study noted, collecting and processing a remittance tax might require the development of new computer infrastructure and databases, staff training, and compliance. In addition, it will also require a lengthy process of development, testing, validation and deployment of software to ensure compliance with the tax, further impacting legitimate money transmitters.[12] TMSRT members would also likely face increased compliance and auditing costs related to the tax. None of these costs, however, will be borne by underground money transfer networks. This will further impact the ability of legitimate licensed money transmitters to compete with such underground networks.

Harm to American Consumers

Licensed money transmitters provide customers with a safe, reliable and affordable way to send money to family and friends, to pay bills and to obtain other financial services. And, the current disclosures and related requirements for transactions that covered by the EFTA, as remittance transfers, provide additional protections and transparency for consumers. The tax imposed by H.R. 1813 would likely discourage many individuals from using the services of licensed money transmitters like TMSRT members as well as of other financial

[12] The GAO Study noted that development efforts and related costs in connection with the remittance transfer disclosures initially required by the Dodd-Frank Act were up to $3 million for some money transmitters.

institutions. Consumers that choose alternative channels to transfer funds will lose these protections. And, for consumers who continue to use licensed money transmitters, the tax would significantly increase the cost of these services.

Finally, it is important to note that this this tax would be imposed on any sender of funds who chooses to transmit funds to countries selected by H.R. 1813. The tax would thus be paid using funds on which consumers have likely already paid income taxes.[13] These consumers will thus be forced to pay taxes on the same money twice—first for earning the money, and then for deciding what to do with it.

The Proposed Tax Would Not Raise a Material Amount of Funds to Pay for a Border Wall

If implemented, the tax would not be likely to raise a material amount of funds even in the best case. Currently, the higher end of estimates of *global* remittances from the United States to a recipient in any country in the world is in the range of $60 billion.[14] According to the GAO Study, of the top five countries that are recipients of remittance transfers from the United States, only one is on the list of specified countries in H.R. 1813 that would be subject to the tax.[15] Given that the majority of the dollar volume of remittance transfers from the United States would likely not be covered by H.R. 1813, it is unlikely that this tax would raise more than a very small fraction of the projected cost of the border wall, even if one were to make the unrealistic assumption that the tax would not result in substantial changes in consumer behavior. And, if more realistic assumptions are made, including the assumption that the GAO Study makes that an international remittance tax would likely result in the diversion of transfers to unregulated and unmonitored networks, as well as accounting for the increased costs for the cost of enforcement of money laundering laws, and the cost of administering the tax, the proposed tax is even less likely to raise significant sums for the border wall.[16] On the other hand, it will likely decrease the effectiveness of anti-money laundering efforts.

+++

[13] American citizens, other individuals lawfully present in America, and others who earn income in America generally pay income taxes and/or payroll taxes.

[14] For example, the most recent World Bank Remittance Outflows analysis, based on calculations using numbers reported by country authorities to the IMF Balance of Payments, estimated that $61.3 billion was remitted from the United States in 2015, *though this number includes employee compensation and not personal transfers only.*

[15] And, of the top 10 countries to which remittances are sent from the United States, only three are on the list of countries that would subject to the tax.

[16] H.R. 1813 would also provide that remittance transfer providers may retain 5% of the taxes collected from five years from enactment of the legislation to cover their administrative costs in connection with the fee, thus further decreasing the tax revenues that would be available to the government.

In short, H.R. 1813 would depress legitimate money transmission activity to the detriment of law enforcement and American businesses, would harm consumers, and would ultimately raise a negligible amount of the funds apparently necessary to pay for the construction of a border wall. TMSRT thus opposes H.R. 1813.

On behalf of TMSRT, I thank you for taking the time to consider these issues, and would be happy to discuss them further or address any questions you may have.

Sincerely,

Bradley S. Lui
Counsel to The Money Services Round Table



February 3, 2017

The Honorable Paul Battles
House Ways and Means Committee
Chairman, Subcommittee on Tax Reform
226 State Capitol
Atlanta, GA 30334

Re: Opposition to H.B. 66, legislation taxing certain money transmission transactions

Dear Chairman Battles:

On behalf of Western Union Financial Services Inc. (Western Union) and MoneyGram International, Inc. (MoneyGram), the top leaders in global payment services which provide consumers and businesses with fast, convenient and reliable ways to send money, we write today regarding H.B. 66. This bill, scheduled to be heard in your subcommittee, would impose a tax on certain money transmission transactions that would negatively impact Georgia businesses and residents. We have serious concerns about the unintended consequences of efforts to tax money transmission services in Georgia and appreciate the opportunity to comment on this legislation.

Impact on Georgia Consumers and Businesses

Western Union and MoneyGram facilitate money transfer services, from paying utility bills to sending money to family members and friends, for Georgia residents from all walks of life. The average transfer in Georgia is about $200 and nearly half of the transactions that originate in Georgia stay in the United States when the transaction is settled. Western Union and MoneyGram help to meet the financial needs of Georgia consumers through 3,900 agent locations, many of which are independent small businesses.

As you know, H.B. 66 would add a fee of $10 to any transmission under $500 and 2% of the principal amount of any transmission exceedingly $500. Not only would H.B. 66 make the money transfer process more expensive for Georgia residents, it would limit consumer choice. A new tax would place a burden on Western Union and MoneyGram agents who may choose to cease offering such services instead of subjecting themselves to a burdensome process to comply with the law. Western Union and MoneyGram partner with over 3,900 business locations in Georgia from convenience stores to mid-size grocery stores to community banks. Making money transmission services more expensive could significantly impact the number and frequency of customers who patronize these businesses which would disproportionately affect smaller businesses.

While H.B. 66 seeks to allow Georgia residents to recoup the proposed fee through income tax return filings, this bureaucratic approach would be onerous for those who meet the requirements

and leave other important segments of the population behind altogether. For example, our nation's military personnel stationed in Georgia may be non-residents and, therefore, ineligible to utilize a tax credit to recoup the fee.

Reporting Requirements and Important Work with Law Enforcement

All licensed money transmission providers are subject to strict oversight by state and federal authorities, and must comply with detailed record keeping and reporting requirements. These include strict anti-terrorism and anti-money laundering laws and regulations.

Western Union and MoneyGram have robust compliance and anti-money laundering efforts resulting in the ability to track transactions and provide real-time assistance to local, state, and federal law enforcement on a wide range of security issues including terrorist finance, drug trafficking, human trafficking, and fraud. Western Union's and MoneyGram's work in this regard has been presented to the Department of Treasury, the Federal Bureau of Investigation, and various foreign law enforcement agencies. One specific example is Western Union's and MoneyGram's work with the U.S. Department of Homeland Security's Blue Campaign. This initiative provides information, training, and outreach to raise public awareness about human trafficking.

If enacted, H.B. 66 would encourage illicit money to move underground and outside of reputable, regulated money transmitters. This would negatively impact law enforcement's ability to stay one step ahead of unscrupulous actors. Furthermore, when Oklahoma instituted a similarly structured tax in 2009, Western Union's and MoneyGram's transaction volumes significantly decreased, so, not only did law enforcement lose the visibility of these transactions, the state captured far less revenue than projected. The loss of visibility and revenue should be considered with respect to H.B. 66.

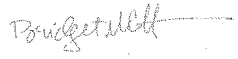
Based on our experience and in an effort to ensure Georgia consumers and small businesses are well served and protected from the unintended consequences outlined above, we respectfully express our opposition to the passage of H.B. 66.

Thank you for your time and attention to this matter. Western Union and MoneyGram welcome the opportunity to serve as a resource should you have questions or concerns about this issue.

Sincerely,



Timothy P. Daly
Western Union
Senior Vice President, Global Public Policy
720-332-4757



Bridget McGovern
MoneyGram
Vice President and Associate General Counsel, External Relations
202-372-5719

cc: The Honorable Jay Powell, Chairman, House Ways and Means Committee

○