LOW COST, HIGH IMPACT: COMBATING THE FINANCING OF LONE-WOLF AND SMALL-SCALE TERRORIST ATTACKS

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

SEPTEMBER 6, 2017

Printed for the use of the Committee on Financial Services

Serial No. 115–37

U.S. GOVERNMENT PUBLISHING OFFICE

29–538 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

WITNESSES

WEDNESDAY, SEPTEMBER 6, 2017

APPENDIX

LOW COST, HIGH IMPACT: COMBATING THE FINANCING OF LONE–WOLF AND SMALL–SCALE TERRORIST ATTACKS

Wednesday, September 6, 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 2:11 p.m., in room 2128, Rayburn House Office Building, Hon. Stevan Pearce [chairman of the subcommittee] presiding.

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

Ex officio present: Representative Waters.

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.

Today's hearing is entitled, "Low Cost, High Impact: Combating the Financing of Lone-Wolf and Small-Scale Terrorist Attacks."

I now recognize myself for 2 minutes to give an opening statement. I want to thank everyone for joining us today. Today's hearing will examine issues concerning small-scale acts of terrorism and the mechanism used to fund this type of terrorism. Although overall numbers remain low, one study has found that since the 1970s, lone-wolf attacks have grown almost 50 percent in the United States, and by over 400 percent in other Western countries.

Law enforcement as well has previously expressed concern that there is a greater likelihood of lone-wolf terrorism than large-scale attacks in the United States. One of the likely reasons is the relatively low cost for funding such an attack. Roughly 75 percent of extremist terrorist plots in Europe occurring between 1994 and 2013 have an average cost of just $10,000.

As we will hear today, whether an act of terrorism is directly funded by a known terrorist group or carried out by a sympathizer, the relatively low financial cost presents a hurdle to tracking the movement of funding through the financial system. Whether it be

through petty crime, working a temporary job, misappropriating government benefits, or engaging in scam transactions, terrorist organizations are utilizing new means to finance their operations, and are increasingly turning to newer financial technologies as well as less traditional transfer methods to move their funds.

As we have seen a change in tactics to lone-wolf terrorist acts, what is clear, however, is that the cooperation between policymakers, law enforcement, intelligence agencies, and financial institutions is necessary to detect, identify, and disrupt the funding of those actors.

In today's hearing, I hope our witnesses can discuss how we are currently combating terrorism and illicit finance including what tools and partnerships are working well in the effort to detect and disrupt lone-wolf and small-cell attacks. I would also appreciate any comments about deficiencies in our system that may impede our fight against terrorist finance.

Finally, I would welcome a discussion about the new and innovative technological solutions that are being developed to help tackle this problem. Inhibiting terrorist financing is not a new problem, but I hope that today we can shed some light on this issue and help inform this subcommittee on ways in which we can help disrupt that flow of money.

Again, I would like to thank our witnesses for being here today. I look forward to their expert testimony on this very important issue.

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

Mr. PERLMUTTER. Thank you, Mr. Chairman. And thank you to each of our witnesses for being here today.

This subcommittee takes on some difficult but important issues. In recent years, we have seen a rise in lone-actor terrorist attacks. While these terrorists are often inspired by extremist ideologies, they have little to no specific help from terrorist organizations, and the attacks are often self-financed, making them more difficult to uncover and prevent.

We have seen that lone-actor terrorists can be radicalized by foreign as well as domestic extremism. In the San Bernardino shooting, the Orlando nightclub attack, and the Boston Marathon bombing, the terrorists were inspired by foreign terrorist organizations.

However, in the Charleston church shooting, the car attack in Charlottesville, and the Planned Parenthood shooting in Colorado Springs, the terrorists were motivated by domestic extremism. Regardless of the source of radicalization, we must look for ways to prevent the financing of these kinds of activities. The low cost of these attacks can be challenging to our current antiterrorism financial protocols, but that doesn't make them any less important to stop.

I am eager to hear from our witnesses on how to recognize financial patterns in small-scale terrorism, how the government or financial institutions can better block extremist networks, and other ideas on how to disrupt lone-actor terrorism financing.

With that, I yield back, Mr. Chairman.

Chairman PEARCE. The gentleman's time has expired. The Chair now recognizes the gentleman from North Carolina, Mr. Pittenger, for 1 minute.

Mr. PITTENGER. Thank you, Mr. Chairman, and Ranking Member Perlmutter, for hosting today's hearing on combating lone-wolf terrorism and small-scale terrorist attacks.

I would also like to thank our distinguished panelists for lending their expertise to our subcommittee, particularly Mr. Reynolds. Thank you for your engagement in working with us and traveling to other countries to carry the important message of terrorism finance and how we can prevent the bad guys from getting the money.

Last Congress, I pursued legislation that would punish those who move to support lone-wolf terrorists. Furthermore, I will continue to pursue legislation that arms law enforcement and assists our partners abroad to mitigate the impact of potential terrorist attacks.

Lone-wolf and small-scale terrorist attacks continue to threaten the United States and the rest of the world. It is important that we continue to track illicit finance and illegal transactions by cooperating with the private sector to thwart these bad actors.

Mr. Chairman, I look forward to today's important hearing, and I yield back.

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

Mr. EMMER. Thank you, Mr. Chairman, for yielding, and thank you for holding this hearing today.

This subcommittee has held a number of important hearings during its inaugural session. And today's topic will hopefully help us better understand and address what seems to be a shift in the way acts of terror and violence are carried out.

While we will never forget the images of a large-scale attack like the one we witnessed almost 16 years ago against the World Trade Centers and the Pentagon, there is an increased and concerning pattern of smaller, less coordinated attacks around the globe.

Less than a month ago, a terrorist using a rented cargo van targeted and killed 14 people in a popular tourist location in Barcelona, Spain. Just over a year ago, on September 17, 2016, a suspected terrorist wielding kitchen knives wounded 10 people at a shopping mall in my district in Minnesota. The attacker was fortunately subdued by the heroic actions of another Minnesotan before any innocent lives were lost. However, areas of recreation and enjoyment must now be viewed as potential soft targets, where even the most common household items can be used as a weapon.

Our financial institutions have and will continue to play a critical role in the fight against terrorism. As food and water are essential to sustaining life, terror organizations need financing and resources to further their agenda of violence and hate. We must continue our efforts to deprive them of these essential resources, and we must constantly evolve as the threats facing our Nation so often do.

I look forward to hearing from our witnesses today and working with my colleagues on this subcommittee to find ways we can part-

ner with our financial services sector to better track and defeat small-dollar, small-scale acts of terror in the future.

Thank you, and I yield back the remaining balance of my time.

Chairman PEARCE. The gentleman yields back. The Chair now welcomes each one of our witnesses today.

To introduce Mr. Moreno, I would like to recognize Representative Lee Zeldin.

Mr. ZELDIN. Thank you, Mr. Chairman.

Mr. Joseph Moreno is a partner in the white collar defense and investigations group at the law firm of Cadwalader, Wickersham and Taft. Mr. Moreno rejoined Cadwalader after serving at the U.S. Department of Justice in the National Security Division's Counterterrorism Section where he investigated and prosecuted international money laundering, material support, structuring, and terrorist financing cases. He was also appointed a Special Assistant U.S. Attorney for the Eastern District of Virginia where he prosecuted a wide variety of criminal cases regarding the Classified Information Procedures Act, the Foreign Intelligence Surveillance Act, and the USA PATRIOT Act.

In 2014, Mr. Moreno was appointed as a consultant to the Federal Bureau of Investigation where he served on the staff of the FBI's 9/11 Review Commission.

Prior to joining his current firm, Mr. Moreno was an associate in the structured finance and white collar crime group at the law firm Skadden Arps. Mr. Moreno earned his undergraduate degree in political science cum laude from Stony Brook University in the greatest Congressional district in America, New York 1, and his JD cum laude from St. John's University School of Law.

A decorated combat veteran, Mr. Moreno is a Lieutenant Colonel in the U.S. Army Reserve. And I was honored to serve with Mr. Moreno, because we were in the same Army Reserve unit until recently.

Thank you, and I yield back.

Chairman PEARCE. Dr. Matthew Levitt, I understand that you have a hard stop at 4:00? Okay. So at that time, I will excuse you. The rest of you are good until 7:00?

Okay. Checking. That was a little grimace there instead of—

Okay. Dr. Levitt is the Director of the Stein Program on Counterterrorism and Intelligence at the Washington Institute for Near East Policy. From 2008 through 2009, he served as State Department Counterterrorism Advisor to the Special Envoy for Middle East Regional Security. From 2005 to early 2007, he served as Deputy Assistant Secretary for Intelligence and Analysis at the U.S. Department of the Treasury.

From 2001 to 2005, Dr. Levitt served the Washington Institute as founding director of its terrorism research program, which was established in the wake of the September 11th attacks. Previously, he served as counterterrorism intelligence analyst at the Federal Bureau of Investigation.

Dr. Levitt holds a bachelor's degree in political science from Yeshiva University, as well as a master's degree in law and diplomacy, and a doctorate from Tufts University Fletcher School of Law and Diplomacy.

Thank you for being here, Dr. Levitt.

Mr. Seamus Hughes is the deputy director of the Program on Extremism at George Washington University. Mr. Hughes previously worked at the National Counterterrorism Center (NCTC) serving as lead staffer on the U.S. Government effort to implement a national countering violent extremism strategy.

Prior to NCTC, Mr. Hughes served as a Senior Counterterrorism Advisor for the U.S. Senate Homeland Security and Governmental Affairs Committee.

On the Hill, Mr. Hughes authored numerous legislative bills, including sections of the 9/11 Commission Recommendations Act, and the Special Agent Samuel Hicks Families of Fallen Heroes Act.

He is a graduate of the University of Maryland and a recipient of the National Security Council outstanding service award and two NCTC Director's Awards for outstanding service. Mr. Hughes also teaches classes at George Washington University and Georgetown University.

Thank you for being here, Mr. Hughes.

Mr. Frederick Reynolds is global head of financial crime legal for Barclays. Mr. Reynolds joined Barclays from Bank of America where he was an FIU executive and was responsible for global AML investigations, global AML detection and monitoring, risk data analytics, and AML behavior modeling.

Prior to entering the private sector, Mr. Reynolds served as the Deputy Director of Treasury's Financial Crimes Enforcement Network, or FinCEN. Prior to being appointed the Deputy Director of FinCEN from 2010 to 2012, he was Deputy Chief of the Asset Forfeiture and Money Laundering section at the Department of Justice where he oversaw numerous high-profile money laundering and financial crime cases, including ones involving Mexican cartels, terrorist financing, and transnational organized crime.

From 2006 to 2010, Mr. Reynolds was a Federal prosecutor at DOJ where he investigated and prosecuted high-profile cases involving significant money laundering, and financial crime in violations of the International Emergency Economic Powers Act and the Bank Secrecy Act.

Prior to joining DOJ, Mr. Reynolds was the assistant attorney general for the Republic of Palau and a litigation associate for several private firms. Mr. Reynolds has an undergraduate degree from Brandeis University and a law degree from Emory University School of Law.

Each one of you will now 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 record.

Dr. Levitt, you are now recognized.

STATEMENT OF MATTHEW LEVITT, DIRECTOR, STEIN PROGRAM ON COUNTERTERRORISM AND INTELLIGENCE, THE WASHINGTON INSTITUTE FOR NEAR EAST POLICY

Mr. LEVITT. Thank you, Chairman Pearce, Ranking Member Perlmutter, and distinguished members of the Terrorism and Illicit Finance Subcommittee of the House Financial Services Committee. It is an honor and a privilege to testify before you today.

Unlike large attacks orchestrated over time by large groups, lone- offender and small-group attacks can be carried out very

quickly with minimal funding and preparation. The result is that, in some cases, authorities can be denied both the lag time within which they can run an effective investigation and the benefit of key traditional trip wires, like the ability to be able to follow travel, communications, and financial trails, that in the past have proved to be especially productive lines of investigative inquiry.

Lone offenders and small groups are—their attacks are on the rise, especially coming on the heels of explicit calls by groups like the Islamic State and al-Qaida for like-minded followers to carry out attacks in their home countries.

ISIL has been pushing such attacks for years now. In an online 2015 book entitled, "How to Survive in the West: A Mujahid Guide," the group argued, and I quote, "With less attacks in the West being group-networked attacks and an increasing amount of lone-wolf attacks, it will be more difficult for intelligence agencies to stop an increasing amount of violence and chaos from spreading in the West."

The terrorist threat from lone offenders in small groups is also magnified by the phenomenon of returning foreign terrorist fighters. Some of these battle-hardened fighters move on to new battlefronts. Some may return disgruntled and disillusioned. Some are sure to return intending to do harm.

The 2015 National Terrorist Financing Assessment Risk notes one case from Houston of an individual who planned to travel abroad to fight with radical groups in Syria by using an expected tax refund to cover his expenses. The same types of simple funding could also underwrite attacks at home. And this includes the variety of trends that we need to look at here, as you have all mentioned, the low cost of attacks, one particular issue. The self-financing is another. That can be using your own salary. And there is nothing at all suspicious about that. It could be small-scale crime. It could be borrowing money from family or friends, either with or without the knowledge that it intends to do some harm.

Just last week, an Uzbek man in Brooklyn pled guilty to conspiring to provide material support to the Islamic State in a related case. There are legal and illegal financial loans.

But one of the things I think is most interesting is that the idea of the lone wolf is actually a little bit of a misnomer. In more cases, people are "known wolves" rather than "lone wolves," either from what they are posting on social media or from what they are telling their close friends and family, or from external activities. External support continues to be something that is a useful line of investigation.

Last month, U.S. investigators uncovered an ISIS financial network that was transferring money to an operative in the U.S. through false eBay transactions. The recipient, Mohamed El-Shinawy in Maryland, pretended to sell printers on eBay as a cover for the payments he was receiving through PayPal and Western Union for operational purposes in the United States.

The U.N. Security Council has reported that despite military pressure and falling revenues, the ISIL core continues to send funds to affiliates worldwide using a combination of money or value transfer services and the transport of bulk cash. This transferring of money is an opportunity for us, even with small-scale incidents.

The U.N. Security Council report goes on to note that the ISIL core has sent money to places where it does not have affiliates, which, according to a member state assessment, is an attempt to prepare for its eventual military defeat in Syria and Iraq. In other words, not only is ISIL preparing to move funds to its other provinces, it is also moving funds to other places where newly inspired followers or returning foreign terrorist fighters can use or access ISIL funds to carry out attacks. Australian officials report similar issues.

The bottom line is that countering homegrown financing is not something new. The 9/11 Commission Report specifically talked about how, while terrorists have shown considerable creativity in how they move money, we have had some success. But over time, if some of their terrorist operations do not require as much outside money that may—they may be more self-funding either through legitimate employment or low-level criminal activity.

We should have anticipated this coming. And, therefore, there are several things that we could be thinking about. The first is that lone offenders and small groups still need money. And despite the challenges noted above, even the Financial Action Task Force (FATF) underscores that their need for money means we have opportunities.

Consider the case of Dhiren Barot in the U.K., where financial trails played one small part in identifying who he was. He was only known as Musa al-Hindi and was thwarted in his plot several years ago to blow up a limousine filled with gas canisters in the City of London.

Second, the private sector has access to tremendous financial information and can be better positioned to act on it and share it with us if we provided them greater insight.

Now, in the U.S. Government, we do this type of thing all the time. We assess and reassess what the trends are. FinCEN does this all the time in terms of updating its automated business rules that develops in terms of how it and its partners search Bank Secrecy Act information. There is a lot more that we could be doing here. And a great example is the U.K.'s joint money laundering intelligence task force. That is a great example in the U.K.

And finally, financial intelligence is not going to solve all of your problems. There will be some cases in a true lone-wolf situation where someone has no connectivity to others and is taking money out of their own bank account, and this particular tool set will not be as effective.

But financial intelligence continues to surprise. In one instance, financial intelligence helped the U.S. Air Force determine what oil refineries to target in Iraq and Syria. And so, we should not rule this out as a tool that will no longer be effective. We just have to find new ways to partner with the private sector to make it as effective as possible.

Thank you very much.

[The statement of Dr. Levitt can be found on page 48 of the appendix.]

Chairman PEARCE. The Chair will now recognize Mr. Moreno for 5 minutes.

STATEMENT OF JOSEPH V. MORENO, PARTNER, CADWALADER, WICKERSHAM & TAFT LLP

Mr. MORENO. Chairman Pearce, Vice Chairman Pittenger, Ranking Member Perlmutter, and distinguished members of the subcommittee, thank you so much for the invitation to appear before you today. It is truly an honor to be part of this discussion.

Since the attacks of September 11th, we have been largely successful in preventing the next catastrophic attack, and have prosecuted hundreds of financiers, facilitators, and charities for supporting terrorism. However, as pointed out, identifying and preventing lone-wolf or small-scale terrorist attacks presents a unique set of challenges. Lone-wolf attackers are typically self-radicalized with no direct connection to an organized terrorist group. With minimal training and coordination, they can carry out a mass shooting, detonate explosives, or drive a vehicle into a crowd of civilians.

These attacks are frequently self-funded at amounts often considered too small to detect solely through the tracking of financial transactions. But studies show there is almost always some identifiable behavior leading up to a lone-wolf attack, whether it be an online manifesto, training, reconnaissance, or the acquisition of weapons or other materials.

Knowing this, we must continue exploring ways to identify these behaviors before an attack takes place. First, we should take a hard look at whether we can better utilize our existing prosecution tools and financial reporting framework. The Bank Secrecy Act criminalizes the act of money structuring or making transactions under $10,000 to cause a bank to fail to report that transaction to the Federal Government. Structuring prosecutions and the use of asset forfeitures have come under criticism in recent years due to cases where the funds of law-abiding citizens were seized, and they were left fighting to get their money back.

As a result, both the IRS and the Department of Justice have taken the position they will focus only on structuring cases that involve significant criminal activity. The problem with this approach is that it focuses only on where the money originates, not on where the money is going.

If a person is making multiple withdrawals of just under $10,000 within days, or withdrawals from multiple bank branches or multiple ATMs on the same day, for example, they are probably trying to hide what they plan to do with that money.

We should also examine how we utilize suspicious activity reports prepared by banks and other financial institutions. We need to explore better technology to flag small transactions that may be indicative of illicit use, such as artificial intelligence systems designed to detect suspicious activity in real time.

At the same time, we need to make sure that joint Federal and local SAR review teams have the personnel and funding they require to get through and follow up on the tremendous volume of reports they receive each year. The suspicious activity reporting process is seriously impeded if the reports are not actually reviewed and acted on.

Second, we need to look at ways that would-be attackers anonymously solicit, move, and spend money. If we were having this con-

versation 15 years ago, we would focus primarily on hawalas, cash couriers, and charities.

Now, new payment methods such as virtual currencies, crowdfunding technologies, mobile payment applications, and online peer-to-peer payment systems provide persons with ever-expanding methods to raise and move funds anonymously. As these technologies develop, we must ensure that our reporting requirements keep pace.

Another emerging issue is the proliferation of pre-paid cards. Today, anyone can go into a supermarket and buy packages of prepaid cards in cash which can be used to purchase virtually anything. You don't even need the physical card to make a purchase. Individuals can cut and paste the account number, expiration date, and security code into an email or text message and effectively transfer that purchasing power anywhere in the world. By doing so, they effectively convert their cash to a form of anonymous buying power, significantly working around the financial reporting safeguards that apply to traditional credit and debit cards.

Finally, we should consider other methods to address this issue. There have been proposals to regulate various types of consumer products commonly used in attacks, such as ammonium nitrate. Tagging agents currently required for plastic explosives could be required for use in gunpowder in bullets and fireworks to help trace those products after an attack. Data on the purchases of items such as pressure cookers, diesel fuel, and other products could also be collected and tracked.

At the same time, we must continue aggressive surveillance and infiltration of websites and social media used to spread propaganda, raise funds, and incite violence. And operators such as Facebook and Twitter must be pressed to enforce their terms of service and close accounts that are used to incite illegal activity.

Just as we strive to cut off terrorist organizations from financial systems, we must also make it as difficult as possible for them to use the internet to finance and coordinate attacks.

Finally, many lone-wolf attackers, at some point, demonstrate indicia of depression, paranoia, or violence prior to an attack. In most communities, the only option for reporting someone is to call the police or the FBI. If there was a mechanism for some sort of mental health intervention, concerned friends and family members may be more willing to get that individual the help they need before they go down the path to violence.

I fully acknowledge that each of these options comes with costs, both to taxpayers and consumers and to individual privacy. And these costs must be weighed against the likelihood these activities would, in fact, be effective, either as prevention and disruption, or for criminal prosecution after the fact.

Addressing the threat of lone-wolf and small-scale terrorist attacks presents many challenges, and I applaud this subcommittee for taking on this difficult issue and opening up this bipartisan dialogue. And I stand ready to answer any questions you may have.

Thank you, sir.

[The prepared statement of Mr. Moreno can be found on page 63 of the appendix.]

Chairman PEARCE. Thank you.

And the Chair will now recognize Mr. Hughes.

STATEMENT OF SEAMUS HUGHES, DEPUTY DIRECTOR, PROGRAM ON EXTREMISM, THE GEORGE WASHINGTON UNIVERSITY

Mr. HUGHES. Thank you.

Chairman Pearce, Ranking Member Perlmutter, distinguished members of the subcommittee, it is a privilege to be invited to speak on the threat of extremist financing in the United States.

Extremism inspired by jihadist groups, like al-Qaida and ISIS, remains a potent threat to the United States. Since 2014, 133 individuals have been charged with ISIS-related activities in the United States. The vast majority of these individuals are U.S. citizens, speaking of a threat of homegrown terrorism.

While violent plots often garner the most attention, a broad swath of cases demonstrate the enduring relevance of finance-related activities by jihadists in the West.

This testimony concerns ISIS-related extremism, but there are other extremist organizations that pose a threat to national security. Recently, the FBI and the DHS issued a joint intelligence bulletin stating that actors of the white supremacist extremist movement will likely continue to pose a threat of lethal violence within the next year.

Despite these concerns, few studies to date unpack the financing of domestic extremism groups. There are significant differences between financing schemes utilized by domestic extremists and their jihadist counterparts.

Funding a designated terrorist organization is a criminal offense under the material support statute, whereas there is no statutory designation for domestic extremist groups. The result is domestic extremist groups are not under the same pressure to disguise their funding as foreign terrorist organizations.

However, I will focus primarily on my testimony on ISIS. The activity of ISIS here in the U.S. ranges from individuals using cryptocurrencies online to coordinated clusters supporting actors abroad. Impactful terrorist attacks do not require large sums of money, but, rather, low-level costs such as plane tickets, guns, or rental cars. In this way, participation in terrorist organizations is easier than it has been before. For counterterrorism practitioners, detecting suspicious financial transactions is difficult. Modern terrorist financing entails a range of behaviors that disguise illicit activity or circumvent detention altogether.

A brief review of the ISIS and America cases highlights the diversity of the modern-day terrorist financing. In one type of scheme, individuals, or groups of individuals, crowdsourced moneys for foreign fighters who were already in ISIS-controlled territory. One illuminating example is a case of a husband-and-wife team in Missouri who raised money for the Bosnian Diaspora, and then gave that money to a high-ranking Bosnian American ISIS commander.

Another type of financing is where individuals or groups garner resources to fund someone to travel overseas. This form of activity was especially common when traveling to ISIS was easier. Matt mentioned the case of a young man from Brooklyn who was financ-

ing two people to go join ISIS. In Minnesota, we had three men who were using fraudulent student loans to fund their travels. However, in the case of the terrorist attack in San Bernardino, the attacker allegedly used legal financial loans to acquire the money necessary to purchase weapons. And sometimes it is a back and forth. Sometimes ISIS is the instigator for funding. A good case of that is Mohamed Jalloh in Virginia, or Aaron Daniels in Ohio, who were giving money to al-Sudani, an external ISIS commander, to fund his attacks.

One of the most striking cases of ISIS-related financing in the U.S. is that of Mohamed Elshinawy. Elshinawy was working with an ISIS commander in Syria. That commander gave him money through a series of U.K. shell companies, and then funded the money through Maryland so he could get enough funding to attack the United States. All told, he got about $8,700 before he was arrested.

The review of the cases reveals four broader trends in the terrorist financing and counterfinancing programs. First, government regulations is not the only approach to deter extremists. A public-private partnership of best practices can sometimes augment a government-led approach.

Second, countering violent extremism programs should target violent extremists of various ideological shades, not just the Omar Mateens of the world, but also the Dylann Roofs.

Third, financing has largely become decentralized, as illustrated by the Maryland case. Terrorists now have a multitude of online platforms to exchange funds. Additionally, relatively small transactions are unlikely to draw attention, allowing terrorist finances to hide in plain sight.

Lastly, initiatives aimed at detecting and disrupting finance-related activities should account for emerging technologies, whether it is violent extremists that mark their transfers in cryptocurrencies, or hide their funds in plain sight, committed terrorist actors are clearly willing to take the road less traveled to advance their aims.

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

[The prepared statement of Mr. Hughes can be found on page 38 of the appendix.]

Chairman PEARCE. The Chair now recognizes Mr. Reynolds for 5 minutes.

STATEMENT OF FREDERICK REYNOLDS, GLOBAL HEAD OF FINANCIAL CRIME LEGAL, BARCLAYS

Mr. REYNOLDS. Thank you, Chairman Pearce, Vice Chairman Pittenger, and Ranking Member Perlmutter. I appreciate the opportunity to appear before you here today to discuss how the financial sector and law enforcement can work together to combat lone-wolf terrorist attacks.

Over my career, I witnessed the critical role that financial institutions play in the detection and prevention of money laundering and terrorism financing. Without their assistance, it would be difficult, if not impossible, for law enforcement to follow the money.

Recently, we have witnessed the rise of lone-wolf terrorist attacks. Because these attacks are often inspired by, but unconnected to larger terrorist groups, the techniques that we typically employ to track the terrorists are, at times, ill-suited to this new threat.

When looking to identify the financial indicators of lone-wolf attacks, the challenge for financial institutions is threefold. First, lone-wolf attacks are characterized by low-dollar financial transactions. This makes our traditional detection and reporting tools less effective.

Second, lone wolves don't exhibit typical terrorist financing behavior, frequently using their own clean money for the attack. Or said differently, their financial behavior blends with the myriad legitimate transactions conducted every day by law-abiding customers.

Third, financial institutions are currently limited by domestic laws in their ability to share information between institutions or even across borders within the same institution. This can result in financial institutions being unable to identify normal client behavior.

Given these challenges, how do financial institutions differentiate between normal customer activity and a customer planning a lone-wolf attack? Often, a single piece of information—an account number, an IP address, or even a telephone number—becomes a Rosetta Stone that allows financial institutions to correctly identify a nefarious actor engaging in what might be otherwise innocuous conduct.

While not a silver bullet, continuing to receive these Rosetta Stones from law enforcement and modernizing the current sharing system, is critical to the detection and prevention of future attacks.

A few areas where information sharing could be improved include: authorizing U.S. financial institutions to share SARs with foreign branches and affiliates; explicitly expanding the types of information sharing permitted under the Section 314(b) safe harbor; deprioritizing the investigation and reporting of low-value activity and allowing financial institutions to reallocate these resources to higher value intelligence activities; encouraging the formation of a U.S. joint money laundering intelligence task force; and clarifying financial institutions' ability to discuss the filing of SARs when working together on a case, and encouraging them to jointly file a SAR.

I would like to take a moment to illustrate the power of information sharing by discussing an investigation that Barclays conducted after law enforcement alerted us to an IP address that it believed was connected to a terrorism suspect.

Using this IP address, Barclays identified Mr. A, who was a student. Mr. A received money from a variety of sources, including over 522,000 pounds from Mr. C, 10,000 British pounds from Mr. J, and 4,000 pounds from Mr. C.

Through further network analysis, we identified that Mr. C was part of a broader funding mechanism for potential terrorist activities. Additionally, we found that in addition to funding Mr. A, Mr. J also funded Mr. M, whom Barclays had previously tracked and reported as a potential foreign terrorist fighter. In Mr. H and Mr. B, whom Mr. A also funded, both had characteristics of foreign ter-

rorist fighters. Perhaps most interestingly, we determined that Mr. A transferred money to a heavy machinery company that makes oil field placement parts.

From one IP address, we were able to identify related individuals who may have funded multiple foreign terrorist fighters, purchased oil-filled parts, and had links to others who were also funding or supporting suspected terrorist activities. While not every IP address will yield such potentially significant results, this case illustrates the power of the public-private partnership.

Before I close, I would be remiss if I did not address the very real issue of customer privacy. Barclays takes our customers' privacy interests seriously. And rather than cast an impossibly wide net that includes data from millions of innocent customers, targeted information sharing allows us to focus on the few high-value cases where true national security risks are present. Moreover, by increasing our understanding of these transactions, it will allow us to discount alerts that would otherwise turn into SARs, because we cannot understand the purpose of the transaction. So while at first it seems counterintuitive, robust information sharing actually enhances individual privacy, though admittedly not for the lone-wolf terrorist.

Financial institutions want to get this right. We are committed to ensuring that terrorists do not use our institutions to fund their activities. But we cannot do it alone. We need to be able to share and receive information both from law enforcement and between financial institutions to be most effective in identifying terrorist financing.

I would like to, once again, thank the subcommittee for the opportunity to speak on this important topic as well as for its continued engagement on this important national security issue. I look forward to your questions.

Thank you.

[The prepared statement of Mr. Reynolds can be found on page 71 of the appendix.]

Chairman PEARCE. Thank you, each one of you, for your presentations today.

The Chair will now recognize himself for 5 minutes for questions.

Mr. Reynolds, you appropriately, at the end of your presentation, talked about the need for privacy concerns and special people who are uninvolved.

How do you see that playing out in our attempts to detect and deter? Tell me a little bit more about that?

Mr. REYNOLDS. I think it is a great question, Mr. Chairman. And I think that in many ways, we have to balance, obviously, customer privacy and some of the new technology that we have to exploit data.

One of the reasons why I am a great supporter of increased information sharing is because I think it allows financial institutions, first and foremost, to target particular individuals, or particular cells or groups, and to do network analysis that is a great benefit to law enforcement.

So, again, rather than casting a very broad net, it allows us to really focus on the individuals who are of most concern to law enforcement which, in my view, helps protect customer privacy.

Second, especially in the United States, very often because of the way the rules are structured, where an institution cannot discern, really, from what is in front of it, the lawful, or commercially reasonable purpose for the transaction, very often by default, you have to file a SAR. So in my view, very often institutions have to file SARs on cases where, if they had additional information on that particular customer, that particular transaction, they very well might not file that SAR. So I do think it both enhances our ability to focus on those suspects that present the greatest national security issues, but also allows us not to file on customers whom, I think with just a little more information, we could probably understand the point of the transaction and, therefore, we wouldn't need to file a SAR.

Chairman PEARCE. And on page 3, Mr. Reynolds, in your testimony, you talk about the need for financial institutions to be able to receive and share information.

In your opinion, is that sharing going on currently, or do we need a change in law, a change in regulations? And if the sharing is ongoing, do you think that it is not enough or—give me a little bit more flesh there, if you can.

Mr. REYNOLDS. Sure.

So it currently is going on. I would have to say that I think our law enforcement partners are working very hard, most especially the FBI, at sharing information. So I do want to give credit where credit is due. I do think there is a great amount of sharing that goes on. I think, though, that, really, we could do more. And I think if we had more targeted sharing we would do better.

On Section 314(b), I think that is where we probably do need either a regulatory or a legislative fix. Currently, under the regulations and law, institutions can only share where there is a suspicion of money laundering or terrorism financing. So what that essentially means is, once you have already detected something you have decided is suspicious, that is the point when you are really allowed to share.

Really, in my view, we need to back that up, because some of the benefit to sharing is actually detecting the activity in the first place. I think if you look at lone-wolf terrorism, like we are looking at here today, this is a great example where if we moved that sharing line back and institutions were allowed to share at an earlier stage, I think we would have a greater ability to both understand transactions, so exclude innocent suspects, but also focus on those suspects who present the greatest risk.

Chairman PEARCE. Dr. Levitt, if you could, I would like your opinion on the privacy issue also, and how we are balancing that, and what your long-term concerns would be. Because typically, in my opinion, we establish a protocol, and then we try to work up to the edge of the protocol. Sometimes, we might go over that. And so I would like your insights, if you could?

Mr. LEVITT. I agree completely with Mr. Reynolds that we have to take the privacy concerns into account in the very first moment and balance these equally important concerns. I also think that if we provide more information, we could have better SARs filing.

It was my experience at Treasury that we would sometimes find ourselves swimming in a sea of unnecessary SARs. And it takes

time to go through those. So even from the law enforcement side, from the government side, this has great utility.

It is difficult, though, because if we do expand the ability, for example, under Section 314(b), if we move the needle earlier in the process as the baseline, so you are going to be opening up more accounts to potential investigation on the potentially negative side. The potential positive side is that you will be in a better position to rule out the people that you don't really need to be looking at. But you could be looking at a larger number of accounts in the first instance. And so I think we need to be clear about what it is we are concerned about with privacy.

I think the biggest thing is how that information is handled. What is the purpose of looking, how you look, what is done with that information as opposed to, in that first instance, how strong is the baseline for the look. Because I agree, right now the baseline is such that if you don't already have a money laundering or terror financing concern, you can't look. And for the purpose of lone offenders or lone wolves, that is a little bit too late.

Chairman PEARCE. Thank you. My time has expired.

I now recognize the gentleman from Colorado, Mr. Perlmutter, for 5 minutes for questions.

Mr. PERLMUTTER. I want to follow a similar line. Mr. Reynolds, Mr. Hughes, you talked about public-private partnerships. And, Mr. Reynolds, you gave us the example of Mr. A, Mr. B, Mr. C, Mr. D, Mr. H, and Mr. J. But it all came off of one IP address that was delivered to you.

So explain to me—are you expecting something from law enforcement to help you focus? Because basically, this was coming from probably—and I think, Mr. Hughes, you talked about it—some social media statement or something that tipped off law enforcement to help you focus. So is that what you are expecting from the FBI or somebody?

Mr. REYNOLDS. I think that is absolutely right, Congressman. In this case, it was an IP address that was given to us. And what we found is, while the bank—and I won't speak for every bank, but I think most banks have strong programs and work very hard to detect these on their own.

What we have found is that, where we are given that piece of information, whether it is an IP address or a phone number or a name or an account number, very often it is that initial thread that we are able to pull that really allows us to do some very, very exciting network analysis and allows us to really build out the network. Because, again, when you are talking about lone-wolf terrorists, very often, their activity looks very much like a normal consumer.

Mr. PERLMUTTER. Would it have made any difference? In your example, you said that one of the transfers was for 522,000 pounds. If it were a smaller amount, would you have not been tipped off?

Mr. REYNOLDS. No. I think, actually, we would have still found that. The 522,000, to be clear, was not one transfer, it was multiple transfers over time. So what we did is we essentially started from Mr. A, who was the initial person we detected using that IP address, and then started to build out using other factors, and looked and really built the network out for Mr. A, and then found a lot of the actors. And then it jumped to—as you can see in the chart,

there are various parts of the chart, it is quite large. In fact, we sort of condensed some of it to make it fit on one page.

But at the end of the day, we found, actually, multiple groups that were all in concert and acting together. We saw links between them, whether it be addresses or transfers. And so what we were able to do to the—this was the U.K. Government who had given us this information—we were able to then turn back to the U.K. Government and give them a chart. And, again, we obviously don't have visibility into exactly what these individuals were doing other than their financial footprint, but we were able to give the U.K. Government a very clear picture of what, at least to us, looked like a financing network. And it really came from that one IP address.

Mr. PERLMUTTER. Mr. Hughes?

Mr. HUGHES. Yes. I think you are absolutely right. In many ways, you are just looking—law enforcement is going to be a thread, and you want to pull it to see how big the sweater is, right? And so you are looking for law enforcement to give you something that is going to give you leads.

I would note, though, when you look at the actual homegrown terrorism attacks, the successful attacks, the overwhelming vast majority were already on the FBI's radar prior to attack. And so it is not necessarily the lack of information. It is the lack of the ability to act, and sometimes people haven't crossed the legal threshold. Sometimes the FBI doesn't have the resources to run things down. And so I think that is where the public-private partnership comes into play.

So going to Barclays and saying, I have this, I know there is something there. You have some resources there. Can you help me pull this thread a little bit more? I think that is where we play a role.

Mr. PERLMUTTER. All right. Mr. Moreno, I want to switch to domestic terrorism for a second, because you talked about that and the difference between the laws available for detecting a foreign kind of financial assistance versus domestic. And I am thinking of Timothy McVeigh and Terry Nichols blowing up the Murrah Building in Oklahoma City.

So I don't know how much that ammonium nitrate, or whatever it was he packed into that truck cost him, maybe you guys have some estimate, but how—I am worried about those guys too—would you say we can best stop that murderous act?

Mr. MORENO. Yes, sir. I think that the approach for domestic attacks is a bit different. I know there has been talk about potentially criminalizing or creating a proper Federal crime for domestic terrorism versus just what we have now, which is basically application of State and Federal law.

As far as the ammonium nitrate from the Oklahoma City bombing—we have had DHS-proposed rules for about 10 years now. The fact is that we just haven't seen a lot of further explosives attacks with ammonium nitrate use. So I think in each one of these cases, we really have to balance the costs: the cost to the government; the cost to the consumer; and the cost to people's privacy. People do not want to be tracked. And are we going to be running down every time someone goes to Home Depot and buys fertilizer versus a significant purchase of product used in an attack like that?

So, I think in each case, we have to take the lessons learned from the attack and figure out how much we are willing to invade the privacy of consumers versus the potential for the use of that same sort of material in a future attack.

Mr. PERLMUTTER. Thank you.

Mr. Chairman, I yield back.

Chairman PEARCE. The gentleman's time has expired. And the Chair now recognizes the Vice Chair of the subcommittee, Mr. Pittenger, for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman.

Mr. Reynolds, from your experience at FinCEN, how many SARs report were filed each year?

Mr. REYNOLDS. It is very significant. I don't know the current total. But I know that about 2 million SARs are filed each year.

Mr. PITTENGER. This is from financial institutions here in the United States?

Mr. REYNOLDS. Yes, sir.

Mr. PITTENGER. Can you say to what extent or range, from your experience at Bank of America and at Barclays, how many reports that you would have to file each year?

Mr. REYNOLDS. From Barclays, it is probably in the several thousand. For Bank of America, it is well over 100,000 a year.

Mr. PITTENGER. Yes, sir.

And from your testimony, what you have said, that the—if you had the legal capacity to receive information from the Federal Government in terms of particular IDs and individuals that they are pursuing, that would then reduce, in vast amount, the number of individuals that you are having to send reports on and give oversight to; is that correct?

Mr. REYNOLDS. Yes, I would completely agree with that.

Mr. PITTENGER. Yes, sir.

So let's look at sharing data between institutions and your own and other institutions.

While there has been latitude there, is there a restriction or an inhibition to do that reference to legal concerns? Is there a need for a safe harbor for institutions to make sure that they can do this? Is there a gray area there that we need to clarify?

Mr. REYNOLDS. There is. Under current regulation, the way it reads right now is that you have to have a suspicion of money laundering or terrorism financing. So as one of my fellow panelists pointed out, at that point, it really is too late because—

Mr. PITTENGER. It's very subjective in some respects.

Mr. REYNOLDS. It has already happened. It is much too late. And I think the real benefit of the sharing, whether it is from the government or whether it is under the safe harbor between institutions, really comes where institutions can leverage the power of the data analytics that they have now, and they can look across the data. And I think, to your point, which I think is exactly the correct one, is that it both allows us to target those people who are suspicious, because you can see multiple sides of the transaction, as opposed to just the side that Barclays or just the side that Bank of America sees. You can see all different sides of the transaction. So it allows you to better target those individuals you really care about.

But likewise, by being able to see all sides of the transaction, you actually are able to discount a great number of these SARs that we would otherwise file just simply because we lack information to discount the suspicion, which really is the standard, that if you can't discount the suspicion, you have to file.

And so in many cases, I think we file where, if we knew a little more, we probably wouldn't have to.

Mr. PITTENGER. Yes, sir. I think it is well said.

It is so important for us right now to pull back and take a full view of how—of assessing this and come up with a different basis for how we can pursue these individuals. And I think all of us who cherish our privacies and civil liberties, we would respect the type of engagement that you have proposed today.

Mr. REYNOLDS. Thank you.

Mr. PITTENGER. Thank you.

Mr. Hughes, I would like to ask you, with reference to those who provide material support to lone-wolf terrorists, are we doing enough to punish them, or are there any gaps that law enforcement or Congress could address?

Mr. HUGHES. In regards to material support, I don't believe so, because the material support clause is actually quite elastic and broad-based. So unlike other countries, if you are driving to the airport to go jump on a plane to go to Syria, you can get arrested for the drive. And so the material support clause, right or wrong, gives law enforcement a large latitude to do that.

We have also seen law enforcement be pretty creative in the way they do arrests for individuals they may be concerned about that doesn't rise to a level. A good case is in California, 2 young men got arrested for 26 charges of bank fraud. They were clearly ISIS supporters through and through. But there wasn't enough to rise to a material support of the case. So I think you are seeing that law enforcement, in many ways, aren't allowing the system to light up in the way they used to, because they are concerned about these lone-wolf attacks. The gentleman who stabbed 10 people in Minnesota, right? And so they are not letting people talk to other people. And they are closing in earlier on, and so they are more willing to use forward-leaning prosecutions.

Mr. PITTENGER. Thank you.

Thirty seconds, Mr. Levitt. To what extent are foreign governments involved, in your opinion, in helping fund bad actors affiliated with or otherwise associated known terrorist organizations?

Mr. LEVITT. State sponsorship is still a very major problem. It is a separate problem from the lone-wolf or lone offender problems. To the contrary, we have lots of good partners around the world. As you heard before, the Barclays case involves the U.K., where people are trying to work together with us to deal with foreign terrorist travelers in particular. But there still are plenty of countries out there, the Irans of the world, et cetera, that pose significant problems. But I would argue that is a separate problem.

Mr. PITTENGER. Is Qatar a concern to you?

Mr. LEVITT. I had the opportunity to testify on Qatar recently. And, yes, Qatar is a concern. It is also not the only concern in the region. Some of the issues that have been raised about Qatar are very substantive, and some of them are not. So it is a complicated

issue. It doesn't fit into a black-or-white, but there is more that Qatar could do as there is more that others in the region could do.

Mr. PITTENGER. Thank you.

Chairman PEARCE. The gentleman's times has expired. The Chair now recognizes the ranking member of the full Financial Services Committee, the gentlelady from California, Ms. Waters, for 5 minutes.

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

In the years since 9/11, our Nation has witnessed its share of attacks by homegrown violent extremists inspired by foreign terrorist organizations. This includes the San Bernardino shooters who tragically took the lives of 14 and wounded 21 others, as well as the Pulse nightclub shooter who callously took the lives of 49 and wounded another 53 innocent victims.

However, as the recent events in Charlottesville, which took the life of Heather Heyer and two VA State troopers, have reminded us, extremists radicalized by foreign terrorist groups are not the only terrorists with the capacity and the will to target and kill American citizens. Indeed, domestic terrorist attacks have become more frequent in recent years.

I just took a look at what has happened since 1992: Ruby Ridge standoff, three killed, two wounded; Oklahoma City bombing, 168 killed, over 680 wounded; 2009, United States Holocaust Memorial Museum shooting, one killed, one wounded; 2012, Wisconsin sheikh temple shooting, killed six, wounded four; 2013 Los Angeles International Airport shooting, attack on TSA, officer killed, one wounded; 6/2015 Planned Parenthood shooting, killed three, wounded nine; 2017, Portland train attack, killed two, wounded one; Charlottesville, car ram attack, killed 3, wounded 19; and I am worried about these domestic attacks.

As a matter of fact, I was forced to focus on it a little bit more yesterday at my office in Los Angeles. One of the people opening the mail opened an envelope, and a bunch of powder fell out with a note about me dying and killing Hillary Clinton, and on and on and on.

This is getting more frequent. And I know that we have privacy concerns and information sharing and all of that. But I am wondering, what can we do to get a handle, a fix on these lone killers? And not simply just throw our hands up and say we can't really do anything because of privacy concerns. And I am wondering, particularly at our financial institutions and banks, et cetera, if questionnaires that do not invade privacy, but simply ask questions about what the intentions are for the use of certain money under certain circumstances, and those people can say whatever they want to, and they can respond in whatever way they want to. But if resources are used to go out and commit killings, et cetera, they will have lied on the questionnaire. And perhaps that can trigger some kind of action to begin to prevent this kind of domestic terrorism. I think we should focus a lot on domestic terrorism also.

So I would like to ask again, given all that you have said about how difficult it is and the privacy concerns, do you have any thoughts about what we can do to begin to deal with the KKK and the white nationalists, the extremists, the alt right, they are on the

internet, they are Breitbart. If you look at YouTube, you see how much they want to kill me and others. What can we do?

Anybody?

Mr. HUGHES. I think there are a couple of things back there.

First is, I absolutely agree it is not an either/or proposition. You should be worried about the Omar Mateens, the Orlando shooters of the world as much as you are the James Fields and the Dylann Roofs of the world. And I am concerned, when we look at these issues, that we tend to bifurcate it and make it into buckets. There are different programs that we could address on these things.

Domestic extremists tend to use criminal activities in order to fund their attacks in a way that jihadists don't. So they are usually more likely to pop on the radar on these things. There are a number of different organizations that are doing interventions and spaces on far right and domestic extremism groups like Life After Hate in Chicago.

Ms. WATERS. Thank you very much. I am going to have to interrupt. I have to yield to Mr. Gottheimer. He has to go, so I will yield to him.

Mr. GOTTHEIMER. Thank you very much.

I want to recognize the program on extremism for bringing light to the recent report that a senior ISIS official used eBay and PayPal to funnel a terrorist in the United States.

Today, I am writing to FinCEN to urge them to take additional steps to curb money laundering and suspicious financial transactions online. As technology advances and lone-wolf terrorists continue to innovate, how can Federal enforcement efforts keep pace to crack down illicit use of new transaction methods? And I am open to anyone responding.

Mr. LEVITT. I will just say in brief, because no one else was lighting up, that that is actually a success case. I mean, that gentleman was stopped. That means of transfer, as sophisticated as it was, was identified. I would not cite that as a case of, oh, my God, we need to do more. I would cite that as a case of, they are trying to get sophisticated. We are pretty sophisticated, too. We were on top of that. We thwarted that case.

But your overall point is absolutely on target. And that is the whole purpose of this hearing, I think, to figure out how we can fine-tune our tools in those cases which are the exception to prove the rule, which is to say that they truly are lone wolves, where they are using their own money or they are taking out a loan legitimately, or doing some type of crime that might not come on our radar. These are the cases that are really different.

For the vast majority of other things, we have pretty good systems in place. They can be fine-tuned in various ways to facilitate better sharing within the financial community between government and financial services. We have been talking a lot about government providing information to banks. That is very important. We also need to talk about the information that banks see so they can provide usable SARs to investigators.

But what is different here is, what do we do about those cases where someone is taking $50, a knife out of the drawer, $2,000. And the answer is, we are going to have to couple this toolkit with a whole bunch of others, including old-school HUMINT and basic

investigations, because this is not going to solve all our problems. There will be cases where finance is not going to be the biggest part of our toolkit.

Mr. GOTTHEIMER. Thank you.

Chairman PEARCE. The gentlelady's time has expired. The Chair now recognizes Mr. Rothfus for 5 minutes.

Mr. ROTHFUS. Thank you, Mr. Chairman.

Dr. Levitt, I want to start with you. Mr. Reynolds had talked about a case where law enforcement came to Barclays, I think with an IP address, and so that the investigation was able to go forward on that basis.

Can you think of any information not currently available to law enforcement that might allow authorities to identify lone wolves if financial institutions started gathering that information? Again, in the case that Mr. Reynolds cited, it was the law enforcement that came with the IP address to the financial institutions. But can you think of other information a financial institution might be gathering that would help in a detection?

Mr. LEVITT. In advance of this hearing, I gave this a lot of thought. And the simple answer is, I don't yet have a great answer. Because most of the activity, as you have heard my fellow panelists say, that we are talking about in a true lone-wolf situation, is going to look completely innocent with the exception of someone who engages in crime or misfiles or lies on a loan application where we might find out about them for other purposes. But someone who just takes out money from their bank accounts, or gets a job for a couple of months or asks mom or dad or a sister or whomever for funds, that is going to be very, very hard to track.

The only thing I can think of is this: We need to take a close look at the very granular, detailed information that we collect, the type of thing that makes the analysts really excited, right? The email address, the phone number, the driver's license number, and more recently, the IP address. Are there other types of things that we could be collecting that would actually be useful, not collecting for collection's sake? I think a lot of people were surprised about how incredibly powerful the IP address could be as a tool, and especially at a time when people might be lone wolves, but will still say something on social media.

Mr. ROTHFUS. Mr. Moreno, you identified a number of types of financial services that the lone wolves utilize. I think you mentioned the pre-paid cards and other things. Is there a favored type of financial services that lone wolves use?

Mr. MORENO. Sir, I don't know if there is any one favored method, but there is certainly a buffet of options that are now at the disposal of folks, that weren't there even 5 years ago. And I think really the point is, if people think they can move money, solicit money, raise money, in a more anonymous fashion, then they will try to do so.

Mr. ROTHFUS. Would it not lose some anonymity, though? The case you cited, I think we could take the payment card information and send it via text. I guess if you have a throw-away phone, you can maintain anonymity there. But it would put some fingerprints on it, wouldn't it?

Mr. MORENO. It would, sir, yes. But I think there are additional steps. So, for example, for pre-paid cards, we can put limits on how and what can be purchased with those types of pre-paid cards. People can buy packs of 4 or 8 or 12 of them and put together a few hundred dollars. Or if we said that you can only use those types of cards in certain retail storefront locations and not online, or if you could not aggregate them and buy expensive items, or if you needed the physical card, and perhaps a chip with it. I think there are some reforms we can do to sort of plug those gaps. And I think we can look at those types of plugging actions in all varieties of these new kinds of emerging ways of payment. But I think really the key is to shine light on who is using this, both as a deterrent, so people don't think they can get away with these sorts of transactions anonymously, but also as a way to prevent and prosecute after the fact.

Mr. ROTHFUS. Mr. Reynolds, we talked a little bit about that suspicious standard in 314(b). Can you give some examples of activities that might be detected by earlier information sharing if not for that standard in there?

Mr. REYNOLDS. Sure. Let me give an example that we have seen in other cases. I saw this when I was on the government side, but I think it would be equally applicable to terrorist financing. You may have a person who, for instance, would have a bank account at bank A, and there is money going in and out of the account, nothing terribly suspicious. So if you just look at that, if a person who works at sort of a mid-level job, the pay coming in looks commensurate with the job, so there is no reason to look at that account again. If I then told you that in addition to having an account at bank A, this person had an account at bank B, C, D, E, and F, and we saw money coming into all of those accounts as well, suddenly that person is incredibly suspicious. But this is exactly the sort of information that you could not share currently.

Mr. ROTHFUS. Would there be a limiting principle, though, for a financial institution as it does this kind of information sharing, if it is not a suspicion standard?

Mr. REYNOLDS. So, again, I think in the law, the definition of "suspicious," obviously, is very technical in the law. And what I would argue is certainly to the extent that you don't have a need to look at a customer, then I don't think you should be looking at that customer. And certainly, in my experience, that has been the rule that everyone lives by. What I would say is that I think that there are some opportunities. If you are using larger data sets, you don't actually have people looking at that data. So the data itself is sitting there. But it is not something that people are going through. No one is looking at it. No one is saying, oh, I saw that Mr. Reynolds likes to buy comic books, and he has spent $500. There is no one actually looking at that. What it is, instead, is it is algorithms that are running across the data. And one of your algorithms may be, for instance, to look for an individual who has these certain financial parameters and has five or more accounts across institutions.

Now, there may be a very good reason that person does and it could be quickly discounted by an analyst. But I would suggest that is the sort of thing that you would want an actual human being

to then look at and determine, okay, this looks out of character for this person. This is not what we would expect for this particular customer. So let's look a little closer and understand, why do they not look like everyone else? And I think that is the fundamental point that we are talking about, is that thread, whether it is provided by the government or provided by big data, that thread to pull on.

Chairman PEARCE. The gentleman's time has expired.

The Chair will now recognize Mr. Lynch for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. And I thank the ranking member. I want to thank the witnesses for your help as well. Some of you are frequent flyers to this subcommittee. So I really appreciate it.

With respect to lone-wolf and individual-actor events, I worry that we are not using the right tools. There is that old saying that when the only tool on your tool belt is a hammer, everything starts to look like a nail. And so we have a fairly robust financial services community that is highly regulated. We have the USA PATRIOT Act. So we have those tools that we can use to try to track organizations and how they are funding terrorism.

I am not so sure that is applicable with individual actors, though. I can say that the cases that I have been most familiar with, the Marathon bombings and a couple of other so-called lone-wolf attacks that have come before the committee. It was really behavioral abnormalities that really presented themselves. And in looking back, those were the things that sort of—would have raised the red flags, not—well, there was one case where the gentleman purchased a large knife. But even that was fairly—in retrospect, it looked serious. But when it happened, it probably wasn't.

Mr. Hughes, you appeared before the subcommittee when we talked about deradicalization. And some of those approaches, better communications with our folks in the Muslim community, mosques. We had a couple of cases where the imams said that an individual was acting out and was a security concern even within the mosque. Those type of reporting events are probably, in my mind, more applicable to the individual cases than trying to look at somebody's bank account and figure out what they are doing there. Are you of the mind that doing this, from a financial standpoint, is the best way to get at these individual actors and so-called lone-wolf terrorists? Anybody?

Mr. HUGHES. Let me jump in, and then maybe my colleagues can join in, too. I tend to believe that the financial reviews are probably going to be later on in the investigation. And so the case that you had mentioned, the young man in Massachusetts with the large knife, he was also talking to Junaid Hussain in Raqqa. So that is your red flag. And the issue becomes that he hadn't crossed the legal threshold. So there was a full investigation, but not enough to arrest. And so there is not a safety net to kind of veer these folks towards disengagement, deradicalization, the stuff Mr. Moreno talked about. There is no ability for the mosque in Boston to send those two folks somewhere else. And until we figure that out, that is actually the gaping hole. If you talk to the FBI, they are saying, "We don't have enough men and women to sit and run 8-hour shifts outside of a kid's house until they turn 18."

Mr. LYNCH. Right.

Mr. HUGHES. So I need to have different tools. Because I really want to focus on the guy that I am really worried about in Indiana, but I can't, because I know this guy in Boston is also concerning. So we have to provide some non-law-enforcement off-ramps to both law enforcement but also communities to build those partnerships. And you are absolutely right. In about 60 to 70 percent of the cases, depending on how you look at the studies, there is a bystander effect. People see something concerning but don't know what to do with it. And so they are watching this train wreck happen in slow motion. And we as a Federal Government, and we as community partners, have not provided any kind of tools and responsibilities for folks to deal with this.

Mr. LYNCH. Anybody else? Mr. Levitt? Dr. Levitt, I'm sorry.

Mr. LEVITT. That is fine. The only one who cares about the "Doctor" is my mother and—well, maybe she is watching. Thank you.

Mr. LYNCH. Well, that is important then.

Mr. LEVITT. From Massachusetts, she cares.

Mr. LYNCH. There you go.

Mr. LEVITT. Look, the first thing to say is that these are not mutually exclusive. The question isn't, do we do financial lines of inquiry or do we work with communities to try and off-ramp people who can be off-ramped, and do other things for people who can't, but work with communities who are there on the ground and have that—of course, we do all these different things. And in different cases, different tools will be applicable. I think what we are going to find is that in the case of lone or—because this bystander effect may be a little bit more known—wolves, what we are going to find is that financial information or intelligence is not going to be the panacea, but it will be a piece. It will plug a hole of something. It will help make a link. It will help contribute to a link chart. And while we would love for all of this to be as preemptive as possible, sometimes it won't be.

Mr. LYNCH. Right.

Mr. LEVITT. But the financial piece will almost always be really important in the post-blast of what happened. So if you look back—I was the government's expert witness in the Boston Marathon case. There is a financial piece there too. And that is always very important. So it is not a question of either-or. It is just leveraging all of them, and that is why I keep saying there is going to be a financial role in this, and there is more we can do. But at the end of the day, the true lone offender, whether from a foreign ideology or domestic ideology, and those are both terrorists who need to be dealt with, we have to use our entire tool kit. And money is not always going to be the strongest tool for some guy who is just taking a couple hundred dollars out of his or her bank account.

Chairman PEARCE. The gentleman's time has expired.

Mr. LYNCH. Thank you. And I yield back. I thank the chairman.

Chairman PEARCE. The Chair will now recognize the gentleman from Colorado, Mr. Tipton, for 5 minutes.

Mr. TIPTON. Thank you, Mr. Chairman. It's a complex issue, when we are talking about trying to be able to track anything from somebody who wants to be able to buy a knife to someone who wants to buy ammonium nitrate, how to be able to draw those to-

gether, a $50 purchase versus a $1,500 purchase, to be able to navigate that and to be able to identify them.

Mr. Levitt, when you were making your opening statement, said something that I thought was interesting, that the private sector has a lot of information if we give them greater insight. And I think you were just alluding to some of that. But what greater insight can we give to the private sector? What are going to be the triggers to be able to notify authorities of what to look for? And to a degree, something that we haven't hit an awful lot on, how do we still protect some of those privacy concerns?

Mr. LEVITT. The government is constantly looking at other information that is not available to the public and identifying trends. Some of those trends could be very useful; some of them will be less useful. Sometimes the government won't know what trend is useful until it speaks to the private sector, the people who are experts in banking and finance, and sees that they can add something to the conversation and demonstrate that, well, it is significant in this type of activity, but not in the other. If we are not having a really ongoing, regular, and robust public/private dialogue where the government is saying, here are things we are really looking at, we are really interested in, and the private sector is saying, okay, great, here is what we need more from you to be able to give you more effective SARs, then we are missing an opportunity.

I do think the U.K., as some of my fellow panelists have pointed out, has a new and interesting model. It may not be perfect for us. But the National Crime Agency oversees this effort to have an ongoing discussion and dialogue. Part of that would have to be, as I think it was Mr. Reynolds who said, combined with an effort to enable banks to talk to one another and convince them that it is in their interests as well. But I do think we need to push in that direction. Because at the end of the day, we are not talking about $1,500. We are talking about $50 or $4 or no dollars if you are taking something out of the kitchen drawer.

Mr. TIPTON. Thank you.

And you bring up an important point. Mr. Reynolds, maybe if you would speak on this a little bit more? You had stated that Barclays has maybe several thousand SARs reports, I think, and Bank of America may have a couple of hundred thousand. In terms of that communication between our financial institutions, is this proprietary? Is it something that is inhibiting that sort of conversation from going on? And, also, would you maybe speak a little bit to knowing your customer in terms of maybe not making that SAR simply because you know what that customer's business is like?

Mr. REYNOLDS. Absolutely. This actually is one of the restrictions that we labor under right now is institutions can't discuss SARs amongst themselves. So, for instance, if Barclays were to file a SAR on company A, and Bank of America had that same customer, we are actually not allowed, under domestic law, to discuss with Bank of America the fact that we filed a SAR, which is somewhat ironic, because probably the single strongest factor to suggest that a customer may be suspicious is the fact that you filed a SAR. And that is actually the one thing you can't talk to your peer institutions about. So it becomes a very, very delicate discussion where not only can you not mention a SAR, but you can't discuss anything that

would give an indication that you filed or did not file a SAR as to that customer. So these discussions are incredibly technical and very difficult to have, which makes it increasingly difficult, I think, to share, even when you are jointly working on a case. Under current guidance, you can't—for instance, let's say you have been working with Bank of America under 314(b) on a case, I can't say to Bank of America, I really think this is suspicious, I am going to file a SAR. That would be illegal. So that becomes very, very challenging to share information about that.

In terms of Know Your Customer (KYC), I think you are absolutely right. My view is that the bank which owns that customer really has the best opportunity to know what that customer looks like, what they should be doing, what they shouldn't be doing, and what looks suspicious. And so if I am able to speak to another institution who owns that customer and has the KYC for that customer, they can very often explain to me very quickly why what looks suspicious to me is actually not suspicious at all. And so then I am not wasting government time by filing a SAR, and I am not wasting quality analyst investigator time further investigating that case.

But, likewise, by getting KYC information from another institution, I can better understand that customer and I may actually determine that something that looks ordinary otherwise may actually be suspicious. So I absolutely agree with that. But I think that the sharing of KYC information, to the extent we can under Safe Harbor, is a very effective way to understand those customers better and determine whether their behavior is suspicious or not.

Chairman PEARCE. The gentleman's time has expired.

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

Chairman PEARCE. The Chair now recognizes Mrs. Maloney for 5 minutes.

Mrs. MALONEY. I thank the chairman for recognizing me, and I thank the chairman and the ranking member for holding this hearing on so-called lone-wolf terrorist attacks. It is particularly important to me since I have had some in my district, and, in fact, one about 6 months ago in the Chelsea area where a homemade bomb went off. It didn't kill anyone, but it injured many.

So, my question is on terrorism financing. It appears, according to press reports and other reports I have read, that terrorists are moving away from the financial system because of the oversight of the banks, of the know-your-customer requirements, and are going to bitcoins. There have been several published reports that criminals used bitcoins to finance the sale or purchase of sex trafficking victims and other illegal activities, and drugs, and guns, and other areas.

What is the penalty for using bitcoins in our financial system to finance criminal activity? Is there a sanction? Is there a fee? Is there a penalty that is placed on someone who uses bitcoins for dangerous purposes?

And, actually, Mr. Perlmutter, and Mr. Chairman, we should look at bitcoins. Because they are escalating forward in our economy as a way of financing crime, really terrible crimes.

But, what is the penalty for using bitcoins? What is your knowledge of bitcoins and financing crimes?

Mr. REYNOLDS. I can start on that. From the penalty perspective, ma'am, the penalty would be no different for using bitcoins as for using any other form of currency. So whether it is cash, wires, checks, pre-paid cards, or bitcoin, the penalties will all be the same. Bitcoin is considered currency under U.S. law. So if you laundered money or funded terrorism with bitcoin, the same penalties would be applicable as if you did it with U.S. dollars. I think the challenge is that bitcoin obviously presents a greater ability to remain anonymous, which, obviously, a wire transfer, a traditional wire transfer, would not. So I think that is the key difference between the two. But in terms of penalties, they would be the same.

Mrs. MALONEY. Talking about being anonymous, in the district that I represent, many criminals don't use the banking system, they just purchase real estate because there are no questions asked. They have $100 million, or $100,000, or whatever, and they go buy a piece of real estate, no questions asked. You sell it, and you have your money to do whatever you want.

And a number of us have worked on legislation to bring an accounting for what we call beneficial ownership, that people should have to reveal the true beneficial ownership. What is your feeling on that? Would that be a source of combating terrorism financing?

Mr. REYNOLDS. I will start again. I am a strong supporter of the legislation. So I would strongly encourage passing it. I think it would be tremendously helpful, both to law enforcement—looking from my law enforcement background, I know it would have been tremendously useful to have it when I was a prosecutor—and from a financial institution's perspective. It would also be incredibly valuable for the work that we do.

Mrs. MALONEY. And the The Committee on Foreign Investment in the United States (CFIUS) bill which looks at foreign investment from the lens of whether or not it is a threat to our national security, how do you feel that law is operating? Do you think it needs to be strengthened? It is a tool to combat terrorism, and financing, and financial terrorism in other areas, the CFIUS bill?

Mr. LEVITT. I haven't thought about that question for this hearing because it seems to me it is a slightly different issue. I think of CFIUS—and I worked in CFIUS at one point in government. It is incredibly important. But traditionally, actually, it is something different than terrorism. There are sometimes terrorism pieces to it. But, overall, it is about larger issues. And certainly, in terms of the lone offender and the small scale, I don't know of any case that has come anywhere the size of something that would be real estate purchases or FIS. That is a much larger, broader terror finance question.

Mrs. MALONEY. And do you think you could just look at the transactions in a lone wolf, in a bank, and suspect, this lone wolf didn't—a pressure cooker, where he put everything in there and created a pressure cooker bomb. But purchasing these items would not set off any red lights. And so how can we get more red lights that would help us track these lone wolves?

Mr. HUGHES. There are some programs. The FBI runs InfraGard, which works with private companies to essentially set up trip wires to alert folks. So, a good case, Najibullah Zazi buys a bunch of materials in Denver to build a bomb, and the local beauty salon, calls

the FBI and says, I am a little worried about this guy. And so to the extent we can kind of build up those relationships and get that type of public/private partnership going a little bit more, I think it would be useful.

Mrs. MALONEY. Thank you. My time is up.

Chairman PEARCE. The gentlelady's time has expired.

The Chair now recognizes the gentleman from Texas, Mr. Williams, for 5 minutes.

Mr. WILLIAMS. Thank you, Mr. Chairman. And I thank all of you for your testimony today. We appreciate it greatly.

I will get right into the questioning.

Dr. Levitt, terrorist financing has shifted dramatically over the years, due in large part to the increased use of social media that we talked about. In your opinion, where do you think the future of terrorist financing lies? And what measures can we take to combat it?

Mr. LEVITT. So, in my experience, terror financing is a non static issue. It is constantly changing. It is changing based on the actions we take to combat it and to restrict the environment in which illicit actors can finance their behaviors and also based on what opportunities present themselves. And that means it is not always moving in one direction. When the terror finance tracking program was exposed several years ago, we saw that—we worried that maybe some terrorists would stop using the formal banking sector. They still did. But they also went back old school and they used cash couriers.

If you look at the U.N. Security Council's latest report on the Islamic State, they, too, have member states reporting that today, as the Islamic State is on its back heels, it is increasingly using cash couriers. And so, we have to constantly assess and reassess, figure out which tools are going to be most effective. I think that is part of the conversation that could then be had, or be better had, between the public and private sectors, not just what is the latest, sexiest thing, but where on that spectrum are things right now at any given time.

Mr. WILLIAMS. Good.

Mr. Reynolds, from your experience in both the public and now the private sector, can you explain how the government can fully investigate and exploit these terrorist networks while ensuring that the American citizen's right to privacy is protected?

Mr. REYNOLDS. Yes. I think the key to that, again, is to the extent that we coordinate between the public and the private sector, the way that I always viewed it in the government is that the public sector tends to have a very good horizontal view. But they don't always have very good tremendous depth on any particular customer, or certainly to their finances, whereas financial institutions have very good depth. So they have very good vertical, but they lack the horizontal that the public sector has. I think that if, in a very targeted way, you can bring together the threats that the public sector has identified, and bring those to the private sector, the private sector can then work to expand out those networks and tell the public sector what it doesn't know.

There were certainly cases that I was involved with over time where we may have thought we had the ring leader of a par-

ticular—whether it be terrorism financing or whether it be money laundering. But we thought we had the ring leader. We brought that to a financial institution who then came back to us and said, actually, you have a mid-level person, here is this whole other level to the organization that you didn't know about, but we were able to determine that they are all connected because, for example, they used the same device ID, which meant they used the same iPad or the same computer to access bank accounts.

So I think that is just one example of where, if you combine those two pieces of information, I think it both focuses the efforts so, again, we are not sort of trolling among millions of customers looking for bad people. We are really focused on the individuals and the information that we know credibly has some link to potentially bad activity, and it will allow us to then, hopefully, move resources away from this sort of lower value intelligence activities and really focus them on the higher value, which I think, in my view at least, enhances privacy.

Mr. WILLIAMS. Good. Thank you.

Mr. Moreno, can you explain how law enforcement and intelligence agencies share information? And do you believe that the government is proficient in this task or are there specific areas of improvement that you would recommend? If so, what would they be?

Mr. MORENO. Sir, I am normally not a person to say, throw money at a problem and that will fix it. But, as a former prosecutor, I can tell you that I think we have fantastic techniques. We have fantastic people. We have great statutes. However, additional resources in these areas would always be welcomed.

So, for example, the SAR review process, I can say from my experience that financial institutions do a great job at investing in technology and issuing SARs. But there are not always enough folks to review them. So when they are reviewed, it could be months afterwards. So in terms of thorough review of SARs and rapid response to the suspicions that are arisen, we can always use more people. Joint terrorism task forces are a great way to integrate Federal, State and local law enforcement to share information. But they are also often short-staffed. So in this area, this is a place where I would say we have a lot of the right tools already. What we sometimes lack is the resources to implement them.

Mr. WILLIAMS. Mr. Reynolds, quickly, we have a small amount of time here, is there another country that is surpassing the United States in their ability to target and neutralize terrorist financing?

Mr. REYNOLDS. I would not say surpassing, but I think the U.K. is equivalent to it. And I think the U.K. has some very exciting now programs and pilots that they are implementing that I would suggest the U.S. should look strongly at implementing as well.

Chairman PEARCE. The gentleman's time has expired.

Mr. WILLIAMS. Thank you, again. I yield my time back.

Chairman PEARCE. And the Chair now recognizes the gentleman from Minnesota, Mr. Emmer, for 5 minutes.

Mr. EMMER. Thank you, Mr. Chairman.

Chairman PEARCE. And just be advised we have votes coming up. We are going to try to get all the questions in before the votes.

Mr. EMMER. And thanks to the panel for being here today.

Mr. Moreno, and I am probably going to be too general, but as we talk about what ways we can address the changing threat landscape, if a terrorist can cause mass destruction casualties with just a few thousand dollars, I think you would agree that we can't just lower the currency transaction report requirement. What, in addition—and maybe you have covered this several times today—but can you succinctly give me what, in addition to that, could we do to—is it the algorithms that we heard earlier that Mr. Reynolds was talking about? How are we going to get ahold of this thing?

Mr. MORENO. Yes, sir. I don't think that changing the limits upward or downward is an easy fix. I think, if anything, you might get more reports but not necessarily better reports. I think we can downscale what we do, I think, to try to better focus on transactions that are suspicious even if they are at the four-figure, or possibly even three-figure level.

Mr. EMMER. And, again, putting in algorithms that identify specific characteristics of a transaction?

Mr. MORENO. Yes, sir. There is always going to be a manual review process. But that should be coupled and in parallel with new technologies, algorithms, artificial intelligence, to flag these transactions. And I know that banks are already investing in those technologies. But I think we can always do more to encourage that.

Mr. EMMER. And, Mr. Reynolds, I wanted to go next to how can we leverage technology, specifically following up on what Mr. Moreno referred to, be it artificial analysis, the data analytics, which you have talked about quite a bit, or something else to make these suspicious activity reports more valuable? And I see that—and I should have thought about this before the hearing when I was preparing. But when Mr. Moreno said we have to have the bodies to review them too, we forget that is a huge piece on the back end of it. But just how can we leverage this technology even better?

Mr. REYNOLDS. I am a huge believer in the big data and technology. But I agree with you that it really has to be a combination of human effort and technology. Technology will only get you so far. I think the first step is to really use technology to look for outliers. Because, ultimately, a lot of these folks are trying to look like everyone else. That is sort of the point of what they are trying to do. But, fundamentally, they aren't like everyone else. And so there are, at times, telltale signs.

Now, it may be that we can't tell the difference without the law enforcement information. In some cases, we can. And so I think what we need to do is leverage as much as we can, big data, to hold together and to recognize that when the BSA system was formed 40 years ago now, we were paper, no cell phones, no internet. Now we are high-speed wire transactions, internet, and paper money is, in many ways, not king anymore. So I think recognizing that and leveraging the data abilities we have is key. But then I agree with you. Then I think what we need to do is try to take those precious resources we have, which are the human resources, and I think really focus them on the most important national security issues. I think right now we are sort of spread across the whole waterfront. In my view, I think what would be better is to really focus

them on the most serious threats and not spread them against what I would consider to be the less serious threat.

Mr. EMMER. And I was going to move on to something else. But what would you define as the most serious threats?

Mr. REYNOLDS. I think when we are—I would expect, in many cases, law enforcement would ultimately provide that to us, and they would tell the institutions what are the most serious threats. But I think, from my perspective, looking at things like terrorism, human trafficking, serious money laundering, serious fraud, cyber activities, those would be the areas where I would most like to focus resources. And I think if we did that, I think that we would provide more valuable intelligence on these national security issues.

Mr. EMMER. That is helpful. When you said it, I was thinking in terms of size and scope as opposed to the actual—what the issue was.

Mr. Levitt, I want to go back to the private sector. Can you talk some more about how we can get more people in the private sector to first recognize that what they are looking at is not normal? I think they do. I typically see things that are out of the ordinary. But we still, I think, are hesitant to raise the red flag and call authorities and say, there is something you need to look at here. Are there some other things we should be doing to try and encourage people in the private sector to notice or be observant of things out of the ordinary and report them?

Mr. LEVITT. I guess I challenge the premise. I think the banks are actually quite good at this, and they are quite eager to be good. If anything, there has been over-reporting of SARs to be overly cautious. I think the biggest issue is that if you have—in the truest lone wolf, you will not have outliers. You will not have telltale signs. There will be nothing to look at unless law enforcement, for some other investigative angle, happens to know that there is something going on. And then the bank can say, well, wait a minute, this guy is only taking out $100 every 2 weeks, but he has never done that before. And suddenly $100 is the issue, not—

Mr. EMMER. I see my time has run out. But I would point out, I am thinking more of this testimony earlier. And I thought it was you talking about mental health issues, they exhibit things beforehand, typically, and we have to figure out a way to observe that and report it. This is what we had reported in the St. Cloud stabbing. There were mental health concerns before this incident. And I see my time has expired.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes the gentleman from Ohio, Mr. Davidson, for 5 minutes.

Mr. DAVIDSON. Thank you, Mr. Chairman. And thank you to our guests. I really appreciate your testimony. And thanks for your expertise.

Mr. Reynolds, you work in the private sector for a financial institution. And I am just curious. Barclays is publicly traded, right? I haven't personally looked at the annual report closely enough to know, but how much do you actually spend on reporting for suspicious activity? Just how much of that annual budget goes to this?

Mr. REYNOLDS. Honestly, I don't know the exact figure. I know that it is fairly substantial in terms of staff. But I couldn't give you an exact figure. I apologize.

Mr. DAVIDSON. Okay. That is all right. And I guess my question is, given that it is a substantial figure, it is not an insignificant figure that is down in the footnotes as rounded out, but it may be summed up in the other operating costs somewhere, how much revenue does this generate for Barclays?

Mr. REYNOLDS. Zero.

Mr. DAVIDSON. Zero.

Okay. So my question is, when we listen to these part B discussions about, frankly, some of the financial institutions, anxious to start collaborating with one another and sharing information across each other, for a portion of their bank that derives zero revenue for the bank, why is it that banks are so ready to engage in law enforcement activity that generates nothing of value for the company? I really appreciate that you want to help with national security. I guess my question is, why?

Mr. REYNOLDS. I think it is fairly simple: I think the bank wants to do the right thing. I think that certainly the bank does not want to bank terrorists. It doesn't want to bank money launderers. It doesn't want to bank human traffickers. And so, certainly, regardless of law enforcement impact, the bank wouldn't want these individuals in their bank anyway. So I think the bank would spend money and dedicate resources to make sure that we don't have those sorts of customers. I think there is an attendant law enforcement benefit as well. But I think certainly just from wanting to be a good corporate citizen and doing the right thing, the bank doesn't want to bank these people.

Mr. DAVIDSON. Okay. So, defensively. Fundamentally, you have something to gain because your bank would have a bad reputation if you became known as the destination for human trafficking financing, for example. So there is a defensive interest in it for the banks. I guess when you look at it, you say, all right, Know Your Customer, know these activities, and you go beyond, maybe open this up to Dr. Levitt, Mr. Moreno, we have spent a fair bit of time on privacy. And I guess my question is, we are down to the point where we are talking about tracking knife purchases and using big data. It is already bad enough that you can't fly with a knife, certain size knives, you go, okay. Nail clippers, maybe. We got past some of that. Things like this.

At some point, does owning a knife need to be on a suspicious report? If I bought a set of knives for the kitchen, do we need to investigate all those? I guess, you see how far down we are into the dialogue. And you have private sector folks who are going to spend more and more, add two or three floors to the building to focus on this, not to mention all the resources we devote to doing this, and in the balance is privacy for people. How do we make sure that we can do—well, we can always do more, but in this case this happened. I guess, how—when the Federal Government operated the Post Office, as we do still today, and there weren't tons of rivals, the government actually still had possession of the data. And they sent it from point A to point B, and without a warrant, they didn't open it up. Lots of things could have been in the mail. But, offi-

cially, we didn't search every package. As far as I know, FedEx doesn't open every package that gets sent. Yet, if it is financial data, fundamentally you don't have anywhere near the same safeguards. So, I guess, how do we get that balance right?

Mr. LEVITT. I guess I would just say, in a nutshell, that you ultimately do have, pretty much, that same protection. We are not looking at every transaction. We couldn't look at every transaction. Even if we wanted to, and we don't, no one is looking at every knife purchase. The whole point is to be focusing only on those cases where, through a variety of different investigative tools, whether it is financial, or the community coming forward, or intelligence, or whatever it is that there is reason to believe to have suspicion that something is off. And we have clear requirements for what hits that threshold. And as Mr. Hughes talked about, sometimes we can't hit the threshold on terrorism, and so we do something else. You don't want to overreact and say, now people are using knives, so knives are the big problem. They are not. But you also want to recognize that because a knife is inexpensive, you can't just assume that the kind of things you had put in place to notice something just under a $10,000 threshold is going to catch this.

Chairman PEARCE. The gentleman's time has expired.

Mr. DAVIDSON. My time has expired, so I yield back.

Chairman PEARCE. The gentleman's time has expired.

I now recognize the gentleman from Arkansas, Mr. Hill.

Mr. HILL. I thank the chairman and I thank the ranking member. This is an important hearing. Thanks for having it. Little Rock had its own situation with a lone wolf back in June of 2009 when a dry cleaner's worker from Memphis who was opening up a new location in Little Rock had become radicalized, and at 10 o'clock in the morning he went up and shot, at point-blank range, two Army recruiters there, killing one of them, Andy Long, and wounding my friend, Private Quinton Ezeagwula. It was a tragic deal. So I appreciate having this hearing. And my predecessor, Tim Griffin, and I worked hard for Quinton and Andy to earn the Purple Heart for that tragedy.

I was just reading a book during August, "In the Skin of a Jihadist," which is a book about radicalization in France and just how few dollars are used in this arena. So I am very sensitive to this issue of a lone wolf. And having seen it in reality in Arkansas, and then reading about just how modest the financing is in this arena, and just how prevalent it has become in Europe. So for banks of all sizes, Mr. Reynolds, I am just curious, if there is off-the-shelf software for their operation, instead of the kind of expense that Barclays or Bank of America would have to go to, that integrates data to make filing a SAR a more sophisticated activity, rather than just the bank transaction that goes across the counter or through the wire room, where a bank of any size can note disposable cell phone purchases, and tickets purchased to certain countries on the credit card, if, in fact, they are a credit card issuer.

Tell me how a bank could really enhance their SAR filing from the obvious. Because that is one of the things. We file SARs in banks just based on things that we observe. We don't actually go hunting for SARs. Perhaps Barclays does. So talk to me, the dif-

ference, but seeing something that is suspicious, and then I have a staff who is hunting through all my customers looking for something that is suspicious.

Mr. REYNOLDS. Sure. There are really two ways to attack the problem. Some institutions just employ one, and some institutions employ both. To your point about commercially available solutions, there are a great number of commercially available solutions that can range from solutions for very, very small banks. So it is a solution that is tailored for a small community bank that will look for various red flag indicators, and will ultimately push those to the relevant AML officer. Very often, a small community bank, there isn't hordes of people. There is an AML officer, and that is the person who—

Mr. HILL. Who does many jobs.

Mr. REYNOLDS. —wears many, many hats, and who works very hard in those institutions. That software is incredibly useful to them because it does help them identify some of those transactions.

Mr. HILL. Does it bring in non-bank data, though? Does it integrate non-bank data at all?

Mr. REYNOLDS. So for some of the smaller solutions, it typically would not. There are other commercially available solutions that will, for instance, bring in negative news on customers. So if there is publicly available news on your customers, it will bring that in. There are some solutions that will go out and look on the web to see if there is derogatory information about customers you may have that will bring that in as well.

The second set of solutions that you typically have for institutions are what I refer to as sort of advanced analytics, a lot of different great companies that are doing some fantastic work in this area. And what those solutions are is to your point of institutions proactively looking for risks within the institution. So that is where, again, they are not looking at individual customers, per se, until they find something. But what they are doing is looking across the data to look for outliers to look for things that just don't make sense for their customer set. And then they focus analysts in on that particular issue. Most large institutions, in my experience, do both. Because given their data sets, just having sort of a standard platform that is looking for red flags is good, and that is what is required. But most banks invest above and beyond what is required and do the proactive analytics as well. Smaller institutions, I think, probably stick to the former. But, again, because they are smaller, I don't know that proactive analytics for a smaller institution would be quite as useful.

Mr. HILL. Quickly, you were talking about Know Your Customer, sharing that information, you do acknowledge that banks can call another bank and say: Are you satisfied with your Know-Your-Customer information about customer X? That is permitted under the law, isn't it?

Mr. REYNOLDS. Absolutely. That is permitted under Section 314(b).

Mr. HILL. Thank you very much.

Chairman PEARCE. The gentleman's time has expired.

I would like to thank each one of our witnesses for your testimony today. You have been very gracious with your time and your answers.

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. This hearing is adjourned.

[Whereupon, at 3:54 p.m., the hearing was adjourned.]

A P P E N D I X

September 6, 2017

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

Low Cost, High Impact: Combatting the Financing of Lone-Wolf and Small-Scale Terrorist Attacks

Written Testimony of:
Seamus Hughes
Deputy Director, Program on Extremism
The George Washington University
Before the U.S. House of Representatives Financial Services Committee
September 6, 2017

Chairman, Ranking Member, and distinguished Members of the Committee, it is a privilege to be invited to speak on the threat of financing of extremism in the United States and the efforts undertaken to prevent it.

The Current Threat Picture

Extremism inspired by jihadist groups like al-Qaeda and the Islamic State (IS) remains a potent threat to the United States. Since the announcement by the Islamic State of the so-called Caliphate in June 2014, GW's Program on Extremism has identified 63 "successful" attacks in Europe and North America. France has experienced the highest number of attacks, followed closely, and perhaps surprisingly, by the United States.[1] Attacks in the United States tend to be significantly less structured and spontaneous than those in Europe, even though some of them (Orlando, San Bernardino) have been no less deadly.

According to law enforcement, at least 250 U.S. persons have traveled or attempted to travel to join extremist groups in Iraq and Syria.[2] Since March 2014, 133 individuals have been charged with terrorism-related activities in connection with IS. There have been arrest in 28 states and the District of Columbia. The average age of charged individuals was 28. While about 30% were accused of plotting domestic terror attacks, nearly half were accused of traveling or attempting to travel abroad.

It is a 'homegrown' phenomenon in the truest sense of the word. The vast majority of those arrested are American citizens or legal permanent residents. While violent plots understandably often garner the attention of policymakers, media, and academics, a broad swath of cases demonstrates the enduring relevance of finance-related activity by jihadists in the West.

At the outset, I note that although my testimony primarily focuses on IS-related extremism, it includes a brief examination of other forms of violent extremism which certainly pose a threat to national security. Historically, other foreign terrorist organizations (FTOs), including Hezbollah and Hamas, have succeeded in establishing extensive financial networks in the U.S, and used their network to spread their message and ideology in the United States. [3] The U.S. Government has also repeatedly warned about the threat posed by other extremist groups. To elucidate, the FBI and DHS issued a Joint Intelligence Bulletin last May, in which they assessed that "lone actors and small cells within the white supremacist extremist movement likely will continue to pose a threat of lethal violence within the next year."[4] Unfortunately, when compared to the surfeit of analyses that comprehensively assess the financing of jihadist actors in the United States, there are very few reviews that document how other extremist groups fund their activities.

---

[1] Vidino, Lorenzo, Francesco Marone, and Eva Entenmann. 2017. "Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West." Milan, Italy: Joint Program on Extremism, ICCT-The Hague, ISPI Report. https://extremism.gwu.edu/sites/extremism.gwu.edu/files/FearThyNeighbor%20RadicalizationandJihadistAttacksintheWest.pdf

[2] Schmitt, Eric, and Somini Sengupta. 2015. "Thousands Enter Syria to Join ISIS Despite Global Efforts." *The New York Times*, September 26, sec. Middle East.

[3] US v. Holy Land Foundation for Relief and Development, et al., Richardson, Texas.

[4] "White Supremacist Extremism Poses Persistent Threat of Lethal Violence". 2017. DHS-FBI Joint Intelligence Bulletin, May 10.

Financing of the extremist's cause in the U.S. varies considerably, ranging from individuals using crypto-currencies online to coordinated initiatives supporting actors abroad. To better understand the current picture, it is crucial to examine the myriad ways in which terrorist financing regulations and how they have shaped the evolution, or perhaps devolution, of modern terrorist financing in America.

Contemporary Financial Activity

Emerging in the post 9/11 era, IS relied upon creative and innovative economic means to fund its attacks within the United States. Departing from the approach used by al-Qaeda, IS has been more self-sufficient, "deriving most of its income from oil sales and criminal enterprises, as well as from money taken through taxes and fees."[5]

To complement airstrikes on IS' assets, including military hardware and oil fields, the U.S.-led coalition implemented measures to weaken the organization's financial networks. Sanctions by the Department of Treasury, which targeted financiers and relevant businesses, seemingly helped chip away at the group's resources on the ground in Iraq and Syria. Ultimately, the factors that currently strain IS' finances pertain to degradation caused by air strikes and territorial losses.

In the fifteen-plus years after President Bush signed Executive Order 13224, which prohibits financial transactions with suspected terrorists, several governments worldwide have implemented a variety of methods to counter networked financing by terrorists. Relying predominantly on asset freezes, blacklists, sanctions, and intensive financial monitoring, the approach has resulted in a diminishing exodus of terrorist networks from the international financial system. At first glance, this appears to be a favorable outcome, but further analysis shows that this approach yields mixed results.

Despite the stark reduction in substantive financial transfers between terrorist organizations and their adherents, events from the same fifteen-year period demonstrate how violent extremists remain capable of funding and coordinating deadly and public attacks. A 2017 study by the International Centre for the Study of Radicalisation claims three factors are largely to blame for the limitation of counter-financing strategies: 1) terrorist financing has adapted to post-9/11 counter-financing strategies, especially blacklists and asset freezes; 2) there is no archetypal 'terrorism financing method,' and perhaps the most salient; 3) the modern terrorist needs little to no money to carry out the attack.

In sum, attempting to find a terrorism financing plot is similar to the proverbial "needle in the haystack": modern terrorist financing has gone underground or can be disguised easily, utilizes a variety of methods, and relies on many small transfers rather than a few large ones.[6]

Even before the advent of the current counter-financing programs, terrorist networks informally generated income and financed their activities through unofficial means that governments or international agencies

[5] Warrick, Joby. 2016. "Inside the economic war against the Islamic State." *The Washington Post.* December 31.
[6] Neumann, Peter (2017). Don't Follow the Money: The Problem with the War on Terrorist Financing". *Foreign Affairs* 94 (4).

found difficult to regulate by. Most notably, many of the precursors of modern terrorist organizations were forged in areas where the vast majority of the population did not have bank accounts and wire transfers. In these cash-based economies, tracing the "paper trail" is particularly challenging even in areas with developed market economies. Banks undertake and process thousands of complex financial transactions each day. It is hard to ascertain which of these transactions are financing terrorism especially when the identities of the account owners remain unknown. Mullah Omar, Usama bin Laden or Abu Bakr al-Baghdadi, for example, would be unlikely to open bank accounts in their own names. Use of third parties or a middle-man creates an obfuscation that banks and intelligence services must look at the method of financing rather than the financiers themselves.[7] That no two terrorist groups generate income in the same way makes law enforcement's job even harder. Each organization must account for their base of adherents, material connections, and geographic backdrop, and one needs different expertise to suss out the perpetrator.

A review of financing of IS-related activities reveals the modern-day financing of terrorism. A teenager in Virginia crafted an online manual on how to send money via Bitcoin to IS while a husband-wife team in Missouri raised money the old-fashioned way by fund raising cash from several members of the Bosnian diaspora. Another Virginia man bought gift cards and messaged their codes to an individual who he believed to be an IS fighter who was to use them to create encrypted online accounts. Beyond IS supporters in America, terrorists worldwide have used a variety of enterprises -- from ivory poaching to oil trading, antique theft to growing heroin.

But, counter-financing programs will struggle for an overarching reason: the "new normal" of terrorist plots is the low-budget attack. Successful terrorist attacks are now being carried out with instrumentalities that are part of our everyday life: a knife or a van. In these "lone wolf" or the errant jihadist types of attacks, the incurred costs are low such as buying the weapon or renting a car. The cost for such instrumentality is low -- a few hundred U.S. dollars.

Travel to join terrorist groups overseas, or financing an individual's journey, is a more expensive form of financial material support, but even then, the cost of a plane ticket is less than a few thousand dollars. In contemporary instances where terrorist attacks or travel are externally financed, the amount of money that must be transferred to fund the scheme fully may not necessarily cross the radar of most monitoring operations.

IS Case Studies

Case studies provide an insight into the contemporary means used by terrorists to finance their attacks in America. One such method scheme is where an individual or group of people crowd-source money for another who has already gone overseas to join IS in its controlled territories. This method of financing terror dates back to pre-IS terrorism financing cases, and comes closest to the meaning of providing material support to a foreign terrorist organization.

---

[7]Neumann, Peter (2017). Don't Follow the Money: The Problem with the War on Terrorist Financing". *Foreign Affairs* 95 (4).

The husband-wife team from Missouri illustrates this type of financing. Ramiz Hodzic and Sedina Unkic Hodzic raised money the old-fashioned way – reaching out to their contacts in the Bosnian diaspora community and receiving the money through Western Union, PayPal and wire transfers. Ramiz and Sedina then sent the funds they had collected to a mid-level Bosnian-American IS commander in Syria.[8] After pooling the money from those who are now their four co-conspirators, the Hodzics also bought military gear and supplies, and sent them to intermediaries in Turkey, Saudi Arabia, and Bosnia and Herzegovina.[9] Some members of this group have defended their actions by claiming that the money was for charitable purposes, or that the money was sent to support individuals from the diaspora abroad-instantly recognizable as built-in defenses for this type of funding scheme.[10] It remains to be seen if those defenses will prevail at trial.

At times, it is the IS operative overseas who is the instigator and convinces the lone individual to raise money stateside. Illustrative of such a scheme is the case of Aaron Daniels, a 20-year-old Ohio man, and Mohammed Bailor Jalloh, a former Virginia National Guardsman. Both men pleaded guilty to charges of providing material support as they had sent money to individuals that they believed were vetted by Abu Sa'ad Sudani, a known IS external operations planner who was later killed in a 2016 coalition airstrike.[11] In a more innovative example, another Virginia resident, Haris Qamar, purchased gift cards and sent the codes to an individual that he believed to be an IS operative overseas.[12]

The next type of financing is seen when individuals or groups garner resources so as to finance a person's travel abroad to join IS. Illustrative of such a financing scheme is a case stemming out of the Eastern District of New York with players from other states including Illinois and New Jersey.

Beginning in January 2015, Abror Habibov, a 30-year-old Uzbek citizen living in Brooklyn, New York, financially facilitated Abdurasul Juraboev and Akhror Saidakhmetov's attempts to join IS.[13] Habibov owned several technology repair kiosks in malls around the country and was Saidakhmetov's employer.[14] He provided funds to Saidakhmetov and Juraboev to purchase plane tickets, first in the form of payment in advance for Saidakhmetov's work, and later as a lump cash payment of $500 for the plane ticket.[15] Then, Habibov fundraised money with Akmal Zakirov, Dilkhayot Kasimov, Azizjon Rakhmatov, and Dilshod Khusanov so that Saidakhmetov and Juraboev would have access to money to buy weapons after they arrived in Syria.[16]

---

[8] *USA v. Ramiz Ziyad Hodzic, et. al.* Indictment (2015).
[9] *USA v. Ramiz Ziyad Hodzic, et. al.* Indictment (2015).
[10] *USA v. Ramiz Ziyad Hodzic, et. al.* Defendants' Joint Motion to Dismiss Counts I and III (2017).
[11] *USA v. Aaron Daniels*, Affidavit in Support of an Application for a Criminal Complaint and Arrest Warrant (2016); USA v. Mohamed Bailor Jalloh, Affidavit in Support of a Criminal Complaint (2016).
[12] *USA v. Mohamed Bailor Jalloh*, Affidavit in Support of a Criminal Complaint (2016); USA v. Haris Qamar, Criminal Complaint (2016).
[13] *USA v. Abdurasul Hasanovich Juraboev, et al.* Complaint and Affidavit of Arrest Warrant (2015).
[14] *USA v. Abdurasul Hasanovich Juraboev, et al.* Complaint and Affidavit of Arrest Warrant (2015).
[15] *USA v. Abdurasul Hasanovich Juraboev, et al.* Complaint and Affidavit of Arrest Warrant (2015).
[16] *USA v. Abdurasul Hasanovich Juraboev, et al.* Complaint and Affidavit of Arrest Warrant (2015).

At times, the financing of the plot is so intricate and separate from the act of material support that prosecutors are able to bring additional charges against the defendant. Such was the case when prosecutors charged Nader Elhuzayel with material support and financial fraud. Elhuzayel was convicted for attempting to join IS in Syria, along with 26 counts of bank fraud. To fund his travel to the Middle East, Elhuzayel deposited stolen checks into accounts at three different banks, then withdrew the money at various branches and ATMs.[17] When the banks discovered the fraud and closed Elhuzayel's accounts, he was unthwarted.[18] Elhuzayel turned to his friend and co-conspirator Muhanad Badawi. Badawi then purchased a plane ticket to Turkey for Elhuzayel, using his federal financial aid debit card. Elhuzayel and Badawi were both arrested when Elhuzayel attempted to board his flight. Badawi was also charged with material support to a terrorist organization, and one count of federal financial aid fraud.[19]

Misappropriating federal funds to finance terror travel is on the rise. Three Minnesota men, linked by a broader effort to travel to IS-controlled territory, engaged in financial fraud to achieve that aim. Guled Omar, for example, "withdrew $5,000 cash from his federal educational financial aid debit card" before his first attempt at leaving for IS which failed. .[20] Omar's second attempt to travel to IS-controlled territory led to his arrest, and eventually to his conviction for attempting to provide material support to a foreign terrorist organization and attempted federal financial aid fraud.[21]

Mr. Omar's co-defendants Hanad Musse and Hamza Ahmed were similarly found guilty for attempting to provide material support and financial aid fraud for their respective efforts to finance their travel to IS-controlled territory by fraudulent means.[22]

In some cases, public formal charges are never filed but the story reveals the methodology used to finance the act of terrorism, In an interview with *BuzzFeed News*, Hoda Muthana, a woman who migrated to IS-controlled territory in 2015, admitted to using her college tuition to pay for her plane ticket to join IS .[23] Muthana explained, "I signed up for classes and withdrew [from] them immediately so I could get a check back."[24] The precise logistics and legality of this transaction remains unknown, as law enforcement filed no publicly-available charges, but this method of terrorism-related financing demonstrates how difficult it is to detect and disrupt rudimentary plots.

---

[17] DOJ Press Release, Two California Men Convicted of Conspiring to Join ISIL, June 21, 2016.
[18] Suduck, Joshua, "2 Anaheim Men Found Guilty of Trying to Help the Islamic State." *Orange County Register*, June 22, 2016.
[19] DOJ Press Release, Two California Men Convicted of Conspiring to Join ISIL, June 21, 2016.
[20] *USA v. Mohamed Farah, et. al.* Criminal Complaint and Affidavit (2015), p.15.
[21] DOJ Press Release, Federal Jury Convicts Three Minnesota Men for Conspiring to Join ISIL and Commit Murder in Syria, November 15, 2016.
[22] DOJ Press Release, Three More Minnesota Men Sentenced to Providing Material Support to IS, November 15, 2016.
[23] Hall, Ellie. 2017. "Gone Girl: An Interview With An American In ISIS." *BuzzFeed.* Accessed August 25. https://www.buzzfeed.com/ellievhall/gone-girl-an-interview-with-an-american-in-isis.
[24] Hall, Ellie. 2017. "Gone Girl: An Interview With An American In ISIS." *BuzzFeed.* Accessed August 25. https://www.buzzfeed.com/ellievhall/gone-girl-an-interview-with-an-american-in-isis.

Finally, in the case of three teenagers from Denver, Colorado, who attempted to travel to IS-controlled territory in 2014, a pair of sisters stole $2,000 from their father along with their passports.[25] At this time, authorities have not filed any charges likely because the teens were minors.[26] Ultimately, however, this type of theft does not amount to a federal offense until resources are used in support of a terrorist organization. This technicality makes it especially difficult for lawmakers to develop approaches that could counter this level of activity.

Violent Far Right-Wing and Anti-Government Case Studies

There are similarities and differences between the financing schemes utilized by violent, far-right extremists and their jihadist counterparts. One major difference is that financing of designated foreign terrorist organizations like IS, Al Qaeda, or Hezbollah is an *ipso facto* criminal offense under the material support statute (18 U.S.C. § 2339), whereas there is no statutory "designation" for domestic extremist groups. Thus, in order to prosecute such financing, the government must either prove that a) the funding was directly intended to commission a crime or b) the funds were obtained through criminal activity. The result is that violent, far-right groups are simply not under the same pressure to disguise their funding as FTOs. Nevertheless, the violent far right-wing groups have also used similar methods to finance their criminal activities. Funds used to promote and execute violent attacks place the groups under the same scrutiny and thus force them to conceal their financing methodology.

For decades, violent, far-right extremist networks in the United States have utilized the proceeds from illegal operations to finance their activities. In the mid-1980s, an offshoot group of the Aryan Nations, colloquially known as "The Order," conducted a series of robberies on Brinks armored vehicles. They laundered the nearly $4.1 million they made and used it to fund and arm various white nationalist groups.[27] Similarly, individuals tied to Timothy McVeigh, the perpetrator of the 1995 Oklahoma City bombing, raised funds for their cause through robbery: a group called the Aryan Republican Army committed a series of 22 bank stick-ups throughout the Midwest to finance an "all-out race war."[28]

More recently, however, members of anti-government extremist organizations have turned to more convoluted plots to finance their groups. In 2011, Army Private Isaac Aguigui killed his pregnant wife for the insurance money to help fund his anti-government militia. Aguigui received $500,000 from her insurance policy. Aguigui then purchased $30,000 worth of guns and ammunitions for his militia group, FEAR (Forever Enduring Always Ready).[29]

---

[25] Arapahoe County Sheriff's Office, Offense Report, October 21, 2014.
[26] Temple-Raston, Dina. 2014. "ISIS Used Predatory Tools and Tactics To Convince U.S. Teens to Join," *NPR News.*
[27] Canter, David V. 2009. The Faces of Terrorism: Multidisciplinary Perspectives. John Wiley & Sons. p.173
[28] Perliger, Arie. 2013. "Challengers from the Sidelines: Understanding America's Violent Far-Right." West Point, NY: Combating Terrorism Center at West Point. https://ctc.usma.edu/posts/challengers-from-the-sidelines-understanding-americas-violent-far-right.
[29] Crimsider Staff, "Army private convicted of murdering pregnant wife," *CBS News,* March 24, 2014.

In 2013, Michael Lee Fullmore planned to establish a violent offshoot of the Georgia Knight Riders of the Ku Klux Klan. To fund his endeavor, Fullmore sold firearms to convicted felons. Fullmore was arrested by the FBI after he stated his desire to bomb a Hispanic Catholic church to an informant.[30] In 2014, supporters of the Nevada rancher Ammon Bundy organized a Gofundme.com page to provide support to the militias occupying the Malheur National Wildlife Reserve: the page was taken down for violating the site's terms of service, but the supporters did not face prosecution.[31]

These cases demonstrate two of the problems in prosecuting funding schemes for far-right terrorist groups. First, individuals can only be arrested if the funding is directed towards a particular crime or the means of funding was obtained during a crime. Second, the statutes do not allow for targeting networked financing schemes (involving multiple individuals) due to the lack of a list of designating domestic extremist groups.

Identifying the Emerging Threat

As digital communications technologies continue to expedite (and hide) the exchange of information and resources, it is necessary to examine the adaptation of terrorist financing efforts. The case of Ali Amin, a Virginia teenager who used a Twitter account to promote IS' propaganda, is illustrative of the threats the U.S. will continue to face for years to come. Specifically, Amin's Twitter account discussed the use of Bitcoin, a cryptocurrency, to fund IS and then disseminated his knowledge of the subject. Using the handle @AmreekiWitness, Amin compiled a "how-to" of best practices for digital currency use to support IS, and disseminated it on his Twitter account.[32] Speaking to an audience of more than 4,000 followers, Amin tweeted over 7,000 times.[33]

Amin went so far as to write an article entitled, "Bitcoin w'al-Sadaqat al-Jihad" (Bitcoin and the Charity of Jihad). His article "discussed how to use bitcoins and how jihadists could utilize this currency to fund their efforts."[34] Punctuating the operational security benefits afforded by Bitcoin, Amin's "article included statements on how to set up an anonymous donations system to send money, using bitcoin, to the mujahedeen."[35] Expanding his scope of influence, Amin also ran a pro-ISIL blog, "Al-Khilafah Aridat," which distributed articles similar to his piece about cryptocurrency, explaining in detail technical steps IS supporters should take to ensure their security and anonymity online.[36] While not immediately threatening, Amin's ability to educate his followers on operational security poses a critical challenge to

---

[30] US Attorney's Office, Western District of Virginia, "Georgia Man Sentenced to Prison for Selling Firearms to Felons to Support Violent Klu Klux Klan Group," *Press Release,* December 20, 2013. Schoenmann, Joe. 2014.
[31] "Cliven Bundy's Supporters Seek Crowdfunding to Sustain Militia - Las Vegas Sun Newspaper." May 15. https://lasvegassun.com/news/2014/may/15/cliven-bundys-supporters-seek-crowd-funding-sustai/.
[32] *USA v. Ali Shukri Amin*, Statement of Facts, (2015).
[33] Zapotosky, Matt. 2015. "Va. Teen Admits He Was Secret Voice behind a pro-ISIS Twitter Account." *Washington Post*. June 11. https://www.washingtonpost.com/local/crime/northern-va-teen-admits-running-pro-islamic-state-twitter-and-helping-man-join-terrorist-group/2015/06/11/1d0cb33e-0eef-11e5-9726-49d6fa26a8c6_story.html.
[34] *USA v. Ali Shukri Amin*, Statement of Facts, (2015).
[35] *USA v. Ali Shukri Amin*, Statement of Facts, (2015).
[36] *USA v. Ali Shukri Amin*, Statement of Facts, (2015).

policymakers and law enforcement officials. In this capacity, it is crucial to postulate the various tactics used by actors that evade detection using untraceable anonymizing tools and cryptocurrencies.

Of all the instances concerning IS-related financing in America, the most striking is that of Mohamed Elshinawy, which is the first and only publicly known case in which money flowed from the Islamic State into America for to fund a terror attack in the U.S. Elshinawy first drew attention from federal law enforcement after he received a $1,000 Western Union money transfer from an Egypt-based IS operative.[37] Over time, Elshinawy and his co-conspirators "utilized various financial accounts and services to transfer monies into the United States from overseas to be used to conduct a terrorist attack."[38] Elshinawy tried to evade detection by pretending to sell printers on eBay, which served as his cover so that he could accept IS-linked funding through PayPal. Using this approach, Elshinawy "received a total of at least $8,700 from individuals [he] understood to be associated with" IS.[39] In August 2017, Elshinawy pleaded guilty to multiple terrorism charges.[40]

Elshinawy's network appears to be more sophisticated and farther reaching than most others in the U.S. and law enforcement unpacked a "global financial network centered on a British technology company used by Islamic State to clandestinely move money around the world." As reported in the *Wall Street Journal*, "This case suggests how Islamic State is trying to exploit holes in the vast online financial world to finance terror outside its borders."[41] As opposed to using sizable sums siphoned through banks, Elshinawy used innocuous transactions that allowed money to flow into the United States and fund acts of terrorism.

Recommendations

More so than ever before, it is necessary for the government to stymie the financing of violent extremism. FTOs have adapted to post 9/11 financial regulations and the threat picture, particularly in the context of terrorist groups like al-Qaeda, and now, the Islamic State is creative and ever-evolving. Federal regulation makes large scale and traditional transfer of funds among terrorists more dangerous and therefore less feasible. Extremists has adapted by resorting to an amorphous range of alternative practices.

- Counter-terrorism practitioners should recognize that regulation by governments will not deter the extremist; he or she will only adapt. Existing approaches that fight terrorism using economic tools sometimes yield unintended consequences, namely the anonymization of financial

---

[37] Stewart, Christopher S., and Mark Maremont. 2017. "American Pleads Guilty to Accepting Islamic State Money to Fund Terrorism." *Wall Street Journal*, August 15, sec. US. https://www.wsj.com/articles/man-accused-of-using-ebay-for-terrorist-funding-agrees-to-plead-guilty-1502811513.

[38] *USA v Mohamed Elshinawy,* Indictment, (2016), p3.

[39] *USA v Mohamed Elshinawy,* Criminal Complaint and Affidavit, (2016), p7.

[40] DOJ Press Release, "Man Pleads Guilty For Conspiring To Provide And For Providing Material Support To ISIS," August 15, 2017.

[41] Maremont, Mark, and Christopher S. Stewart. 2017. "FBI Says ISIS Used eBay to Send Terror Cash to U.S." *Wall Street Journal*, August 11, sec. US. https://www.wsj.com/articles/fbi-says-isis-used-ebay-to-send-terror-cash-to-u-s-1502410868.

exchanges and possibly encourage low-budget attacks which are less likely to be traced by law enforcement.

- Countering Violent Extremism (CVE) efforts in both the previous administration and the current one appeared to target one form of extremism –jihadism. The previous administration, while not explicit in its public messaging, but clearly in its implementation, focused almost entirely on countering Islamic State-inspired terrorism. The current administration's withdrawing of a grant award to an organization that primarily counters white supremacist-inspired terrorism indicates a similar, singular focus. CVE programs would do well to concentrate not only on the threat posed by violent extremists of various ideological shades such as Omar Mateen, but also others like Dylann Roof.

- Initiatives aimed at detecting and disrupting finance-related terrorist activity should recognize the potential and proliferation of emerging technologies. Whether violent extremists mask transfers in cryptocurrencies or hide funds in plain sight, committed terrorist actors are clearly willing to take the road-less-traveled to advance their aims. Counter-terrorism practitioners need to anticipate their next step and plan a defense. The U.S. government should continue to hold banks, along with other financial-transaction providers, responsible for adhering to federal law. Moreover, the U.S. should work to ensure that our allies encourage equally discerning measures for their own private companies. In doing so, the U.S. government needs to understand how such steps change the nature of the threat rather than mitigate terrorist financing altogether.

Low Cost, High Impact: Combatting the Financing of Lone-Wolf and Small-Scale Terrorist Attacks

Dr. Matthew Levitt
Fromer-Wexler Fellow and Director, Stein Program on Counterterrorism and Intelligence,
The Washington Institute for Near East Policy

Testimony submitted to the Terrorism and Illicit Finance Subcommittee, House Financial Services Committee
September 6, 2017

Chairman Pearce, Ranking Member Perlmutter, distinguished members of the Terrorism and Illicit Finance Subcommittee of the House Financial Services Committee, it is an honor and privilege to testify before you today on this timely and important matter.

Homegrown violent extremists (HVEs), acting alone or in small groups, pose a particularly challenging and immediate threat to U.S. national security. This is true of HVE's acting based on basis of international or domestic extremist ideologies or agendas. The nature of this threat has forced officials to contend with the reality that radicalization happens here in the United States. Even the strictest of immigration policies would not effectively address this issue because radicalization happens here. According to a 2017 Department of Homeland Security (DHS) report, "most foreign-born, U.S.-based violent extremists likely radicalized several years after their entry to the United States."[1] DHS's findings echo a December 2016 report issued by the U.S. House Homeland Security Committee, which concluded that "The United States faces its highest Islamist terror threat environment since 9/11, and much of the threat now stems from individuals who have been radicalized at home."[2]

Homegrown violent extremism can include a spectrum of terror threats from foreign-inspired, enabled, or directed plots. Social media and online communication networks have enabled groups such as ISIS to inspire individuals beyond the territory it controls to carry out attacks in the name of the Islamic State. Additionally, the "influencers" (jihadist voices who may or may not have any formal ties with major jihadist groups but who disseminate jihadist material and rhetoric) and the mirror effect of individuals becoming either "inspired" or "radicalized" by

[1] "TRMS Exclusive: DHS document undermines Trump case for travel ban," *MSNBC*, March 2, 2017, http://www.msnbc.com/rachel-maddow-show/trms-exclusive-dhs-document-undermines-trump-case-travel-ban
[2] "The ISIS Terror Threat in America," Terror Threat Snapshot December 2016, Homeland Security Committee, https://homeland.house.gov/wp-content/uploads/2016/12/December-Terror-Threat-Snapshot.pdf

consuming this material from their computers, without necessarily having any direct links to jihadist clerics or groups, have also taken advantage of the new media landscape.[3]

Once an individual or small group has become radicalized and is determined to carry out a terrorist attack, there are many ways they may fund their attack. In contrast to the highly sophisticated attacks of September 11th, which cost about $500,000 and took years of planning to execute, lone offender and small group attacks can be carried out very quickly, with minimal funding and preparation.[4] The result is that in some cases authorities could be denied both the lag time within which they can run an effective investigation and the benefit of key tripwires—like the ability to follow travel, communications and financials trails—that in the past proved to be especially productive lines of investigative inquiry.

Terrorist attacks carried out by lone offenders or small groups are on the rise, especially coming on the heels of explicit calls by both Islamic State and al Qaeda leaders for like-minded followers to carry out attacks in their home countries targeting civilian targets.[5] Both groups have published how-to guides offering advice on how to carry out attacks with homemade improvised explosive devices (IED's), vehicles, knives, arson, and more.[6] In November 2016, for example, al Qaeda in the Arabian Peninsula (AQAP) published its 16th edition of *Inspire* magazine which praised three prior lone actor attacks, called for more of the same, and provided operational suggestions for such attacks.[7] In July the Islamic State released an e-book in Turkish with instructions for conducting attacks alone.[8] Additionally, the ninth volume of the ISIS periodical *Rumiyah*, published in May, contained details on the ideal weapons and targets for lone wolf attacks.[9] Indeed, the group has been pushing such attacks for years now. In an online e-book entitled *How to Survive in the West: A Mujahid Guide (2015)* the group argued: "With less attacks in the West being group (networked) attacks and an increasing amount of lone-wolf

---

[3] Matthew Levitt, editor, "Defeating Ideologically Inspired Violent Extremism," Washington Institute for Near East Policy, March 2017, http://www.washingtoninstitute.org/uploads/Documents/pubs/Transition2017-CVE-6.pdf

[4] Lee Hamilton and Thomas H. Kean, "The 9/11 Commission report: final report of the National Commission on Terrorist Attacks upon the United States", 2004, http://www.9-11commission.gov/report/911Report_Exec.htm

[5] EUROPOL made note of this phenomenon in a bulletin: "Lone Actor Attacks – Recent Developments," European Counter Terrorism Centre, EUROPOL, July 20, 2016, https://www.europol.europa.eu/publications-documents/lone-actor-attacks-recent-developments; The FBI has warned of terrorist calls for attacks targeting hospitals, for example. See "Terrorists Call for Attacks on Hospitals, Healthcare Facilities," FIRE LINE: Intelligence for Fire, Rescue and EMS, February 8, 2017, prepared by FBI Directorate of Intelligence, Office of Intelligence and Analysis, https://info.publicintelligence.net/DHS-FBI-NCTC-HospitalAttacks.pdf

[6] "EU Terrorism Situation and Trend Report 2016," EUROPOL, 2016, https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016

[7] "The 9/17 Operations," *Inspire Magazine*, November 2016, https://azelin.files.wordpress.com/2016/11/inspire-magazine-16.pdf

[8] "Lone Wolves Handbook," June 22, 2017, https://yalnizkurdunkitabi.wordpress.com/2017/06/22/yalniz-kurdun-el-kitabi-kitap/

[9] "The Ruling on the Belligerent Christians," *Rumiyah*, May 2017, https://azelin.files.wordpress.com/2017/05/rome-magazine-9.pdf

attacks, it will be more difficult for intelligence agencies to stop an increasing amount of violence and chaos from spreading in the West."[10]

Clearly, this has had some effect. In recent years, the pool of potential homegrown terrorists has expanded: Today there are open investigations on about 1,000 potential homegrown violent extremists in all 50 states.[11] And yet, not all of America's radicalized individuals have been motivated by the Islamic State's appeals for lone wolves. Ahmad Khan Rahani, the suspect believed to have been behind the bombings in New York and New Jersey, reportedly was inspired by the U.S.-born al Qaeda cleric Anwar al-Awlaki—who was killed in 2011 by a U.S. drone strike in Yemen, but whose radical preaching lives on in online videos. A note apparently left by the bomber referred to Awlaki and the Boston Marathon bombers, who were also inspired by Awlaki.[12] Indeed, while much of the discussion surrounding lone offenders and small cell attacks has focused on the Islamic State and its affiliates, al Qaeda continues to pose a persistent threat we cannot afford to ignore.[13] Indeed, the online recordings and writings of the late al Qaeda ideologue and radicalizer Anwar al-Awlaki continue to pop up in terrorism cases as particularly effective extremist material which still inspire and radicalize lone offenders and small groups of HVEs to carry out attacks.[14]

Finally, the terrorist threat from lone offenders or small groups is magnified by the phenomenon of returning foreign terrorist fighters (FTF's). "The rate of foreign fighter travel to Syria is unprecedented" NCTC Director Nick Rasmussen testified in 2015, adding that it "exceeds the rate of travelers who went to Afghanistan and Pakistan, Iraq, Yemen or Somalia at any point in the last 20 years."[15] Many of these battle-hardened fighters will move on to new battlefronts, and others may return home disgruntled or disillusioned by what they saw in Syria and Iraq and prove no threat at home. But some will, and these could either act on their own or recruit a small group to carry out an attack.

---

[10] "How to Survive in the West: A Mujahid Guide," 2015, https://www.investigativeproject.org/documents/misc/863.pdf.

[11] "Deputy Attorney General Rosenstein Delivers Remarks at the 10th Annual Utah National Security and Anti-Terrorism Conference," United States Department of Justice, August 30, 2017, https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-10th-annual-utah-national-security-0

[12] "Bomb Suspects 'Rambling' Journal Praised Top al-Qaida Operative, Sources Say," Jonathan Dienst, Pete Williams, and Tom Winter, *NBC New York*, September 20, 2016, http://www.nbcnewyork.com/investigations/Pressure-Cooker-Bomb-27th-Street-Manhattan-Boston-Marathon-Ahmad-Rahami-394117971.html

[13] "How al-Qaeda Survived Drones, Uprisings, and the Islamic State," Edited by Aaron Zelin, Washington Institute for Near East Policy, June 2017, http://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus153-Zelin.pdf

[14] The Lessons of Anwar al-Awlaki," Scott Shane, *New York Times*, August 27, 2017, https://www.nytimes.com/2015/08/30/magazine/the-lessons-of-anwar-al-awlaki.html?mcubz=0&_r=0

[15] Nick Rasmussen, "Countering Violent Islamist Extremism: The Urgent Threat of Foreign Fighters and Homegrown Terror", Hearing before the House Committee on Homeland Security, February 11, 2015, http://docs.house.gov/meetings/HM/HM00/20150211/102901/HHRG-114-HM00-Wstate-RasmussenN-20150211.pdf

Identifying HVE's before they attack is a tremendous challenge. "We are looking for needles in a nationwide haystack," FBI Director James Comey testified in July 2016, "but even more challenging, we are also called upon to figure out which pieces of hay might someday become needles. That is hard work, and it is the particular challenge of identifying homegrown violent extremists."[16]

The 2105 National Terrorist Financing Risk Assessment notes the case of Michael Todd Wolfe, from Houston, who planned to fund his travel abroad to fight for radical groups in Syria by using an expected tax refund of $45,000 to cover his expenses. The same type of simple self-funding could also underwrite attacks at home. "Of particular concern," the assessment bluntly concluded, "is that these homegrown violent extremists may use this type of activity to fund domestic terrorist activity in support of extremist ideology espoused by a terrorist group, but without direct assistance from the terrorist group."[17]

In the past, following the money has been a particularly effective intelligence and investigative tool for counterterrorism officials trying to map out terrorist networks and identify terrorist operatives and prevent attacks. But by their very nature, lone offender and small-scale terrorist attacks are less vulnerable to many of the traditional tools in the counter-terror finance toolkit.

The Financial Action Task Force (FATF) succinctly summarized the problem:

> In contrast to large terrorist organizations, small cells and individual terrorists face only minor financial needs since costs of terrorist attacks are often small. As such, lone actors and small cell terrorist networks have a much smaller funding requirement given that they do not control territory, field conventional militias, engage in recruitment or propaganda operations, operate checkpoints or deliver social services.[18]

The Challenge of Homegrown Financing

Homegrown violent extremists (HVEs) may raise funds for several purposes, including to carry out attacks at home, to fund their own or others' travel to foreign conflict zones, or to provide material support to a terrorist organization at home or abroad. Whatever the intent, the funding sources and means of transferring these funds are typically the same.

Looking back at homegrown plots in the West—including both homegrown networks and lone offenders—several key patterns emerge.

---

[16] James Comey, "Worldwide Threats to the Homeland: ISIS and the New Wave of Terror," Hearing Before Committee on Homeland Security U.S. House of Representatives, July 14, 2016, http://docs.house.gov/meetings/HM/HM00/20160714/105134/HHRG-114-HM00-Wstate-ComeyJ-20160714.pdf

[17] "2015 National Terrorist Financing Risk Assessment," U.S. Department of Treasury, 2015, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

[18] "Emerging Terrorist Financing Risks," Financial Action Task Force, October 2015, http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

1. Low-Cost Attacks

As large, complex terror plots are becoming increasingly difficult to carryout, many terrorists are setting their sights lower and are planning smaller, cheaper attacks. Whereas the September 11th attacks cost approximately $400,000-$500,000, took years to plan, and involved dozens of people, today's lone offender and small cell plots may cost as little as $100.[19] According to the 2014 The Norwegian Defence Research Establishment report, 75% of the 40 jihadi plots studied in Europe between 1994-2013 cost less than $10,000 to execute.[20]

Lone offender and small terror cells are able to keep costs low for their plots since they have few members to train and equip, rely on simple weapons such as knives, and in contrast to larger terrorist organizations, they are not subject to the high and indirect costs of developing and maintaining a terrorist organization.[21]

In Great Britain and France, knives and cars are two of the most commonly used weapons in small scale attacks.[22] Both are unsophisticated, readily available and often involve no costs at all since they are already in the possession of the attackers.

In 2013, Michael Adebolajo murdered Lee Rigby, a British soldier in London. Adebolajo first ran Rigby over with his car and then stabbed him to death with a machete and a knife. Adebolajo purchased the knives the day before the attack, likely for no more than £20 or £30.[23]

In another case in September 2014, Ahmad Numan Haider used a knife to attack two counter-terrorism police officers in Melbourne, Australia.[24] In December that same year, Haron Monis held 18 people hostage in a café in Melbourne, and ultimately killed on person.[25] Monis used an

---

[19] Lee Hamilton and Thomas H. Kean, The 9/11 Commission report: final report of the National Commission on Terrorist Attacks upon the United States, 2004, http://www.9-11commission.gov/report/911Report_Exec.htm
[20] "The financing of jihadi terrorist cells in Europe," Emilie Oftedal, Norwegian Defence Research Establishment (FFI), January 6, 2015, http://www.ffi.no/no/Rapporter/14-02234.pdf
[21] Ibid.
[22] "Lone-Actor and Small Cell Terrorist Attacks: A New Front in Counter-Terrorist Finance," Tom Keatinge and Florence Keen, Centre for Financial Crime and Security Studies, January 24, 2017, https://rusi.org/publication/occasional-papers/lone-actor-and-small-cell-terrorist-attacks-new-front-counter
[23] "What led Michael Abdebolajo and Michael Adebowale to murder Rigby?" Laura Smith-Spark and Kellie Morgan, *CNN*, December 19, 2013, http://www.cnn.com/2013/12/19/world/europe/uk-soldier-killing-profiles/index.html.
[24] "Inquest finding into the death of radicalized teen Numan Haider," James Dowling, *Herald Sun*, July 31, 2017, http://www.heraldsun.com.au/news/law-order/inquest-finding-into-the-death-of-radicalised-teen-numan-haider/news-story/2e7b7bb84e585b41433f06ee21bf5c51
[25] "Sydney siege inquest: Man Haron Monis was a 'psychopathic lone wolf terrorist," Australian Associated Press, *The Guardian*, May 2, 2016, https://www.theguardian.com/australia-news/2016/may/02/sydney-siege-inquest-man-haron-monis-was-a-psychopathic-lone-wolf-terrorist

unregistered sawn-off shotgun in the attack that is thought to have been purchased for a low-price on Australia's "grey market."[26]

While the causalities in these and similar attacks are usually low, the perpetrators nonetheless received publicity, instilled fear in the public, and killed targets. Therefore, though causalities may be lower for smaller-scale attacks, the threat they pose to the public must not be underestimated.

2. Self-Financing

In many cases, lone offenders or small groups of may self-finance their activities through legal means such as dipping into their own bank accounts, taking out a loan, receiving welfare payments, or working at a job to raise sufficient funds. They could generate funding through illegal activities. In Europe, since 2001, the proportion of cells that are self- financed through legal activities is higher than those cells that receive external funding.[27]

As demonstrated above, self-financed attacks tend to be cheaper, less sophisticated, and smaller-scale than more expensive attacks. But with fewer opportunities for error, and lacking the need to amass large amounts of money that could raise suspicions, self-financed attacks are more likely to be successfully carried out than attacks that receive external funding. According to the 2014 Norwegian Defence Research Establishment report, "among entirely self-financed cells, 53% have managed to carry out their plans, compared to only 21% among those that receive some external support."[28]

Beyond European cases, in several cases homegrown violent extremists in the U.S. have also used their own salaries to fund attacks. For example, Christopher Lee Cornell saved his own money to buy supplies for his plot to set off bombs near the U.S. capital. In 2015, Cornell had enough money to purchase two semiautomatic weapons and 600 rounds of ammunition with the intention of building, planting, and bombing the U.S. Capitol and shooting people as they ran away.[29] The FBI caught Cornell before his was able to execute his plan; however, he had still managed to raise enough money to fund his plot.

---

[26] "Lone-Actor and Small Cell Terrorist Attacks: A New Front in Counter-Terrorist Finance," Tom Keatinge and Florence Keen, Centre for Financial Crime and Security Studies, January 24, 2017, https://rusi.org/publication/occasional-papers/lone-actor-and-small-cell-terrorist-attacks-new-front-counter

[27] Lee Hamilton and Thomas H. Kean, The 9/11 Commission report: final report of the National Commission on Terrorist Attacks upon the United States, 2004, http://www.9-11commission.gov/report/911Report_Exec.htm

[27] "The financing of jihadi terrorist cells in Europe," Emilie Oftedal, Norwegian Defence Research Establishment (FFI), January 6, 2015, http://www.ffi.no/no/Rapporter/14-02234.pdf

[28] Ibid.

[29] Criminal Complaint for Christopher Lee Cornell, United States District Court for the Southern District of Ohio, January 15, 2017, https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/01/15/cornell_complaint.pdf.

In 2016, Lionel Nelson Williams of Suffolk, Virginia, provided a $200 prepaid cash card to a person he thought was an ISIS affiliate.[30] The FBI has noted that prepaid cards are an easy and accessible way to transfer money, yet are very difficult for authorities to track. They are anonymous and once purchased, the money may be sent anywhere around the world.[31] A month later, in November 2016, Williams used an electronic money transfer service to transfer $50 for the purchase of 10,000 rounds of AK-47 ammunition to a supposed ISIS affiliate in the Middle East.[32] Bank records indicate that Williams had limited money in 2015-2016, while these activities were going on. Nonetheless, Williams was willing to fund weapons for ISIS from his own bank account.

Some lone offenders and small cells that do not have sufficient salaries accept money from their families, or some money take without their knowledge.[33] In other cases, self-financed terrorists ask to borrow money from friends and families without disclosing or being truthful about what the money would be used for.[34] In the case of Mohammed Merah, discussed in greater detail below, Merah received some financial and material support from his family before carrying out a series of shootings in France in 2012. His sister bought him cell phones, allowed him to use her internet while planning his attack, and purchased plane tickets for him. In an interview, she admitted to giving him her credit card to buy plane tickets from France to Damascus, though she said he paid her back afterwards. Last week, an Uzbek man in Brooklyn pled guilty to conspiring to provide material support to the Islamic State.[35] He raised the money he needed to attempt to travel abroad and join ISIS—some $2,400—from fellow Uzbeks in Brooklyn who donated their own money to support his terrorist travel.[36] Another defendant was charged in this case last week.[37]

Criminal Activities: Crime has the potential to bring in sufficient funds for a homegrown attack as well. While criminal groups, lone offenders, and small cells may differ ideologically, they

---

[30] Affidavit in Support of an Application for a Criminal Complaint for Lionel Nelson Williams, U.S. Department of Justice, December 22, 2015, https://www.justice.gov/opa/press-release/file/920321/download

[31] Gerald Roberts, "Money Flow in the Age of ISIS," May 15, 2015, *Washington Institute for Near East Policy*, http://www.washingtoninstitute.org/policy-analysis/view/money-flow-in-the-age-of-isis

[32] Affidavit in Support of an Application for a Criminal Complaint for Lionel Nelson Williams, U.S. Department of Justice, December 22, 2015, https://www.justice.gov/opa/press-release/file/920321/download

[33] "The financing of jihadi terrorist cells in Europe," Emilie Oftedal, Norwegian Defence Research Establishment (FFI), January 6, 2015, http://www.ffi.no/no/Rapporter/14-02234.pdf

[34] Gerald Roberts, "Money Flow in the Age of ISIS," May 15, 2015, *Washington Institute for Near East Policy*, http://www.washingtoninstitute.org/policy-analysis/view/money-flow-in-the-age-of-isis

[35] "Brooklyn, New York, Resident Pleads Guilty to Conspiring to Providing Material Support to Terrorists," U.S. Department of Justice, August 14, 2015, https://www.justice.gov/opa/pr/brooklyn-new-york-resident-pleads-guilty-conspiring-provide-material-support-terrorists

[36] "Fifth Defendant Charged with Attempt and Conspiracy to Provide Material Support to ISIL," U.S. Department of Justice, June 11, 2015, https://www.justice.gov/opa/pr/fifth-defendant-charged-attempt-and-conspiracy-provide-material-support-isil

[37] "Defendant Charged With Conspiring and Attempting to Provide Material Support to ISIS and Al-Nusrah Front," U.S. Department of Justice, August 31, 2017, https://www.justice.gov/opa/pr/defendant-charged-conspiring-and-attempting-provide-material-support-isis-and-al-nusrah-front

often cooperate and collaborate on crimes to raise money for attacks.[38] In Europe, petty crime appears to be the second largest source of funding for lone offenders and small cell groups.[39] In South East Asia, in particular in the Philippines and Indonesia, terrorists have raised funds for attacks by robbing people, smuggling goods and drugs, kidnaping, and extortion.[40]

Mohammed Merah, who carried out three attacks in France in 2012, relied on criminal activities as his main source of funding for the attacks, namely theft, robbery, and drug trafficking.[41] Merah earned $58,000 by acting as a drug courier between Spain and France, and was also heavily involved in a criminal network in France.[42] He had at least 18 convictions from French courts for his involvement in burglaries, thefts, robberies, and other petty crimes.[43] Merah used this money to fund his travel to Pakistan in 2011, where he received training at a camp controlled by Tehrik Taliban Pakistan and al-Qaida in Waziristan. When he returned to France in November 2011, he had approximately $24,500, but wanted to raise additional money.[44] Merah refused to admit to the exact crime, but he said he reconnected with his criminal networks and "did some work with them," earning him a little over $12,000.[45]

Merah claims that al Qaida offered to finance his attacks; however, he refused, claiming it was "easy to get money in France." In addition to the money he earned from crime, he also received some support from welfare and from his family.[46] By March 2012, he had purchased the weapons he would use in his attack, as well as addition arsenal, guns, and ingredients for petrol bombs that were later found in his apartment.

In one case in the United States, Abdul Malik Adbul Kareem, who was convicted by a federal judge in Arizona in March 2016 "of conspiracy to transport firearms and ammunition in interstate commerce with the intent to commit murder and aggravated assault," made a false

---

[38] Gerald Roberts, "Money Flow in the Age of ISIS," May 15, 2015, *Washington Institute for Near East Policy*, http://www.washingtoninstitute.org/policy-analysis/view/money-flow-in-the-age-of-isis

[39] "The financing of jihadi terrorist cells in Europe," Emilie Oftedal, Norwegian Defence Research Establishment (FFI), January 6, 2015, http://www.ffi.no/no/Rapporter/14-02234.pdf

[40] "Terrorist Financing Regional Risk Assessment 2016: South-East Asia and Australia," AUSTRAC, 2016, http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL_0.pdf

[41] "Exclusif - Transcription Des Conversations Entre Mohamed Merah et Les Négociateurs," Liberation FR, July 17, 2012, http://www.liberation.fr/societe/2012/07/17/transcription-des-conversations-entremohamed-merah-et-les-negociateurs_833784.

[42] Makarenko, Tamara. Europe's Crime-Terror Nexus: Links between Terrorists and Organized Crime Groups in the European Union. European Parliament, 2012. http://www.europarl.europa.eu/document/activities/cont/201211/20121127ATT56707/20 121127ATT56707EN.pdf.

[43] Paul Cruickshank and Tim Lister, "How Did Mohammed Merah Become a Jihadist?" *CNN*, March 26, 2012, http://www.cnn.com/2012/03/26/world/europe/france-shooting-suspect/index.html

[44] Thibault Raisse, "Le Pacte Secret de Merah Avec Un Lieutenant de Ben Laden," *Le Parisien*, March 21, 2014, http://www.leparisien.fr/faits-divers/le-pacte-secret-de-merah-avec-un-lieutenant-de-ben-laden-21- 03-2014-3693621.php.

[45] "Exclusif - Transcription Des Conversations Entre Mohamed Merah et Les Négociateurs," Liberation FR, July 17, 2012, http://www.liberation.fr/societe/2012/07/17/transcription-des-conversations-entremohamed-merah-et-les-negociateurs_833784.

[46] "Size of Merah Gun Arsenal Amazes French Public," Andrew Osborn, *IOL News*, March 23, 2012, http://www.iol.co.za/news/world/size-of-merah-gun-arsenal-amazes-french-public- 1.1263042#.U198AVfc9nU.

insurance claim to raise money for his plot in Texas.[47] Kareem pretended to be injured in a car accident and made an insurance claim based on his injuries to raise money for the weapons and ammunition that he would later purchase for a plot to attack on Prophet Mohammed cartoon contest in Texas. The exact amount he received from his claim as well as the price of the weapons he purchased are both unknown.[48]

Legal Financial Loans: Lone offenders and small cells in the Unites States and abroad have exploited different types of loans in order to fund attacks. Ahmedy Coulibaly, one of the three terrorists in the Paris attacks in 2014, funded his plot by taking out a £6,000 loan from the credit agency Cofidis. He provided the agency with a phone bill, pay slips, and identification in order to obtain the loan and finance his operation.[49] The two Kouachi brothers reportedly received $20,000 from al-Qaeda in the Arabian Peninsula, but the rocket-propelled grenade launcher and the Kalashnikov automatic assault rifles used by the Kouachis cost less than $6,000.[50]

The San Bernardino shooter, Syed Rizwan Farook, who killed 14 people in the 2015 shooting, borrowed $28,500 from Prosper Marketplace, a San Francisco online lender, just two weeks before the December 2nd attack.[51] Officials believe that this loan may have financed the ammunition, pipe-bomb parts, and shooting practice at local gun ranges.

Online loans are an easy way to gain fast access to large sums of cash, in contrast to credit cards, which take much longer to process and oftentimes require a strong financial history. While banks and money lenders have to check customers' names against a federal database of known terrorists and criminals, lone offenders and homegrown violent extremists are often not known to law-enforcement authorities and may slip under the radar.

More recently, Salman Abedi, the suicide bomber from the May 2017 Manchester arena attack, took advantage of European loans in order to fund his attack.[52] Abedi collected at least £7,000 from the Student Loans Company, which is covered by taxpayer money.[53] Abedi was eligible for student loans after enrolling in Salford University in October 2015, though it is suspected that he

---

[47] Michael Martinez and Scott Glover, "ISIS supporter convicted in failed plot targeting Mohammed cartoon contest," *CNN*, March 17, 2016, http://www.cnn.com/2016/03/17/us/texas-garland-cartoon-shooting-abdul-malik-abdul-kareem-conviction/index.html

[48] Ibid.

[49] Rukmini Callimachi and Jim Yardley, "From Amateur to Ruthless Jihadist in France: Chérif and Saïd Kouachi's Path to Paris Attack at Charlie Hebdo," *The New York Times*, January 17, 2015, http://www.nytimes.com/2015/01/18/world/europe/paris-terrorism-brothers-said-cherif-kouachi-charliehebdo.html.

[50] "Belgian Arms Dealer Confesses to Supplying Paris Attackers," Shlomo Papirblat, *Haaretz*, January 14, 2015, http://www.haaretz.com/news/world/1.637034

[51] "Loan to San Bernardino shooter draws scrutiny to online lending industry," James Rufus Koren and Jim Puzzanghera, *LA Times*, December 11, 2015, http://www.latimes.com/business/la-fi-prosper-regulation-20151210-story.html

[52] "Exclusive: Manchester suicide bomber used student loan and benefits to fun terror plot," Robert Mendick, Martin Evans, and Victoria Ward, *Telegraph*, May 27, 2017, http://www.telegraph.co.uk/news/2017/05/26/exclusive-manchester-suicide-bomber-used-student-loan-benefits/

[53] Ibid.

did not show up for courses and signed up for his degree with the sole intention of collecting his loans.[54]

David Videcette, a former Metropolitan police detective who helped investigate the 2005 London bombings, said that it is not uncommon for terrorists to finance their attacks "at the expense of the taxpayer."[55] The British government has admitted in the past that there is no way mechanism in place for them to monitor how students are using their loans, and that they do not know how many terrorists may be exploiting this system.[56]

External Support: Though most lone offenders or small groups are self-funded, there are examples of lone offenders who have connections to terrorist organizations and receive external monetary support to carry out attacks abroad. Nine out of ten cells that receive external support have at least one member who has been trained and/or fought abroad, according to a Norwegian study.[57] For example, the 2001 and 2003 shoe-bombers, Richard Reid and Saajid Badat, who attempted to blowup aircrafts with explosives hidden in their shoes, received training and material support from al Qaeda leaders in Afghanistan.[58]

In addition to receiving foreign support, some homegrown violent extremists raise funds at home to send abroad. In one example, Ali Shukri Amin, a teenager from Virginia, used Twitter to circulate instructions on how to fund ISIS through Bitcoin.[59] He first began tweeting in 2014, and became increasingly radicalized and motivated to help people join the ISIS, either financially or by traveling to Syria.[60] His Tweets stressed the anonymity of Bitcoin, and how donors' personal information as well as amount of funding would remain undiscovered and unknown to authorities. Amin was arrested in 2015 and in June that year he pled guilty to providing material support to ISIS.

3. Transfer Methods

While transferring funds is most common among individuals or groups who receive external funding from larger terrorist organizations, even smaller cells or lone attackers may need to transfer money. When the Islamic State controlled territory, it drew foreign fighters from around the world who would sometimes transfer funds to the Islamic State. According to a recent U.N. Security Council Report on ISIL, cash, money service businesses such as Western Union, and

---

[54] "Exclusive: Manchester suicide bomber used student loan and benefits to fun terror plot," Robert Mendick , Martin Evans, and Victoria Ward, *Telegraph*, May 27, 2017, http://www.telegraph.co.uk/news/2017/05/26/exclusive-manchester-suicide-bomber-used-student-loan-benefits/

[55] Ibid.

[56] Ibid.

[57] The data on foreign fighters is adapted from the data set "Foreign Fighter Observation Set 1.0 (.xls)" complied by Thomas Heghammer, available at hegghammer.com/text.cfm?path=2176.

[58] "Sources: Reid is al Qaeda operative," Maria Ressa, *CNN*, December 6, 2003, http://edition.cnn.com/2003/WORLD/asiapcf/southeast/01/30/reid.alqaeda/

[59]"A Teen's turn to radicalism and the U.S. safety net that failed to stop it," Yasmeen Abutaleb and Kristina Cooke, *Reuters*, June 6, 2016, http://www.reuters.com/investigates/special-report/usa-extremists-teen/

[60] Ibid.

bank transfers were among the most popular methods of transferring funds.[61] These same methods are now available for individual or small groups of operatives who could receive external support from the remnants of ISIL or, theoretically, for the movement of money between cell members.

The U.N. Security Council reported in August that "despite military pressure and falling revenues, the ISIL core continues to send funds to its affiliates worldwide, using a combination of money or value transfer services and the transport of bulk cash."[62] The report goes on to note that "ISIL core has also sent money to places where it does not have affiliates, which according to a Member State assessment, is an attempt to prepare for its eventual military defeat" in Syria and Iraq. In other worlds, not only is ISIL preparing to move funds to its other provinces, it is also moving funds to other places where newly inspired followers or returning foreign terrorist fighters can use ISIL funds to carry out attacks. The U.N. also expressed concern that returnees were being briefed in detail on how to act when questioned by government authorities to avoid deportation and arrest, and noted that at least a small category of individuals intend to conduct terror attacks on their return from jihadi battlefields.

Australian officials are similarly concerned. According to an Australian report, "regional authorities are concerned by funds flowing into the region to support local terrorism networks." The report notes that "given only small sums are required to stage a deadly attack, even modest amounts of funding from foreign terrorist groups pose a significant risk to the region's security."[63]

U.S. authorities are equally concerned, as highlighted by a recent case here in the Washington, D.C. area which offers a concrete example of ISIS apparently attempting to provide funds for an attack here in the United States.[64] Last month, U.S. investigators uncovered an ISIS financial network that was transferring money to an operative in the U.S. through false eBay transactions.[65] The recipient, Mohammed Elshinawy, pretended to sell printers on eBay as a cover for the payments he was receiving through PayPal and Western Union for "operational purposes" in the U.S.[66]

While the details and extent of the international financial network have only recently been uncovered, Elshinawy had been on the FBI's radar since at least 2015. In December 2015, he was arrested by the FBI in Maryland for receiving money from ISIS to carry out an attack in the

---

[61] "Twentieth report of the Analytical Support and Sanctions Monitoring Team," United Nations Security Council, August 7, 2017, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2017/573
[62] Ibid,
[63] "Regional Risk Assessment on Terrorism Financing, 2016: Southeast Asia and Australia," AUSTRAC, http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL_0.pdf
[64] "FBI Says ISIS Used eBay to Send terror Cash to U.S." Mark Maremont and Christopher Stewart, *Wall Street Journal*, August 10, 2017, https://www.wsj.com/articles/fbi-says-isis-used-ebay-to-send-terror-cash-to-u-s-1502410868
[65] Ibid.
[66] Ibid.

U.S. He was later convicted for "attempting to provide material support to the Islamic State of Iraq and the Levant (ISIL), obstruction of agency proceedings; and making false statements and falsifying or concealing material facts."[67]

While many cash based transactions occur in personal meetings between terrorists and the perpetrators of the attack, in some cases, terrorist groups rely on cash couriers to transfer the money to their affiliates. ISIS has often broken down into smaller amounts in order to make the transaction harder to detect, according to a U.N. report.[68] Couriers, often selected for their nationalities and ability to enter certain countries, are paid by ISIS to deliver money to associates abroad. However, the movement of funds is highly dependent on transit routes, many of which have been shut down in order to prevent this very issue. Consequently, ISIS has encouraged its affiliates to become more self-sufficient and self-fund attacks.[69]

While ISIS and other large terrorist organizations have been cut off from the formal banking system, terrorists are still able to exploit the system to transfer funds. Since many lone or small groups are self-financed, often using their own income to fund attacks, they have legitimate bank accounts and credit cards which may be abused to pay for attack-related expenses and transfer money between cell members. In one example, in 2010, Nasserdine Menni was found guilty of transferring £5,725 to Taimor Abdulwahab, who carried out a suicide bombing in Sweden in December 2010.[70] Menni transferred the money through multiple bank accounts he had open, some of which were under aliases.[71]

The U.S. Treasury Department's Terrorist Finance Tracking Program (TFTP) collects data on international financial transactions to gain information about terrorist networks and plots.[72] The TFTP has successfully intercepted many illegal transactions and thwarted many plots, such as threats to the 2012 Summer Olympic Games in London, and a 2011 assassination plot to kill the Saudi Arabian Ambassador to the United States.[73] But in the case of small scale plots by lone offenders or small groups, international transactions are less likely to take place. Nonetheless, while this may not prove to be as effective a disruption tool in these cases, it will still prove to be an effective investigative tool in the wake of an attack. The TFTP played important roles in the

---

[67] "Maryland Man Charged With Attempting to Provide Material Support to ISIL," U.S. Department of Justice, December 14, 2015, https://www.justice.gov/opa/pr/maryland-man-charged-attempting-provide-material-support-isil

[68] "Twentieth report of the Analytical Support and Sanctions Monitoring Team," United Nations Security Council, August 7, 2017, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2017/573

[69] Ibid.

[70] "Terrorist Finance Tracking Program. Questions and Answers," The United States Department of the Treasury, http://www.treasury.gov/resource-center/terrorist-illicitfinance/Terrorist-Finance-Tracking/Documents/Final%20Updated%20TFTP%20Brochure%20%288-5- 11%29.pdf.

[71] Ibid.

[72] Ibid.

[73] "Terrorist Finance Tracking Programme," European Commission on Migration and Home Affairs, https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp_en

investigations that followed several terrorist attacks, including the 2013 Boston bombings.[74] While no one system can monitor every transaction, the TFTP is an important measure that the West has in place to address terrorist's exploitation of the international banking system.

Lastly, the hawala or other informal value transfer systems are also popular methods of transferring money for terrorism.[75] While the hawala system is rarely used to transfer money within a small terrorist cell or within Europe, for example, it has been a popular method of transferring funds from European jihadi cells to terror groups abroad.[76]

Countering Homegrown Financing

The challenges posed by lone offender and small group terrorism should not have come as a surprise to practitioners. Indeed, the 9/11 Commission Report forecasted that such a development would likely occur:

> Though progress has apparently been made, terrorists have shown considerable creativity in their methods of moving money. If al Qaeda is replaced by smaller, decentralized terrorist groups, the premise behind the government's efforts—that terrorists need a financial support network—may become outdated. Moreover, some terrorist operations do not reply on outside sources of money and may now be self-funding, either through legitimate employment or low-level criminal activity.[77]

Financial information will always have post-blast utility for investigators piecing together what happened after an attack or disrupted plot, but there is no getting around the fact that HVE trends may undermine the efficacy of some elements of our traditional financial intelligence (FININT) toolkit as a preemptive investigative and intelligence tool. FININT, however, is only one tool in a much larger intelligence toolbox. But while other tools—in particular old-school HUMINT operations—take on greater importance in such cases there is still much that "following the money" can do in tandem with other tools. Despite all of the above, authorities are not without recourse to minimize the challenges posed by small-scale, homegrown terrorist financing.

1. Even lone offenders and small groups need money. Despite the challenges noted above, FATF underscores that even lone actors or small cells have financial needs that must be met: "That said [small cells and individual terrorists] must have the financial means to provide for their own food, shelter, communication devices, transport and any

---

[74] Ibid.
[75] "The financing of jihadi terrorist cells in Europe," Emilie Oftedal, Norwegian Defence Research Establishment (FFI), January 6, 2015, http://www.ffi.no/no/Rapporter/14-02234.pdf
[76] "The financing of jihadi terrorist cells in Europe," Emilie Oftedal, Norwegian Defence Research Establishment (FFI), January 6, 2015, http://www.ffi.no/no/Rapporter/14-02234.pdf
[77] National Commission on Terrorist Attacks upon the United States, Thomas H. Kean, and Lee Hamilton. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States,* (Washington, D.C.: 2004), p.383

procurement requirements for terrorist plots."[78] Often, even lone offenders and small groups will have ties—including financial ties—to others that could provide leads for intelligence and law enforcement officials. Consider cases of crowd-sourcing online or within the local community, or those in which operatives rely on family or friends for seed money for their operations or terrorist travel plans. Contrary to convention wisdom, sometimes even a small financial footprint can have investigative utility.

2. In the purest sense, cases of actual lone wolves are still rare. More often than not, most operatives referred to as lone wolves might more accurately be described as known wolves. Since wolves are pack animals, "lone wolf" is meant to conjure the image of someone who has rejected his nature and is now acting completely independently — a rogue individual operating outside the scope of any cell, network, or group. But while there are cases of inspired individuals — often people from broken homes[79], with criminal records or histories of mental instability[80] — who attack on their own with no formal ties to any group, those rare cases are the exceptions that prove the rule. More often than not, evidence indicates that suspects thought to have been lone wolves might more accurately be described as known wolves — people whose radicalization, suspicious travel, suspicious financial activities, criminal activities, or changes in behavior were observed by acquaintances. In this regard, programs aimed at preventing and countering violent extremism (P/CVE)—which are incredibly important in their own right—could also provide useful points of entry for financial insight and investigation.

3. The private sector has access to tremendous financial information and could be better positioned to act on or share this information with relevant authorities—acting out of the private sector's own business interests—if government did more to help the private sector identify trends and developments in the types of suspicious financial activities to be looked for as the Islamic State morphs as an organization, as al Qaeda resurrects itself, and as lone offender and small group terrorist activities increase in tempo. The US government does this for itself all time. Consider the Treasury Department's Financial Crimes Enforcement Network (FinCEN), which has automated "business rules" it develops to search Bank Secrecy Act (BSA) for key terms, the latest typologies and other trends to identify current terrorist activities. One key development here is the use of IP addresses to help track financial information related to terrorist activities. There is more that could be done to share this information with the private sector, especially regarding trend analysis over time. FATF published a report on typologies in 2015, but that needs

---

[78] "Emerging Terrorist Financing Risks," Financial Action Task Force, October 2015, http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

[79] "My Journey Through Brussels' Terrorist Safe Haven," Matthew Levitt, *Politico*, March 27, 2016, http://www.politico.com/magazine/story/2016/03/brussels-attacks-terrorist-safe-haven-213768

[80] "The Line Between Terrorism and Mental Illness," Jeet Heer, *New Yorker*, October 25, 2014, http://www.newyorker.com/news/news-desk/line-terrorism-mental-illness.

to be updated and such issues should be part of an ongoing public-private conversation. The U.S. should look at the UK's Joint Money Laundering Intelligence Taskforce as an example.

4. FININT can produce surprising leads, as in the targeting information that FININT helped put together for the U.S. military airstrikes targeting ISIS oil income.[81] Following the money will still play an important role even in the space of lone offenders and small cells, especially when these display any form of connective tissue to other operatives, to ISIS planners abroad. But this one tool will always be most effective when applied in a layered fashion with other tools, including tracking communications, running HUMINT operations, and training the public to report suspicious activities more generally. Efforts such as the "See Something, Say Something" public information campaign are an important part of the counterterrorism puzzle.

Dr. Matthew Levitt directs the Stein program on counterterrorism and intelligence at The Washington Institute for Near East Policy. A former Treasury Department Deputy Assistant Secretary for intelligence and analysis, Levitt co-teaches a graduate course on combating the financing of transnational threats in the security studies program at Georgetown University and sits on the advisory boards for the Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies and the Rethinking Counter-Terrorist Finance Project at the Royal United Services Institute.

[81] "In taking economic war to Islamic State, U.S. developing new tools," Yeganeh Torbati and Brett Wolf, *Reuters*, November 24, 2015, http://www.reuters.com/article/us-france-shooting-usa-sanctions-insight/in-taking-economic-war-to-islamic-state-u-s-developing-new-tools-idUSKBN0TD0BJ20151124

WRITTEN TESTIMONY OF

JOSEPH V. MORENO
PARTNER, CADWALADER, WICKERSHAM & TAFT LLP

BEFORE THE

COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE
HOUSE OF REPRESENTATIVES

CONCERNING

LOW COST, HIGH IMPACT: COMBATTING THE FINANCING OF LONE-WOLF AND SMALL-SCALE TERRORIST ATTACKS

PRESENTED ON

SEPTEMBER 6, 2017

WRITTEN TESTIMONY OF
JOSEPH V. MORENO
PARTNER, CADWALADER, WICKERSHAM & TAFT LLP

BEFORE THE

COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE
HOUSE OF REPRESENTATIVES

CONCERNING

LOW COST, HIGH IMPACT: COMBATTING THE FINANCING OF LONE-WOLF AND SMALL-SCALE TERRORIST ATTACKS

SEPTEMBER 6, 2017

Chairman Pearce, Vice Chairman Pittenger, Ranking Member Perlmutter, and distinguished Members of the Subcommittee, thank you for the invitation to appear before you today. My name is Joseph Moreno, and I am a partner at the law firm of Cadwalader, Wickersham & Taft. During my career I have served the government in a variety of capacities, including as a federal prosecutor at the Department of Justice in the National Security Division's Counterterrorism Section, specializing in the financing of domestic and international terrorist attacks, as a staff member to the FBI's 9/11 Review Commission, and on active duty with the United States Army during Operations Enduring Freedom and Iraqi Freedom. It is an honor to be appearing before you today, along with this panel of very distinguished experts, to testify on the financing of lone-wolf and small-scale terrorist attacks, and how regulators, law enforcement, and the private sector can together combat this threat more effectively.

I. Introduction

Since the attacks of September 11, 2001, we have effectively taken our anti-money laundering, economic sanctions, intelligence surveillance, and law enforcement structure and shoehorned into that a system of disrupting and prosecuting terrorist financing. Using the Bank Secrecy Act, the USA PATRIOT Act, the International Emergency Economic Powers Act, and the Foreign Intelligence Surveillance Act, we have been largely successful in preventing the next well-funded catastrophic terrorist attack. And, through use of the material support and terrorist financing statutes,[1] the international money laundering statute,[2] and other laws at our disposal, we have successfully prosecuted hundreds of cases involving terrorist financiers, facilitators, and charities who knowingly provided cash, services, or other items of value to terrorist groups.

---

[1] 18 U.S.C. §§ 2339A-D.

[2] 18 U.S.C. § 1956(a)(2)(A).

However, identifying and preventing lone-wolf or small-scale terrorist attacks presents a unique set of challenges. There is no standard law enforcement profile of the "lone-wolf terrorist."[3] They are typically self-radicalized with little or no direct connection to or communication with an organized terrorist group. They exist in plain sight within our borders, living and working alongside us, with full access to bank accounts and credit cards and social media. With minimal coordination, training, or funding, they can carry out a mass shooting at a school or church, detonate explosives at a mall or during a public event, or drive a car into a crowd of civilians. These attacks are frequently self-funded at a cost of a few thousand or even a few hundred dollars, amounts which are often considered too small to detect solely through the tracking of financial transactions.[4]

It may be tempting to conclude that disrupting and preventing these lone-wolf and small-scale attacks cannot be addressed through law enforcement tactics or legislative or regulatory solutions. However, studies of lone actor terrorists have found that there is almost always some identifiable behavior leading up to an attack, whether it be online publication of a statement or manifesto, preparatory activities such as training or reconnaissance, or the acquisition of weapons, explosives, or other materials.[5] Knowing this, it is encouraging that, through the leadership of this Subcommittee and discussions such as the one we are having today, we can explore ways to identify these behaviors using our existing law enforcement and financial reporting structures, while at the same time look for new ideas to allow the public and private sectors to work together and more effectively address this threat.

II. Applying Our Existing Financial Reporting and Enforcement Framework

First, we need to take a hard look at whether we can better utilize our existing law enforcement and financial reporting framework to identify transactions that may be an indicator of an impending attack.

---

[3] *See* Bates, Rodger A. (2016), "Tracking Lone Wolf Terrorists," THE JOURNAL OF PUBLIC AND PROFESSIONAL SOCIOLOGY, Vol. 8, Iss. 1, Art. 6.

[4] For purpose of comparison, the September 11, 2001 attacks on New York and Washington were estimated to have cost between $400,000-$500,000 to execute, consisting largely of travel, flight training, passports and visas, and cost of living for the hijackers. In contrast, the November 2015 attacks in Paris, the December 2015 attacks in San Bernardino, California, and the August 2017 attacks in Barcelona are each estimated to have cost the attackers less than $10,000, primarily for firearms, ammunition, explosive materials, and rental vehicle costs. *See* Maruyama E. and Hallahan, K., *Following the Money: A Primer on Terrorist Financing*, Center for a New American Security (June 9, 2017), *available at* https://www.cnas.org/publications/reports/following-the-money-1; Harrell, Peter, "The threat of small-dollar terrorism," *Politico* (Aug. 29, 2017), *available at* http://www.politico.com/agenda/story/2017/08/29/the-threat-of-small-dollar-terrorism-000503.

[5] *See* Gill, P., Horgan, J. and Deckert, P. (2014), "Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists," JOURNAL OF FORENSIC SCIENCES, Vol. 59, No. 2, pp. 425–435.

A. Money Structuring Law

The Bank Secrecy Act criminalizes the act of "structuring," or making currency transactions under $10,000 to purposefully cause a bank to fail to file a Currency Transaction Report. Structuring prosecutions have come under criticism in recent years on the argument that an individual may be criminally prosecuted simply for the way they conducted their banking, even if the funds they used in the transaction were obtained in a perfectly legal way. This, coupled with the aggressive use of civil asset forfeiture laws, has led to unfortunate situations whereby funds of law-abiding citizens were seized and the time, expense, and burden was effectively shifted to them to fight for their money back. In 2014, the Internal Revenue Service announced that it will effectively no longer pursue the seizure and forfeiture of funds related to legal source structuring cases.[6] The following year, the Department of Justice announced that it would focus only on structuring cases involving significant criminal activity.[7]

The problem with this approach is that structuring remains one of the most effective ways to identify and prevent criminal or other behavior when the only information available is financial records. Much of the criticism raised about structuring prosecutions is focused on whether the amounts deposited were earned legally. That makes sense from a tax or other criminal prosecution perspective. However, individuals also engage in structuring based on amounts they withdraw, and they are more likely to try and avoid reporting if they plan to use those funds for some improper purpose. So, regardless of where an individual's funds originated, if they are making multiple withdrawals of just under $10,000 within days, or withdrawals from multiple bank branches or cash machines on the same day, for example, they are probably trying to avoid scrutiny of how they plan to use that money.

In the absence of some other source of information to tip off investigators – such as an informant, an undercover asset, or some form of surveillance – looking for structuring or other suspicious financial activity is the primary means of identifying and preventing activity before such funds can be deployed for illicit purposes. In addition, seizing the assets of someone who has engaged in structuring is the most effective way of preventing their use in future terrorist or criminal activity. If assets are seized, investigators should quickly speak with the suspects about why they are engaging in such a pattern of transactions. If the explanation is valid and legitimate, the funds should be immediately released. If, however, the explanation is not plausible, there is likely a reason the individual is seeking to hide from scrutiny either the origin of the funds, or the intended purpose for them going forward.

This is not to say we should not be aware of the plight of small business owners and other individuals who have done nothing wrong but whose funds are seized nonetheless. These citizens often face the long and expensive challenge of trying to regain their assets, and I applaud Congressional efforts to reform this process and help ensure that innocent citizens are not run over by overly-aggressive prosecutors. However, if the goal is vigilant disruption and prevention

---

[6] Treasury Inspector General for Tax Administration Report No. 2017-30-025, *Criminal Investigation Enforced Structuring Laws Primarily Against Legal Source Funds and Compromised the Rights of Some Individuals and Businesses* (Mar. 30, 2017).

[7] U.S. Department of Justice, Press Release 15-400, *Attorney General Restricts Use of Asset Forfeiture in Structuring Offenses* (Mar. 31, 2015).

of terrorist attacks, we must remain willing to vigorously pursue structuring prosecutions and selectively utilize assert seizures as a means of addressing this threat.

B. Suspicious Activity Reporting

Another existing process to look at is how to better utilize the Bank Secrecy Act's requirement that financial institutions issue suspicious activity reports ("SARs") to report potential funding of lone-wolf and small-scale terrorist attacks. The $10,000 threshold for Currency Transaction Reports, and the $5,000 trigger for most mandatory suspicious activity reporting, have been in place since the 1970s. There have been calls in the United States to reduce these amounts to capture additional transactions, as was done several years ago in the European Union.[8] However, in reality that would likely only lead to a higher volume but not necessarily a higher value of reports. What we need to explore is better technology and methodologies to identify small transactions that may be indicative of illicit use, such as the abrupt closure of an account, wire transfers by an individual who historically only made cash transactions, or the movement of funds through multiple accounts or among multiple customers. In addition, manual transaction screening should be conducted in parallel with new artificial intelligence technologies designed to detect suspicious activity in real time.

Efforts by banks and other financial institutions to avoid missing a suspicious transaction often results in over-reporting, which simply floods the system and makes it less likely that truly high-risk behavior will be identified. Financial institutions need greater feedback from FinCEN as to what is expected so that reporting can be meaningful rather than just voluminous. At the same time, we need to ensure that SAR Review Teams have the personnel and funding they require to get through the tremendous volume of reporting they receive, and the ability to follow up quickly when they identify suspicious activity. Being able to rapidly conduct interviews and assess whether a suspicious transaction is an actual threat is essential in the effort to prevent and disrupt a potential attack. The suspicious activity reporting process is seriously impeded if the reports filed by our financial institutions are not actually reviewed and acted on.

III. Limiting Opportunities to Anonymously Raise, Transfer, and Use Funds

Second, we need to look at ways that would-be attackers anonymously solicit, move, and spend money.

Historically, a hallmark of terrorist financing prevention has been to isolate terrorist organizations from funding sources and the global banking system. This does not translate directly in the case of lone-wolf or small-scale terrorists; however, what we can focus on is how groups and individuals seek to solicit, pool, and transfer funds outside the financial system that allows them to do so without revealing their identity. So long as people believe they can move money in a truly anonymous fashion, those avenues will be a tempting way to finance terrorism and other criminal activity.

---

[8] On June 25, 2015, the European Union Fourth Anti-Money Laundering Directive was issued which, among other things, reduced the cash reporting threshold from €15,000 to €10,000 for financial institutions and certain dealers in goods.

If we were having this discussion fifteen years ago, we no doubt would be focusing on hawalas, cash couriers, and charities as primary ways of moving money undetected. Now, new digital payment methods ("NPMs") such as virtual currencies, mobile payment applications, and online peer-to-peer payment systems provide individuals with ever-expanding methods to move funds anonymously.

Major banks in the United States have been collaborating on digital payment platforms which permit small dollar value transfers to or from a registered bank account. Some of the more established vendors such as PayPal also enforce "know-your-customer" processes either directly or via relationships with commercial bank accounts or credit card accounts linked to their customers' accounts. However, other emerging technologies and currencies, including constantly emerging new mobile applications, eWallets, crowd-funding technologies, and virtual currencies have little or no processes in place for identifying or confirming the identities of their users, exposing new holes which can be taken advantage of. These technologies typically involve no face-to-face interactions between vendors and their customers, impose few or no limits on the dollar value of transactions that may be made, and have no restrictions on moving money across borders. As these technologies develop, we must ensure that our reporting requirements keep pace, and consider requiring the financial institutions that do business with NPM vendors implement compliance programs to potentially include usage and geographic restrictions and customer due diligence requirements.

Another emerging issue is the proliferation of prepaid and gift cards. Today, anyone can go into a supermarket and purchase packages of American Express, MasterCard, or Visa prepaid cards. Those cards can be used to purchase virtually anything anywhere across the globe. The same goes for Starbucks and other retail store cards, which are increasingly being accepted by online vendors as a virtual form of payment. Individuals can purchase prepaid cards, then cut and paste the account number, expiration date, and security code into an email or text message and effectively transfer that purchasing power anywhere in the world. By doing so, they effectively convert their cash to a form of anonymous buying power, significantly working around financial reporting safeguards that apply to traditional credit and debit cards. Proposals have been made to limit the use of such cards, including requiring the actual physical card and chip to be used or to limit their use to certain retailers or in certain dollar amounts. But they currently remain as a nearly unregulated form of buying power.

IV. Taking a Comprehensive Prevention and Detection Approach

Finally, we should consider other methods of assisting and funding efforts at the federal, state, and local levels to help prevent and detect the threat of lone-wolf and small-scale terrorist attacks. This may include:

- Regulating Products Commonly Used in Attacks. Further efforts can be made to pursue regulation of products whose purchase may not necessarily raise red flags from a financial reporting perspective. It has been over twenty years since the 1995 bombing of the Oklahoma City federal building by Timothy McVeigh, and the Department of Homeland Security's Ammonium Nitrate Security Program remains in

proposed rulemaking status.[9] If implemented, this rule would create a registration program for purchasers and sellers of ammonium nitrate, and impose reporting and recordkeeping requirements on businesses who sell it. Tagging agents currently required for plastic explosives could be required for use in the gunpowder in bullets and fireworks to help trace those products after a firearm or bombing attack. Data on the purchasers of pressure cookers, diesel fuel, and other consumer products could also be collected and mined.[10]

- Monitoring Extremist Websites and Social Media. We must support funding for law enforcement to continue aggressive surveillance of websites, social media accounts, newspapers and magazines such as *Inspire*, and television broadcasts used by terrorist organizations to spread propaganda, raise funds, and incite violence. In the most extreme cases of websites or other venues being used to identify victims or coordinate attacks, we should utilize active countermeasures to infiltrate and disrupt them. At the same time, operators such as Facebook and Twitter must be pressed to enforce their terms of service and close accounts that are used to incite illegal activity. Just as we strive to cut off terrorist organizations from financial systems, we must try and make it as difficult as possible for individuals to use the Internet and the media to finance and coordinate terrorist attacks.

- Enhancing Mental Health Resources. Any discussion of lone-wolf terrorist attacks would be remiss if it did not touch on the fact that many attackers at some point demonstrate indicia of depression, paranoia, violence, or some other anti-social behaviors to friends, neighbors, family or co-workers prior to an attack. In most states and communities, the only option for reporting on someone exhibiting these behaviors is to report them to local police or the FBI. For many people, they will not take that step for fear the potential attacker will be arrested, or that it may come back they were the source of the tip. But if there was a mechanism for some sort of mental health intervention, particularly starting at a young age, concerned friends and family members may be more willing get that individual the help needed before they go too far down the path to violence.

I raise these options with full awareness that each comes with its own costs, including additional resources expended by the government to implement and execute these activities; increased costs to consumers and, ultimately, the taxpayer; and, most importantly, the impact on individual privacy. These costs must be weighed against the likelihood these activities would be effective, either as prevention and disruption of potential future terrorist attacks, or as a tool for criminal prosecution after the fact.

* * * * * * * *

---

[9] U.S. Homeland Security Department Proposed Rule, "Ammonium Nitrate Security Program," 6 C.F.R. 31 (Aug. 3, 2011).

[10] *See* Persky, Dori (2013), "Common Materials Turned Deadly: How Much Does America Have to Monitor to Prevent Further Acts of Terrorism?" AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, Vol. 4, Iss. 1, Art. 4.

Addressing the threat of lone-wolf and small-scale terrorist attacks presents many challenges, including how the Executive Branch should apply our existing tools and strategies, and whether Congress decides if we need new statutory tools and funding to prevent such attacks. At the same, these efforts must be balanced against the need to prevent over-intrusion into the privacy and property rights of the American people. I commend the Subcommittee for taking on this difficult challenge and opening up this bipartisan dialogue, and I am confident it will be time very well spent.

I appreciate you including me in this important effort, and I stand ready to answer any questions you may have.

Testimony of Frederick Reynolds, Barclays, Global Head of Financial Crime Legal

Before the House Financial Services Subcommittee on Terrorism and Illicit Finance

Hearing on Low Cost, High Impact: Combating the Financing of Lone-Wolf and Small-Scale Terrorist Attacks

September 6, 2017

Good Afternoon, Chairman Pearce, Vice Chairman Pittenger, Ranking Member Perlmutter, and members of the Subcommittee. My name is Frederick Reynolds and I am the Global Head of Financial Crime Legal for Barclays. I appreciate the opportunity to appear before you today to discuss how the financial sector and law enforcement can work together to combat lone-wolf and small-scale terrorist attacks.

During my time as a federal prosecutor for the Department of Justice, as the Deputy Director of the Financial Crimes Enforcement Network and now in the private sector, I witnessed the critical role that financial institutions play in the detection and prevention of money laundering and terrorist financing. Without their assistance, it would be difficult, if not impossible, for law enforcement to "follow the money." Put simply, financial institutions play an increasingly critical role in the detection and prevention of terrorist attacks.

Since 9/11, the public-private partnership between law enforcement and the financial sector has assisted the government in targeting terrorist organizations, driving them from the formal financial system, and inhibiting their ability to raise funds and operate. Financial institutions have become a first line of defense in this fight and are committed to ensuring that terrorists do not use our institutions to fund their activities.

Recently, we have witnessed the rise of so-called lone-wolf terrorist attacks. Because these attacks are often inspired by, but otherwise unconnected to, larger terrorist groups, the techniques that we have typically employed to track and act against such terrorists are, at times, ill-suited to this new threat. I will focus my testimony today on

how law enforcement and financial institutions can expand and modernize their existing public-private partnership to combat these attacks before they occur.

When looking to identify the financial activity indicators of those planning lone-wolf attacks, the challenge for financial institutions is threefold. First:

(1) Lone-Wolf Attacks Are Characterized by Low Dollar Financial Transactions

There are a number of traditional tools under the Bank Secrecy Act ("BSA") that financial institutions use to report suspected terrorist financing. These tools include Currency Transaction Reports ("CTRs") and Suspicious Activity Reports ("SARs"). CTRs – a report on any transaction in currency over $10,000 – are most effective where criminals are attempting to introduce large amounts of cash into the financial system. However, most lone-wolf attacks are accomplished using much smaller sums, so their transactions likely would not trigger the threshold for filing a CTR. Lowering the threshold for CTRs to capture smaller currency transactions, however, would only result in an influx of reports, most of which would have little value and would instead overwhelm the system with so-called "white noise." Both CTRs and SARs are most effective when the transactions are out of the ordinary either in size (CTR) or activity (SAR). This paradigm is often inapplicable to the lone-wolf attack, which lacks size of transactions or unusual activity, and therefore leads to the second challenge:

(2) *Lone-Wolf Attackers Don't Exhibit "Typical" Terrorist Financial Behavior*

Unlike money laundering, where financial institutions look for indications that criminals are trying to make "dirty" money look "clean," in small-scale terrorist threats, the typology is often the reverse. The terrorist in a lone-wolf attack frequently uses otherwise "clean" money for a criminal purpose.

Financial institutions have an abundance of data available to them, but it is not effective, or even possible, to manually review all customer activity. Instead, the detection of terrorist financing is often dependent on technology, including the use of typologies and scenarios designed to identify "typical" terrorist funding behavior. However, lone-

wolf and small-scale attacks pose a particular challenge because they rarely exhibit "typical" terrorist funding behavior. Or, said differently, their financial behavior appears benign and blends in with the myriad legitimate transactions conducted every day by law abiding customers.

For example, a trip to the hardware store for some nails, screws and fertilizer and the rental of a van appears to many like a normal Saturday afternoon of home improvement projects, and detection typologies are not built to flag this type of activity as suspicious, because doing so would flood financial institutions with false alerts. Moreover, this level of granularity—what someone purchased at a hardware store—is often not available to financial institutions, that at best know a customer spent $300 there. So, even if transactions are scrutinized under lower thresholds, such scrutiny is unlikely to produce valuable intelligence. This goes to the third challenge:

(3) Financial Institutions Need to Be Able to Receive and Share Information

Sharing information is critical to identifying and combating terrorist financing. However, financial institutions are currently limited by domestic laws in their ability to share information between institutions or even across borders within the same institution. Unauthorized sharing can result in significant legal consequences for financial intuitions. For example, probably the most significant red flag of a potential bad actor—a prior SAR—cannot be shared by a U.S. institution with its own foreign branch or affiliate. Such limits on information sharing make an "enterprise wide" anti-money laundering system challenging, since sharing key information about customers and their activity within an institution is often prohibited by domestic law. This can result in financial institutions being unable to identify abnormal client behavior. Or, conversely, it can result in over reporting client behavior that might otherwise seem commercially reasonable given a complete understanding of the customer.

Given the small dollar value and nature of the transactions, how do financial institutions differentiate between normal customer activity and a customer planning a

lone-wolf attack? How do you tell the difference between a weekend gardening trip and someone acquiring supplies for an attack? This is where information sharing becomes critical and helps to fill the knowledge gap. The key to overcoming these challenges is a modernized system of robust information sharing between law enforcement and financial institutions and among financial institutions. While not a "silver bullet," modernizing this system from its current binary sharing model is critical to the detection and prevention of future attacks.

Financial institutions rely on information sharing under Section 314(a) of the USA PATRIOT Act, which specifically authorizes law enforcement to share with financial institutions information such as an account, name, IP address or even a telephone number. Often, a single piece of information allows a financial institution to correctly identify a nefarious actor engaging in what may otherwise appear to be innocuous conduct.

If a financial institution learns from law enforcement that, for example, it suspects an IP address is being used by individuals or entities with ties to ISIS, that information can become the "Rosetta Stone" that enables the financial institution to correctly "translate" a customer's activity. And most importantly, it allows the financial institution to devote resources to specifically review the activity – adding the "human element" to an investigation. An investigator armed with the knowledge that the customer may have ties to terrorism enables them to make connections and judgments that cannot be made by technology alone. Additionally, the investigator's findings can then be fed back into the financial institution's detection typologies and scenarios to enhance its ability to detect similar behavior. Continuing to receive these "Rosetta Stones" is key to our ability to provide timely and high quality intelligence to law enforcement.

Likewise, Section 314(b) of the USA PATRIOT Act provides a safe harbor for sharing certain types of information among financial institutions. Financial institutions are often limited by their role in a financial transaction or the information they have on a

customer. Sharing under Section 314(b) allows financial institutions to pool information from several sources, creating a more fulsome understanding of a potential terrorist threat. For example, where a financial institution acts as an intermediary bank for a payment it suspects relates to terrorist financing, Section 314(b) permits it to reach out to the originator or beneficiary's bank to obtain information on that customer and to share its suspicions. This exchange of information can help to confirm or dispel the suspicion and alerts the other financial institution to its customer's activity. Finally, information sharing can enhance the financial institutions' understanding of the extent of a terrorist's network and assist them in identifying connections between known terrorists and those providing financial or logistical assistance.

However, under current law and regulations, Section 314(b) sharing is both cumbersome and limited. At present, financial institutions can only share information after they have formed a suspicion of money laundering or terrorist financing. Rather than waiting to share until after a suspicion has already been raised, Section 314(b) should be expanded to allow financial institutions to share as part of their attempt to identify, or rule out, suspicious activity. Due to these current limitations, financial institutions are often faced with a Hobson's choice – choose to share information that may lead to the discovery of valuable intelligence for law enforcement and take on legal risk or choose not to share and risk failing to stop a bad actor. Better and safer sharing between financial institutions will result in more targeted and actionable intelligence being provided to law enforcement. A few areas where information sharing could be further improved include:

- Authorizing U.S. financial institutions to share SARs with foreign branches and affiliates;
- Explicitly expanding the types of information sharing permitted under Section 314(b) and expanding the Safe Harbor;

- Deprioritizing the investigation and reporting of information of low law enforcement value and allow financial institutions to reallocate those resources to higher value intelligence activity;
- Encouraging the formation of a Joint Money Laundering Intelligence Taskforce (JMLIT)[1] like group in the United States; and
- Clarifying financial institutions' ability to discuss the filing of a SAR with each other where financial institutions are working together on a case, and encouraging them to file joint SARs.

With your permission, I would like to take a moment to illustrate the power of information sharing by mentioning an investigation that Barclays conducted after law enforcement alerted us to an IP address that it believed was connected to a terrorism suspect. I have attached an anonymized chart to my written testimony that demonstrates the extent of the network that was uncovered as a result of that single IP address. While I do not have time today to go through the complete chart, let me give you some highlights:

- Barclays identified "Mr. A" through tracing the IP address provided by law enforcement. In reviewing Mr. A's activity, we noted that Mr. A (who was a student) received money from a variety of sources including over GBP 522,752 from Mr. C, GBP 10,000 from Mr. J and GBP 4,000 from Mr. I.
- Mr. C[2] sent a variety of small dollar payments to Mr. A, and based on further information developed, we suspected this was part of a broader funding mechanism for illegal purposes.

---

[1] In the United Kingdom, "[t]he Joint Money Laundering Intelligence Taskforce (JMLIT) has been set-up in partnership with the financial sector to combat high end money laundering." *See*, http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit.

[2] For illustrative (and size) purposes, we have condensed multiple suspects into the C, D, E, I, J and K identifiers where such suspects had common typologies and identifiers.

- Through further network analysis, we discovered that Mr. J also funded Mr. M, who Barclays had previously tracked and reported as a potential Foreign Terrorist Fighter ("FTF").
- Additionally, we noted a transfer from Mr. A to Mr. H who traveled to, and made a cash withdrawal at, the Syrian border, where a number of FTFs are thought to cross. Likewise, Mr. A sent money to Mr. B, who also appeared to cross into Syria as an FTF.
- Perhaps most interesting, we determined that Mr. A transferred money to a heavy machinery company that makes oil field replacement parts.

From one IP address, we were able to identify related individuals who may have funded multiple FTFs, purchased oilfield parts for possible shipment to Syria, and had links to others who were also funding or supporting suspected terrorist activities. This one IP address allowed Barclays to map a potential terrorist financing network and share this targeted and valuable information with law enforcement. While not every IP address, name or telephone number will yield such potentially significant results; this case illustrates the power of the public-private partnership.

Before I close, I would be remiss if I did not address the very real issue of customer privacy. As I mentioned at the outset, I have spent much of my career focused on issues of money laundering and terrorism finance. Those experiences have made me a believer in robust information sharing. However, I am also a strong believer in privacy.

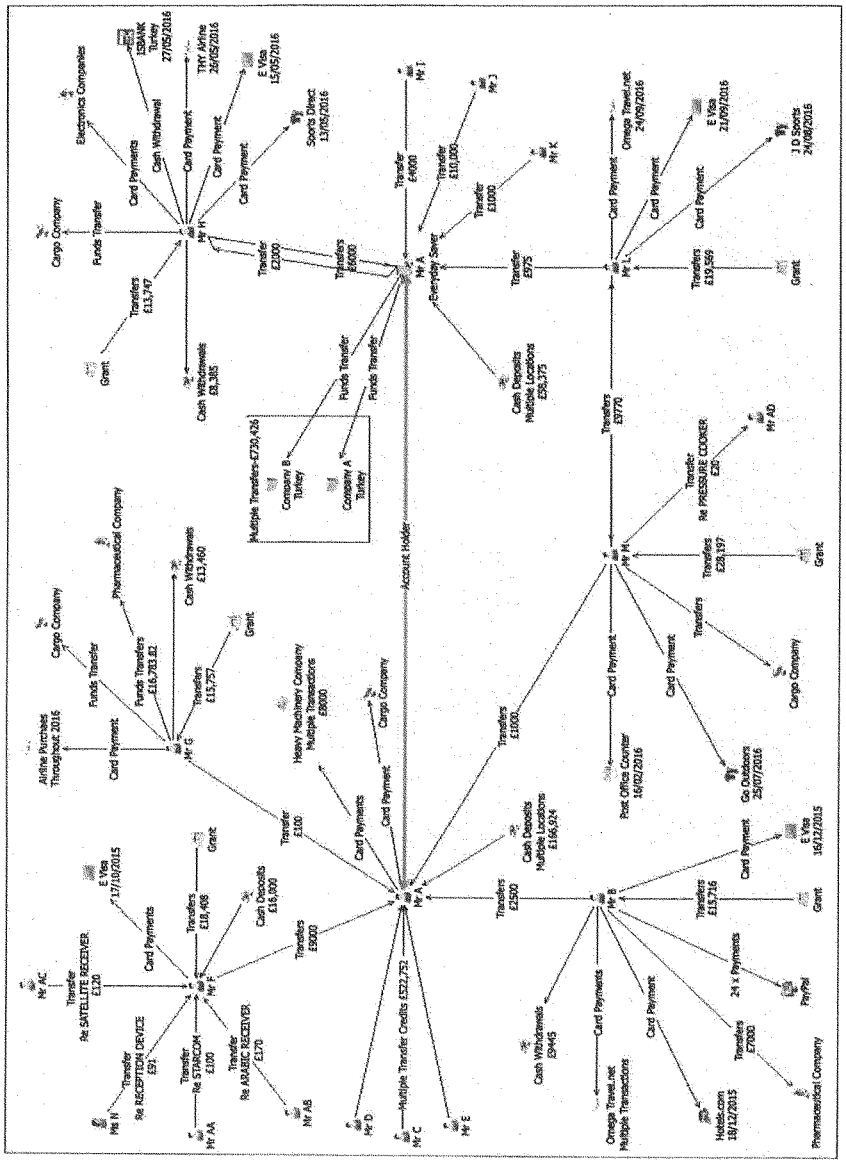
Barclays takes our customers' privacy interests seriously and we work hard to ensure that information about the millions of law-abiding customers we bank is kept confidential. Given this, it is important to note that while at first it seems counter-intuitive, robust information sharing actually enhances individual privacy (though, admittedly, not for the lone-wolf terrorist). Rather than cast an impossibly wide net that includes data from millions of innocent customers, targeted information allows us to focus on the few high-value cases where true national security risks are present.

Moreover, by increasing our understanding of transactions, it will allow us to discount alerts that would otherwise turn into SARs where we cannot understand the purpose of the transaction.

In sum, the targeted information sharing that I illustrated above allows financial institutions to do what they do best: know their customer and focus their investigative resources on transactions and individuals that will produce targeted, high quality information for law enforcement.

Financial institutions want to get this right – we are committed to ensuring that terrorists do not use our institutions to fund their activities. And if we suspect that they are doing so, make no mistake, we will report them to law enforcement. But we cannot do it alone. We need to be able to share and receive information both from law enforcement and between financial institutions in order to focus our efforts and be most effective in identifying terrorist financing. Maintaining open lines of communication also allows all parties to be nimble and ready to adapt to the changing nature of terrorist threats. Increased information sharing between law enforcement and financial institutions will result in a stronger ability to detect and report activity that could indicate a lone-wolf or small-scale attack.

I would like to once again thank the Subcommittee for the opportunity to speak on this important topic. I would also like to thank the Subcommittee and its members for their continued engagement and focus on these important national security issues. I am happy to answer any questions that you may have.


Account Holder
Mr A
Everyday Saver
Mr B
Mr C
Mr D
Mr E
Mr F
Mr G
Mr H
Mr I
Mr J
Mr K
Mr L
Mr AA
Mr AB
Mr AC
Mr AD
Ms N
Multiple Transfers-£739,426
Company A
Turkey
Company B
Turkey
Multiple Transfer Credits £522,752
Transfers £2500
Cash Deposits Multiple Locations £166,924
Transfers £5000
Cash Deposits £16,000
Transfers £18,408
Grant
Transfers £100
Card Payments
Transfer Re SATELLITE RECEIVER £120
Transfer Re RECEPTION DEVICE £91
Transfer Re STARCOM £100
Transfer Re ARABIC RECEIVER £170
E Visa 17/10/2015
Airline Purchase Throughout 2016
Heavy Machinery Company Multiple Transactions £8000
Cargo Company
Pharmaceutical Company
Funds Transfers £15,703.82
Transfers £13,757
Cash Withdrawals £13,460
Transfers £13,747
Cash Withdrawals £8,385
Transfer £2000
Transfers £6000
Transfer £4000
Transfer £10,000
Transfer £1000
Transfer £975
Cash Deposits Multiple Locations £26,375
Transfers £1000
Transfers £9770
Transfers £29,197
Transfer Re PRESSURE COOKER £30
Transfers £19,599
Grant
Post Office Counter 15/02/2016
Go Outdoors 25/07/2016
Cash Withdrawals £9445
Omega Travel.net Multiple Transactions
Hotels.com 18/12/2015
Transfers £7000
24 x Payments
PayPal
Pharmaceutical Company
Transfers £15,716
E Visa 16/12/2015
Omega Travel.net 24/09/2016
E Visa 21/09/2016
JD Sports 24/08/2016
Soons Direct 13/05/2016
E Visa 15/05/2016
THY Airline 26/05/2016
ISBANK Turkey 27/05/2016
Electronics Companies
Card Payments
Cash Withdrawal
Card Payment
Funds Transfer
Cargo Company
Grant