September 6, 2017

Financial Services Terrorism and Illicit Finance Subcommittee: Low Cost, High Impact: Combatting the Financing of Lone-Wolf and Small-Scale Terrorist Attacks

The Financial Services TIF Subcommittee held a hearing today to examine the "patterns and techniques used to fund small-scale and lone-wolf attacks," as well as law enforcement methods to address this type of terror financing. Four witnesses provided testimony:

- Dr. Matthew Levitt, Director, Stein Program on Counterterrorism and Intelligence, Washington Institute for Near East Policy
- Mr. Joseph V. Moreno, Partner, Cadwalader, Wickersham & Taft LLP
- Mr. Seamus Hughes, Deputy Director, George Washington University's Program on Extremism
- Mr. Frederick Reynolds, Global Head of Financial Crime, Barclays

Opening Statements

Chairman Stevan Pearce (R-NM) called the hearing to order. He noted that though overall numbers of lone-wolf terrorism remain low, these events have increased by 50%. Further, these low-cost attacks remain more likely than large-scale attacks. Whether an act of terrorism is directly funded by a known terrorist group and carried out by a sympathizer, the low cost creates challenges in tracing these events. Terror organizations are increasingly turning to new technologies to move funds, and it is clear that the cooperation between policymakers, law enforcement, intelligence agencies, and financial institutions is necessary to disrupt this funding.

Ranking Member Ed Perlmutter (D-CO) reiterated that many attacks are self-financed, and separate from organized terror groups. Attacks have been inspired by foreign organizations or homegrown, but it is essential that we learn to recognize patterns of small-scale terrorism.

Rep. Robert Pittenger (R-NC) recalled his legislation in last Congress to punish those who support lone wolf terrorism. He intends to pursue legislation in this Congress to arm law enforcement and assist foreign partners in efforts to thwart lone-wolf attacks. It is important that we track illicit finance and illegal transactions by cooperating with the private sector.

Rep. Tom Emmer (R-MN) hopes today's topic will help us better understand a shift in the way terror events are carried out. There is an increased pattern of smaller, less coordinated attacks around the globe. Our financial institutions will play a critical role in thwarting these types of terror events; we must constantly evolve to keep pace with the evolution of these threats.

Witness Statements

Dr. Matthew Levitt agreed that lone attacks can be carried out quickly and with little preparation. Lone offenders and small group attacks are on the rise; ISUL has been pushing such attacks for years, encouraging sympathizers to carry out similar events around the globe. The 2015 National Terror Assessment Risk highlighted tax refund as one of the simple financing mechanisms; similarly, self-financing or borrowing money from family or friends can finance attacks without raising suspicions. He called the term "lone wolf" a misnomer, stating that many offenders are "known wolves," making their

views known through social media or other methods. He cited external support as a useful line of investigation, noting that last month law enforcement uncovered an ISIS financial network financed through false eBay transactions. The recipient pretended to sell printers on eBay to cover PayPal and Western Union payments he was receiving in the United States. Levitt noted that lone offenders still need money, and the private sector has access to tremendous financial information. They would be better equipped to act on this information, if they are given a clearer picture of what to look for. Financial intelligence will not solve all problems, but in many cases it provides valuable resources.

Mr. Joseph Moreno noted that identifying and preventing small scale attacks presents a unique set of challenges. Attackers with minimal training and coordination can carry out devastating, frequently self-funded, attacks. Studies show that there is almost always some identifiable behavior leading up to an attack, such as an online manifesto, training, or the purchase of weapons. We must look at how to better utilize our financial reporting framework. If a person is making multiple withdrawals under $10,000 within a few days, they are likely trying to hide how they are using that money. We must also explore better technology to flag smaller transactions that may indicate suspicious use. We must ensure that joint local SAR review teams have the funding and manpower needed to get through the volume of reports they receive each year. Moreno further recommended a look at ways attackers anonymously move money including virtual currencies, crowdfunding, mobile payment applications, and online peer to peer payment systems. We must ensure that our reporting requirements keep pace with these technologies. Further, prepaid cards can be used to transfer purchasing power around the world, converting cash to anonymous buying power. This works around the financial reporting safeguards that traditionally apply to credit and debit cards.

Mr. Seamus Hughes noted that since 2014, 133 individuals have been charged with ISIS-related activities in the U.S.; the vast majority of these persons are U.S. citizens. His testimony applies specifically to ISIS-related activity, though other extremist movements like the white supremacist movement also represent significant threats. The ISIS in America cases highlight the diversity of modern terror financing, including crowdfunding, use of fraudulent student loans to fund travel, and legal financial loans to purchase weapons. He cited four trends found from a review of terror financing cases: first, a public private partnership of best practices can sometimes augment a government-led approach. Second, countering violent extremism programs should target extremists of different viewpoints. Third, financing has largely become decentralized; terrorists now have a multitude of online platforms to exchange funds, using small transactions that do not raise suspicion. Fourth, initiatives aimed at detecting and disrupting illicit activity should account for emerging technologies.

Mr. Frederick Reynolds agreed that traditional terror detection techniques are sometimes ill-suited for disrupting lone-wolf attacks. Traditional reporting tools have difficulty identifying small dollar transactions, and are often confined by domestic laws that make it difficult to differentiate between normal customer activity, and a customer planning an attack. Modernizing the current sharing system is critical to preventing future attacks. He recommended allowing US institutions to share SARs information with foreign branches and affiliates, and explicitly expanding the types of information sharing allowed under 314b. Further, he encouraged the formation of a joint money laundering task force, and encouraging joint SAR filings. Addressing customer privacy, Reynolds encouraged targeted information sharing that allows focus on the few high-level cases.

General Questions

Chairman Stevan Pearce (R-NM) continued on the theme of privacy concerns, asking how this balances with our attempt to detect terror activity. Reynolds replied that increased information sharing allows institutions to target particular individuals or groups who are of highest concern. When institutions cannot discern the lawful reason for a transaction, they must file a SAR; if they had additional information on that customer or transaction, they might not file a SAR. Thus, increased sharing can actually reduce the number of SARs filed, allowing institutions to focus only on cases of concern. Regarding Section 314b, Reynolds called for a legislative fix, noting that current law only allows information sharing for suspicious activity; moving this line back could allow for earlier identification of suspicious actors. Dr. Levitt agreed that privacy concerns must be taken seriously, and added that providing more information would allow for better SARs filing. Numerous unnecessary SARs can bog down law enforcement back, though Levitt noted that moving the information sharing line back could open up a larger number of accounts for monitoring. However, he agreed that it could provide better information for investigation.

Ranking Member Ed Perlmutter (D-CO) focused on public-private partnerships, asking whether Mr. Reynolds is relying on law enforcement information to focus their monitoring. Reynolds replied that many banks have strong detection on their own, but the provision of IP addresses, names, or account numbers by law enforcement allows for significant network analysis. Mr. Hughes agreed, and added that the overwhelming majority of homegrown attacks were already on the FBI's radar. Sometimes there is not enough information to run an investigation, and sometimes there is not enough manpower. Hughes noted that this is where public-private partnerships come into play. Perlmutter turned to domestic terrorism, wondering how we can best prevent this type of terrorism. Mr. Moreno noted that we must balance the cost to the government and consumer vs. the privacy of consumers in tracking transactions.

Rep. Robert Pittenger (R-NC) asked how many SARs are filed each year. Mr. Reynolds did not have the exact number, but noted that FinCEN's database holds 2 million records. Barclays files several thousand reports each year, and Bank of America files reports in the hundreds of thousands. Pittenger reiterated that improved information sharing would reduce the filing of reports, and asked about data sharing rules. Reynolds stated again that sharing can only be facilitated with existing suspicion of money laundering, and pointed out that increased sharing allows for better leveraging of data. Pittenger asked whether there are law enforcement gaps in punishing those who fund terrorism. In terms of material report, Mr. Hughes noted that there are few gaps, as this clause is fairly elastic.

Full Committee Ranking Member Maxine Waters (D-CA) recalled that foreign-radicalized terrorists are not our only concern; homegrown terrorism is on the rise. The recent Charlottesville attack is just the most recent in a series of incidents that are occurring with more frequency. Waters asked what we can do to get a handle on these lone killers, rather than stalling in the face of privacy concerns. She asked what can be done to deal with the KKK, white nationalists, alt-right, and other domestic groups. Mr. Hughes replied that domestic actors are more likely to use criminal methods to fund attacks, and will therefore show up on the radar. Waters yielded to Rep. Josh Gottheimer (D-NJ).

Rep. Josh Gottheimer (D-NJ) recognized specifically the program on extremism that brought to light a report that a senior ISIS official used eBay and PayPal to funnel money to terrorists in the United States. He urged FinCEN to take additional steps to curb money laundering and monitor suspicious online

transactions. He asked how law enforcement can keep pace with new technologies and methods for transferring money. Dr. Levitt characterized Gottheimer's example as a success case rather than a failure, noting that the terrorist was detected and thwarted. However, he agreed with the overall point that we must finetune our resources to detect lone wolf actors. There will be cases where financial detection will not be the biggest resources; we must bundle these resources with traditional investigation techniques.

Rep. Keith Rothfus (R-PA) asked whether there is any information not currently available to law enforcement that might be helpful in the identification of lone wolf terrorists. Dr. Levitt replied that most activity in lone wolf situations looks innocent. We must look closely at the granular information we collect like email addresses, phone numbers, IP addresses, etc., as these are incredibly powerful tools. Rothfus asked whether there is a favored type of financial services that lone wolves use, such as prepaid cards or other methods. Mr. Moreno noted that there is a "buffet" of services that can help people move money near-anonymously. Mr. Rothfus wondered whether prepaid card information sent via text would shed some anonymity, unless through the use of a prepaid phone. Moreno agreed, and added that there can be some limits placed on what can be purchased with prepaid cards: mandating that cards can only be used in stores rather than online, or cannot be aggregated for large dollar purchases, or must only be used via the physical card and chip, could serve to plug illicit activity. Turning to 314b reforms, Rothfus asked whether there would be a "limiting principle" for financial institutions when sharing information under Mr. Reynolds' proposed reforms. Reynolds replied that institutions should not look at a customer without need, but there are opportunities with larger datasets to use algorithms to identify cases that merit further review by an analyst.

Rep. Stephen Lynch (D-MA) stated that in retrospect, behavioral abnormalities more frequently signal a terror attack, rather than financial suspicions. Reporting events from mosque leaders, family members, etc. might provide more insight than monitoring bank accounts. Mr. Hughes replied that financial reviews will likely occur later in the investigations, and acknowledged that earlier red flags might not be enough to signal an investigation. This is where the resource gap is, Hughes stated, noting that the FBI does not have the manpower to monitor all these red flags. Dr. Levitt added that the two are not mutually exclusive; in the case of lone wolves, we find that financial intelligence is not a panacea, but helps link together information. We must use our entire toolkit to identify lone wolf offenders.

Rep. Scott Tipton (R-CO) recalled Dr. Levitt's comments that the private sector could be of tremendous assistance if they were given greater insight, and asked how this could be done. Levitt replied that without a regular public-private dialogue, we are missing an opportunity. We need to encourage banks to communicate better amongst themselves, as well. When asked about information sharing between banks, Mr. Reynolds described the importance of Know Your Customer information from partner institutions can help banks better understand customers and identify suspicious behavior.

Rep. Carolyn Maloney (D-NY) noted that criminals are moving away from banks and toward bitcoin to finance illegal activities such as sex trafficking, drug, and gun offenses. She asked whether there is a penalty for using bitcoin to finance illicit activity. Maloney recommended that the Chairman and Ranking Member look at bitcoin as a growing way of financing crime. Reynolds replied that the penalty for using bitcoin is the same as any other type of financing including cash, check, prepaid card, etc. Bitcoin presents a greater ability to remain anonymous, and this is the key difference we must pay attention to. Following on anonymity, Maloney noted that criminals in her district use real estate to

facilitate the movement of funds; she asked for the panel's opinions on garnering beneficial ownership information as a means of thwarting terrorism. Reynolds stated his strong support for this legislation, noting that it would be valuable to financial institutions.

Rep. Roger Williams (R-TX) spoke to the increased use of social media in terror financing. Levitt replied that terror financing is a non-static issue, noting that we must constantly reassess which tools are most effective. This is a conversation that must include both public and private actors. Williams then asked how the government can effectively exploit resources to identify terrorists while protecting citizens' right to privacy. Reynolds replied that the public sector has a good horizontal view, while it might not have much depth in knowledge on specific consumers. Conversely, the private sector has this depth through its networks. We must work to combine these two pieces of information to focus efforts and move resources away from lower-value intelligence activities. Williams then asked how law enforcement and government agencies share information, and whether it is adequate. Mr. Moreno replied that we have fantastic techniques and people, but we need additional resources. He cited the SAR review process as one area in need of more resources, as staffing issues can mean that reports are not reviewed for months.

Rep. Tom Emmer (R-MN) noted that we cannot simply lower the transaction limit that signals suspicious activity; he asked what else must be done. Mr. Moreno replied that a manual review process must be coupled with new technologies and algorithms to flag suspicious transactions. Emmer asked how we can leverage technologies to make SARs more valuable. Reynolds agreed that we must use technology to look for outliers, and use our human resources to focus on the most important national security issues. He listed terrorism, human trafficking, money laundering, and cybersecurity as areas constituting the biggest threats. Emmer asked what should be done to encourage those in the private sector to notice suspicious activity and report it. Levitt countered that banks are paying close attention, and if anything, we have an issue with overreporting.

Rep. Warren Davidson (R-OH) asked how much Barclays spends on reporting of suspicious activity. Reynolds could not provide the exact figure, but noted that it is "fairly substantial" in terms of staff. Davidson asked how much revenue this generates for Barclays; Reynolds replied that it generates none. Davidson then wondered why banks are so eager to engage in information sharing and law enforcement activity for an issue that generates no revenue for the company. Reynolds replied that banks want do the right thing, and do not want to bank terrorists, money launderers, and human traffickers. Davidson followed on the balance between big data and privacy; Levitt replied that banks do not and cannot look at every transaction. The point is to focus only on specific cases in which there is reason to believe something is off. There are clear threshold requirements, but we must remember that not all suspicious events may be tipped off by transactions greater than $10,000.

Rep. French Hill (R-AR) asked if there is "off the shelf" software that integrates data to make filing a SAR a more sophisticated activity. Reynolds noted that there are several commercially available solutions tailored to banks of various sizes to help flag suspicious activity for AML officers. Second, "advanced analytics" help institutions to look across the data for outliers in their customer set. Most large institutions utilize both resources, while smaller institutions utilize mainly the first resource.

Rep. Stevan Pearce (R-NM) thanked the witnesses and adjourned the hearing.