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.