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.

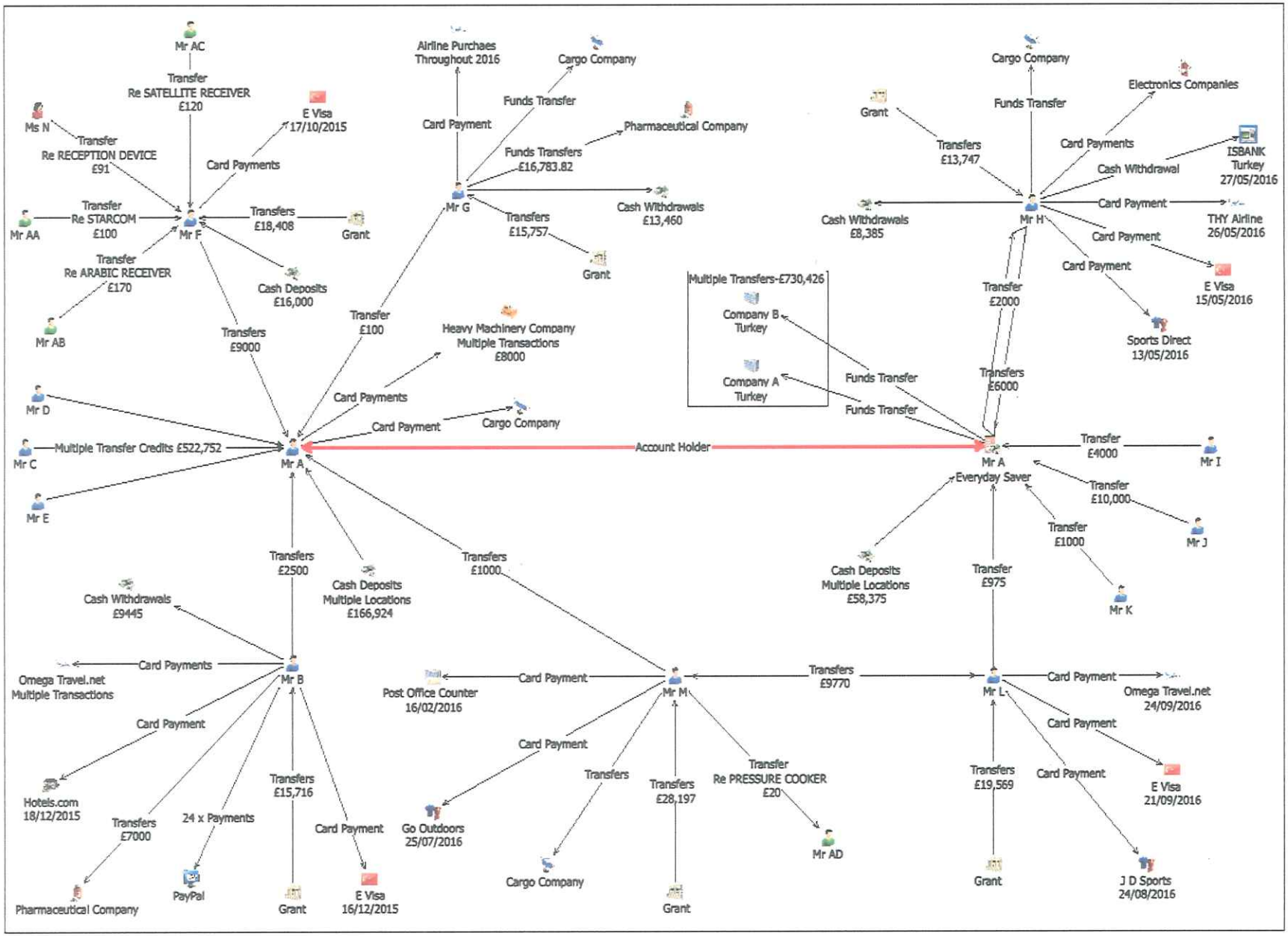
Barclays takes our customers' privacy interests seriously and we work hard to ensure that information about the millions of law-abiding customers we bank is kept confidential. Given this, it is important to note that while at first it seems counter-intuitive, robust information sharing actually enhances 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.


Mr AC
Transfer
Re SATELLITE RECEIVER
£120
Ms N
Transfer
Re RECEPTION DEVICE
£91
E Visa
17/10/2015
Card Payments
Mr AA
Transfer
Re STARCOM
£100
Mr F
Transfers
£18,408
Grant
Transfer
Re ARABIC RECEIVER
£170
Mr AB
Cash Deposits
£16,000
Transfers
£9000
Airline Purchaes
Throughout 2016
Cargo Company
Card Payment
Funds Transfer
Pharmaceutical Company
Funds Transfers
£16,783.82
Mr G
Cash Withdrawals
£13,460
Transfers
£15,757
Grant
Transfer
£100
Heavy Machinery Company
Multiple Transactions
£8000
Card Payments
Mr D
Card Payment
Cargo Company
Mr C
Multiple Transfer Credits £522,752
Mr A
Account Holder
Mr E
Transfers
£2500
Cash Deposits
Multiple Locations
£166,924
Transfers
£1000
Cash Withdrawals
£9445
Card Payments
Omega Travel.net
Multiple Transactions
Mr B
Card Payment
Hotels.com
18/12/2015
Transfers
£7000
24 x Payments
PayPal
Transfers
£15,716
Card Payment
Pharmaceutical Company
Grant
E Visa
16/12/2015
Post Office Counter
16/02/2016
Card Payment
Mr M
Transfers
£9770
Card Payment
Transfers
Transfers
£28,197
Transfer
Re PRESSURE COOKER
£20
Go Outdoors
25/07/2016
Cargo Company
Grant
Mr AD
Multiple Transfers-£730,426
Company B
Turkey
Company A
Turkey
Funds Transfer
Funds Transfer
Cargo Company
Funds Transfer
Grant
Transfers
£13,747
Electronics Companies
Card Payments
Cash Withdrawal
ISBANK
Turkey
27/05/2016
Cash Withdrawals
£8,385
Mr H
Card Payment
THY Airline
26/05/2016
Card Payment
Card Payment
E Visa
15/05/2016
Transfer
£2000
Transfers
£6000
Sports Direct
13/05/2016
Mr A
Transfer
£4000
Mr I
Everyday Saver
Transfer
£10,000
Mr J
Transfer
£1000
Cash Deposits
Multiple Locations
£58,375
Transfer
£975
Mr K
Mr L
Card Payment
Omega Travel.net
24/09/2016
Card Payment
Transfers
£19,569
Card Payment
E Visa
21/09/2016
Grant
J D Sports
24/08/2016