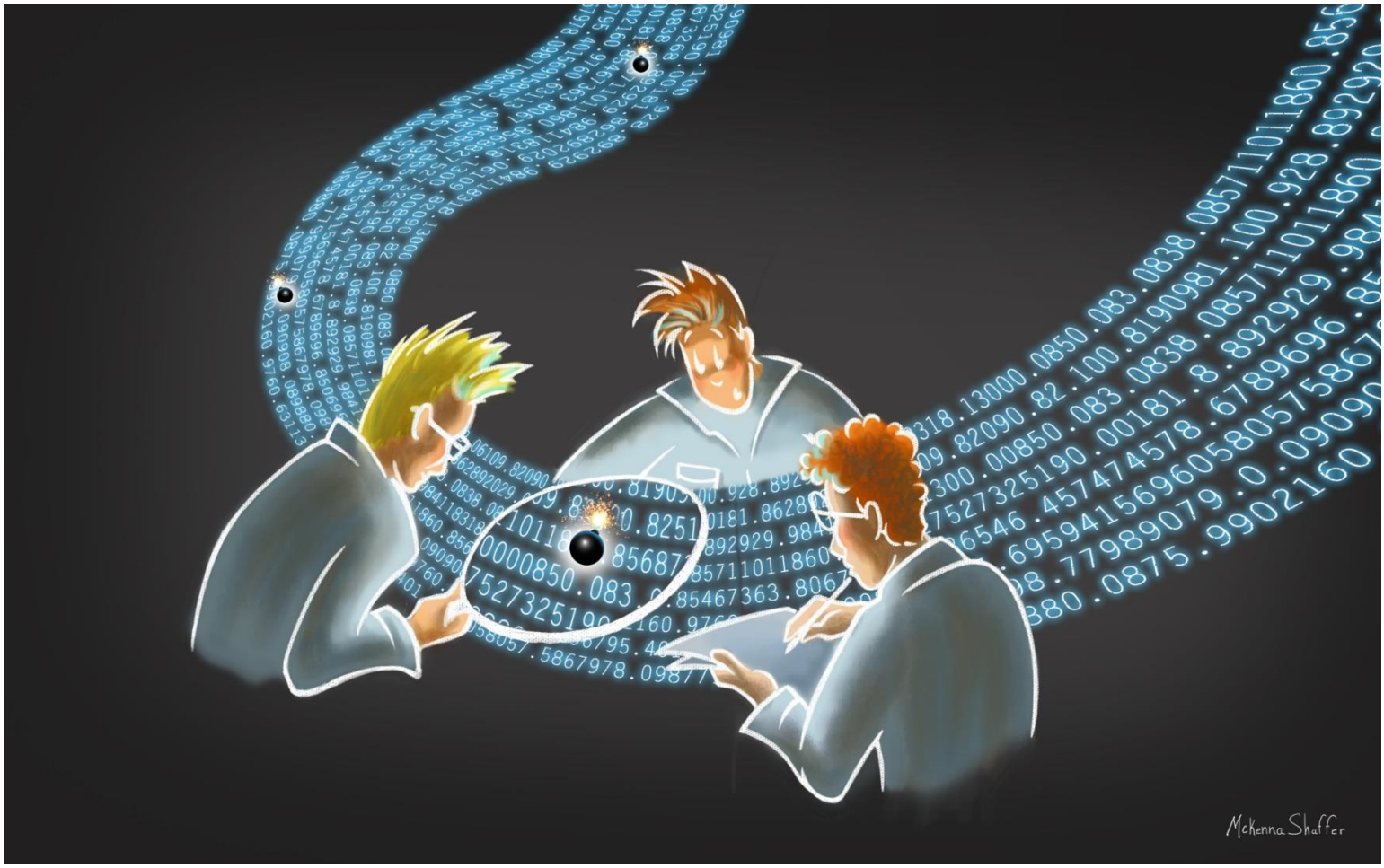
Big Problems In Small Transactions



Illustrations by: McKenna Shaffer

DEBORAH HITZEROTH, CAMS
BSA/AML Compliance Officer
United States Postal Service

CONTENTS

INTRODUCTION

The idiom that good things come in small packages is often true, but when it comes to terrorist financing (TF) tragic events can be funded by very small transactions. The issue facing financial institutions (FIs) is how to detect these microtransactions before they become part of tomorrow's headlines.

The war on terrorism is being fought on many fronts and FIs are playing a key role in the battle by stopping funds destined for terrorist groups. The importance of impeding this money flow was underscored by the National Commission on Terrorist Attacks Upon the United States (9-11 Commission), which stated that fighting TF was one of the most effective ways to deter terrorist activities. In its 2004 report, the commission wrote:

"After the September 11 attacks, the highest-level U.S. government officials publicly declared that the fight against al Qaeda financing was as critical as the fight against al Qaeda itself. It has been presented as one of the keys to success in the fight against terrorism: if we choke off the terrorists' money, we limit their ability to conduct mass casualty attacks. In reality, completely choking off the money to al Qaeda and affiliated terrorist groups has been essentially impossible. At the same time, tracking al Qaeda financing has proven a very effective way to locate terrorist operatives and supporters and to disrupt terrorist plots."[1]

The commission's findings are still true today. In his article, "The Challenges of Terrorist Financing in 2014 and Beyond," Dennis M. Lormel, CAMS, president and chief executive officer of DML Associates, states that "funding is the lifeblood of terrorist organizations."[2]

[1] John Roth, Douglas Greenburg, and Serena Willie, "Monograph on Terrorist Financing," *National Commission on Terrorist Attacks Upon the United States*, July, 22, 2004, 2, http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf.
[2] Dennis M. Lormel, "The Challenges of Terrorist Financing in 2014 and Beyond," *ACAMS Today,* Dec. 2013 - Feb. 2014, http://www.acamstoday.org/wordpress/2013/12/18/the-challenges-of-terrorist-financing-in-2014-and-beyond/.

What has changed since issuance of the commission's report is that, while still difficult, it is no longer impossible to choke off funding. Lormel differentiates the types of terrorist activities and the typical way that each is funded. In the article, he recommends that:

> "It is best to go back to the point of origin and also forward to terrorist strike teams. In that context, there are three funding tracks. The first is funding to a network or organization. This funding stream ranges from hundreds of dollars to millions of dollars. The next track is funding to operations. This funding stream ranges from thousands to hundreds of thousands of dollars. The last track is funding to individuals, cells or groups. This funding stream ranges from hundreds to thousands of dollars."[3]

The financial community has developed effective methods to detect funding streams dealing with the transfer of thousands to millions of dollars and stop these funds before they reach the intended recipients. One of the challenges still remaining is how to detect TF being performed through small transactions. The purpose of this paper is to discuss the challenges of detecting microfinancing of terrorist activities and recommend ways to separate normal activity from transactions with potentially deadly consequences. This paper is based on both research and personal interviews with anti-money laundering/counter-terrorist financing (AML/CTF) experts.

Hiding in Plain Sight

The greatest challenge to detecting microfinancing transactions is simply, as one might expect, their size. The dollar amounts are so small they fall below the normal red flag limits used by most FIs and often get lost in the noise of daily business. According to the commission's report, approximately $300,000 flowed through the 9/11 terrorists' bank accounts over a period of two years using a variety of aliases, banks and routing channels. Once the money was deposited in the hijackers' accounts, most of the activity was for normal living expenses that would be expected for such accounts. Even though the 9/11 hijackers were not money laundering masterminds, they were able to avoid

[3] Ibid.

detection because this type of TF was not widely known at the time. Since it was unsuspected, it went undetected. According to the commission:

"Neither the hijackers nor their financial facilitators were experts in the use of the international financial system. They created a paper trail linking them to each other and their facilitators. Still, they were easily adept enough to blend into the vast international financial system without doing anything to reveal themselves as criminals, let alone terrorists bent on mass murder. The money-laundering controls in place at the time were largely focused on drug trafficking and large-scale financial fraud and could not have detected the hijackers' transactions. The controls were never intended to, and could not, detect or disrupt the routine transactions in which the hijackers engaged."[4]

Fourteen years later, terrorism financed with relatively low dollar amounts and committed by individuals or small groups has unfortunately become familiar scenario. A few examples include:

- March 11, 2004 – Small bombs hidden in backpacks were used to kill 191 people and injure 1,800 more on commuter trains in Madrid. The total cost of the attack was an estimated $10,000.[5]
- July 7, 2005 - Four suicide bombers killed 56 people and injured 700 on the London Underground. In its February 29, 2008, "Terrorist Financing Report," the Financial Action Task Force (FATF) published comments from an investigation of the attacks, which estimated the cost was "less than GBP 8,000…(the) bombs were homemade, and that the ingredients used were all readily commercially available and not particularly expensive."[6]
- December 25, 2009 - Umar Farouk Abdulmutallab, who became known as the underwear bomber, was foiled in his plan to blow up Northwest Flight 253 on its final approach to Detroit. The fact that Abdulmutallab was working with limited funding was illustrated by his reason for choosing Detroit as his target. According

[4] Roth, Greenburg, and Willie, "Monograph on Terrorist Financing," 3.
[5] Financial Action Task Force, "Terrorist Financing Report," February 29, 2008, 7, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.
[6] Ibid.

> to the Associated Press, the destination was selected because "it was the cheapest flight… [Abdulmutallab] also considered blowing up planes above Houston and Chicago, but tickets were too expensive."[7]

Even though it is has become a known typology, terrorism microfinancing is still difficult to detect. The source of the funds for these small transfers are usually varied and come from individuals whose financial accounts have never been flagged for potentially suspicious activity. The funds flow to the terrorist groups in amounts and over time periods designed not to trigger red flags.

In its 2015 study, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)," FATF found that funding for the terrorist group included not only the familiar predicate crimes associated with money laundering, like robbery and drug trafficking, but also smaller amounts.[8] These included:

- Unemployment benefits and family allowances;
- Loans from FIs made to supporters or group members and not repaid;
- Individuals opening multiple bank accounts and using the accounts' overdraft limits to withdraw cash;
- Money raised through social media and sent by cash or wire transfers to the group; and
- Funds deposited in one country, such as the U.S., then withdrawn in a country near areas inhabited by ISIL.

FATF's report is replete with case studies of these funding activities reported by member countries. One trend found to be increasing was microfinancing used to fund foreign terrorist fighters (FTFs). According to the report:

"Terrorist financing risks were discovered regarding foreign cash withdrawals via ATMs that were made in areas located near territories where ISIL operates by

[7] Caulfield, Philip, "Christmas 2009 'underwear bomber' targeted Detroit because it was the cheapest flight," *Daily News*, March 24, 2011, http://www.nydailynews.com/news/national/christmas-2009-underwear-bomber-targeted-detroit-cheapest-flight-report-article-1.118654.
[8] Financial Action Task Force, "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)," February 28, 2015, 22, http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.

unknown individuals…This information reveals the terrorism financing risks posed by the continued ability of the individuals who are believed to have travelled to areas occupied by ISIL to reach their bank accounts in their home countries."[9]

Following its plenary session in February 2015, FATF issued statements asserting that ISIL is a "new type of terrorist organisation with unique funding streams that are crucial to its activities" and that cutting off funding is "critically important."[10]

While FATF's releases were targeted to the governments of member countries, the call to action is equally valid for FIs, including both banks and money services businesses (MSBs). FIs can help cutoff this flow of funds by identifying their TF risks and developing more effective ways to detect, disrupt and deter TF. FIs should also "implement appropriate preventive measures to prevent ISIL from accessing the international financial system, including (those) related to customer due diligence [CDD], correspondent banking, and wire transfers."[11]

FATF's review also found that ISIL is turning from large donors to small individual contributors, which increases the risk for microfunding transactions through FIs. ISIL has found an effective way to reach these contributors by becoming a master of using social media to reach beyond its borders to individuals around the globe. "Emerging technological advancements have created novel virtual pathways to solicit and transfer funds instantaneously to any location," according to the report.[12]

Twitter is commonly used by ISIL's social media arm to spur followers to make donations, some of which are funneled "through unregistered charities in the form of 'humanitarian

[9] Ibid., 23.
[10] Financial Action Task Force, "Action on Terrorist Financing" and "FATF Action on the Terrorist Group ISIL," February 27, 2015, http://www.fatf-gafi.org/topics/fatfgeneral/documents/fatf-action-on-terrorist-finance.html.
[11] Financial Action Task Force, "Action on Terrorist Financing" and "FATF Action on the Terrorist Group ISIL."
[12] Financial Action Task Force, "Financing of the Terrorist Organisation Islamic State," 36.

aid' with terrorists coordinating geographical drop-off points for payments using cellphone applications such as WhatsApp and Kik," according to *Newsweek* magazine.[13] The *Newsweek* article authors found that:

"Hundreds of these social media accounts exist solely for the purpose of retweeting propaganda from ISIS channels—primarily in English—and promoting the contact details of ISIS operatives to "truthful" followers. But once a connection is made, donations to ISIS operations soon follow."[14]

One example of the successful use of social media to raise money for FTFs was documented by *Wired* magazine. In his article, "New Kickstarter Pitch: 'Join the Syrian Uprising'," author Spencer Ackerman details a Kickstarter campaign by two journalists to fund the filming of their fight alongside Syrian rebels.[15] The pair raised more than $15,000 before Kickstarter shut the campaign down.

Social media campaigns are effective in garnering small donations from a variety of individuals across a wide region. These new financing methods can easily slip under the radar unless FIs use new ways to detect them. One way is to make a paradigm shift and look at transactions like a military intelligence unit rather than an AML compliance group.

A New Paradigm

The first step in the process is to understand the environment you are operating in and then develop intelligence start points, according to Lt. Cmdr. Andrew Mackay, an operations officer with the Royal Navy serving as a military liaison officer in Washington, D.C.[16] Mackay derives his advice from almost two decades of experience conducting network analysis and assessing potential threats in the Balkans and Middle East and his postgraduate work through which he is pursuing a Master of Arts degree in Intelligence and International Security at King's College, London.

---

[13] Jannie Di Giovanni, Leah McGrath Goodman, and Damien Sharkov, "How Does ISIS Fund Its Reign of Terror?, *Newsweek*, November 6, 2014, http://www.newsweek.com/2014/11/14/how-does-isis-fund-its-reign-terror-282607.html.
[14] Ibid.
[15] Spencer Ackerman, "New Kickstarter Pitch: 'Join the Syrian Uprising'," *Wired,* August 21, 2012, http://www.wired.com/2012/08/syria-kickstarter.
[16] Lt. Cmdr. Andrew Mackay, Royal Navy, Interview March 6, 2015.

Step One: Intelligence Preparation of the Operational Environment

Intelligence Preparation of the Operational Environment (IPOE) is intended to give a holistic view of the operational environment from physical factors, sociocultural factors through to the information environment and helps create analytic synergy, according to Mackay. It is a dynamic process that can be scaled or tailored to the particular problem. "Once you understand the environment you can set a baseline of normal and abnormal activity and develop the indicators and thresholds for warning," Mackay said.[17] This process is applicable whether reviewing a customer account or a potentially hostile environment in a foreign country. Without taking the time to establish the "normal" it is impossible to detect the abnormal—and also the absence of the normal. Without this intelligence it will be difficult to detect the small transactions that could mean big trouble. "At first glance everything could actually look normal because you are probably dealing with quite savvy terrorists," Mackay said. "They know and understand the thresholds and triggers that will set off red flags, such as the CTR threshold."[18]

Setting the baseline is different than just doing due diligence. It is getting to know the customer and his or her typical behavior and transaction patterns to determine what is normal, abnormal and being able to detect the absence of the normal. With this baseline, it is possible to detect slight but truly abnormal transactions that deserve a closer look. "These slight anomalies are the intelligence start points from which (you can) build out networks using link analysis techniques," Mackay said.[19] For example, money transfers to pay for crowdsourcing campaigns that are irregular for the customer could be a sign of microfinancing of terrorism. When such activity is detected, FIs should dig deeper and ask questions such as the following.

- Who are the other people or groups that have contributed to the campaign?
- To what groups or people are the contributors and the campaign itself linked?

[17] Ibid.
[18] Ibid.
[19] Ibid.

Without a baseline these transactions could easily go undetected. By using them as intelligence start points, FIs can follow the money trail and develop an understanding of the networks and entities involved, ideally ending up at a person—the beneficial owner in financial terms or person of interest in military parlance, according to Mackay.

Step two: Structured Analytic Techniques

This is the point where the data available has been gathered as much as possible, but the intelligence unit is still working with incomplete information and it is time to turn data into actionable intelligence. "You have huge amounts of data and a lot of ambiguity," Mackay said. "You need to apply structure to the information, analyze that information and develop assessments, scenarios and products in order to reduce uncertainty for policy makers and decision makers."[20] When searching for TF, FIs also need to use structured analytical techniques for data reduction and analysis. According to Mackay, this includes:

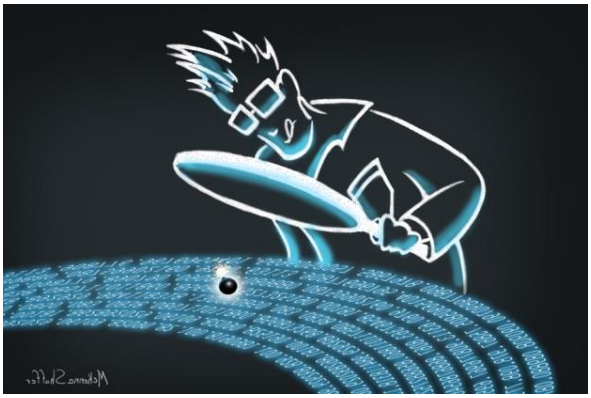
> "Brainstorming, alternate competing hypotheses and many other well-known techniques. Brainstorming, for example, brings together disparate people with different backgrounds who can cut through analytic bias and test the plausibility of scenarios. One of the things that came from the 9/11 commission was there was a lack of imagination and a failure to connect the dots."[21]

Front-line employees can also provide valuable intelligence data—not only on individual events but also on long-term trends and changes in typologies. "Often you get your first lead from human intelligence," Mackay said. "Someone reports it. A bank teller gets a funny feeling about a transaction and starts asking the customer question and then reports it up the line."[22]

[20] Ibid.
[21] Ibid.
[22] Ibid.

LOOK DEEP

Using a mixture of human intelligence along with automated monitoring, as Mackay suggests, can help FIs connect the dots when it comes to detecting terrorism microfinancing. To ensure each dot—or data point—is identified, FIs must review every area of financial activity for a customer or financial product. This includes the flow of funds in and out of bank accounts, the geographical locations of the sender and recipient of wire transfers, and the pattern of prepaid card activities. Currently there are no extensive studies available on the scope of TF through the use of prepaid cards, but anecdotal evidence indicates it could be a growing trend. One documented case was the January 2010 assassination of Mahmoud al-Mabhouh in Dubai. *The Christian Science Monitor* reported that the assassins used prepaid cards, obtained under false identities, to pay expenses prior to the attack. According to the Dubai police:



> "The cards were issued by the Iowa-based MetaBank, which in turn subcontracted the details of the card to New York-based Payoneer, a company that issues prepaid cards and provides banking services similar to Paypal…MetaBank issued the pre-paid cards. But Payoneer is the company that receive[d] payment to be loaded onto the cards and act[ed] as the broker between MetaBank and the customers—in this case the people Dubai police alleged participated in the murder.[23]

According to Jeff Ross, senior vice president, Bank Secrecy Act/anti-money laundering/Office of Foreign Assets Control (BSA/AML/OFAC) officer of Green Dot Corporation and former U.S. Department of the Treasury, senior advisor (law

[23] Dan Murphy, "Hamas Assassination: Debit Cards Issued by Firm with Israeli Ties," *The Christian Science Monitor*, March 2, 2010, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAA&url=http%3A%2F%2Fwww.csmonitor.com%2FWorld%2FGlobal-News%2F2010%2F0302%2FHamas-assassination-Debit-cards-issued-by-firm-with-Israeli-ties&ei=5NcVVbyOONivoQTsv4KQBA&usg=AFQjCNHZNLktLyU9iH8XPOdobcu2ZG_g4w&sig2=CuRTRsCM0Hz9s-W7BnRk3Q.

enforcement) in the Office for Terrorist Financing and Financial Crimes, red flags to look for include:[24]

- Aberrations in any foreign spend or load patterns for prepaid cards or frequency or amount of international wire transfers. It is important to look not only at the dollar amount but the percentage of increases, according to Ross. For example, if there is a rise in the amount of wire transfers into a high-risk country from $400 to $2,000 in a quarter, this is a red flag that the FI needs to dig deeper. Even though this is small in terms of dollars, it is a fivefold increase in the normal pattern.
- The location that prepaid cards are bought, loaded and used. Look both for cards purchased and loaded in the U.S. with withdrawals in foreign locations and also for prepaid cards issued by and loaded via foreign transfers but that are transacting in the U.S. Ross was particularly emphatic that U.S. law enforcement needs to have a firm grasp of all such foreign-issued prepaid cards and card programs that might be doing business in the U.S.
- Money being transferred in to a prepaid card or bank account issued or established in the U.S. from a foreign location.

Other red flags, according to Steve Gurdak, group supervisor for the Northern Virginia Financial Initiative Washington/Baltimore High Intensity Drug Trafficking Area (HIDTA) and a former police detective with 30 years of experience specializing in financial crimes, include:[25]

- Account activity that does not match the account holder's occupation, for example, a student with numerous wire transfers in and cash withdrawals, but no educational expenses.
- Unverifiable employment within an ethnic community.
- The accountholder being supported by another person for no obvious reason. "If not family, the motivation needs to be considered or investigated," Gurdak said.

[24] Jeff Ross, SVP, BSA/AML/OFAC Officer, Green Dot Corp., Interview March 2, 2015.
[25] Steve Gurdak, group supervisor, Northern Virginia Financial Initiative, Washington/Baltimore HIDTA, Interview January 23, 2015.

> "Again the details of who, how and what living expenses are being paid needs to be scrutinized."[26]

To ensure front-line employees and analysts have the information they need to detect the potential terrorist microfinancing, Gurdak recommends building a relationship with local law enforcement as part of the FI's annual training program. "Co-training with law enforcement to recognize this activity provides an opportunity for each side (law enforcement and BSA/AML compliance) to learn from the other," Gurdak said. [27]

GO TO THE NET

Also, take a page out of the terrorists' campaign book and never overlook the Internet or social media. Electronic source intelligence can provide important and readily available information to FIs. Valuable intelligence can be gained from a thorough review of the customer's Web presence. Often there is information in a customer's website, blogs, or Web posting that would increase or decrease the probability that a transaction is suspicious.

Equally important to the information gathered through all of these sources is putting the information in a perspective, according to Tom Keatinge, director of the Centre for Financial Crime and Security Studies at The Royal United Services Institute in London. "Terrorism follows geopolitical activities," Keatinge said. "Be sure monitoring reflects geopolitical activities. Break down (the information) by town and area."[28] Viewed this way, it is easier to connect the dots and the significance behind seemingly random transactions can be detected.

LOOK TO THE PAST

Sometimes terrorist microfunding can only be detected through a preponderance of evidence over time. To identify these transactions, perform periodic reviews of all international transfers of dollar amounts much lower than the FI's normal red flag limit.

---

[26] Ibid.
[27] Ibid.
[28] Tom Keatinge, director of the Centre for Financial Crime and Security Studies, The Royal United Services Institute, March 15, 2015.

For microfinancing, a good starting point is looking for transactions from $50 to $1,000. For small institutions, or ones with a limited international footprint, this can be done manually. For a large international organization, this can be a daunting task. In this case, the FI will need to rely more heavily on automated screening. To narrow the scope of the review, set geographical parameters that include senders in specific high-risk areas in the U.S. to recipients in specific foreign destinations. This type of review can be especially beneficial to MSBs that sell anonymous products like money orders and prepaid cards. Even if the product falls below record keeping limits when sold, looking at where it was purchased and were it was used or cashed can provide a wealth of information.

Reviewing transaction patterns over time to see how they have changed over a five-year period can also provide invaluable data, according to Ross.[29] Pull out previous audits and program reviews and compare the current customer mix and flow of funds with historical data. Risky transactions that may have blended in with daily activity can be detected when comparing chronologically separated transactions.

CONCLUSION

Terrorists, especially ISIL, are constantly changing the way they solicit and receive funds and microfinancing of terrorism is growing. FIs can overcome the challenge of detecting these small transactions by changing their methods as well.

FIs must look at transactions in a new way, blending traditional money laundering red flags with new methods, monitoring not only transactions but also geopolitical events around the world, and by evaluating transactions over time. By incorporating these practices, it becomes easier to detect and stop small transactions from reaching terrorist groups where they can turn in to large and deadly problems.

[29] Ross Interview.

The views expressed in this paper are solely those of the author in her private capacity and do not in any way represent the views of her employer or any other entity related directly or indirectly with the author.

BIBLIOGRAPHY

Ackerman, Spencer. "New Kickstarter Pitch: 'Join the Syrian Uprising'." *Wired,* August 21, 2012. http://www.wired.com/2012/08/syria-kickstarter.

Caulfield, Philip. "Christmas 2009 'underwear bomber' targeted Detroit because it was the cheapest flight." *Daily News*, March 24, 2011. http://www.nydailynews.com/news/national/christmas-2009-underwear-bomber-targeted-detroit-cheapest-flight-report-article-1.118654.

Di Giovanni, Jannie; Goodman Leah McGrath; and Sharkov, Damien. "How Does ISIS Fund Its Reign of Terror? *Newsweek*, November 6, 2014. http://www.newsweek.com/2014/11/14/how-does-isis-fund-its-reign-terror-282607.html.

Financial Action Task Force. "Terrorist Financing Report." February 29, 2008. http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.

Financial Action Task Force. "Action on Terrorist Financing" and "FATF Action on the Terrorist Group ISIL." February 27, 2015. http://www.fatf-gafi.org/topics/fatfgeneral/documents/fatf-action-on-terrorist-finance.html.

Financial Action Task Force. "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)." February 28, 2015. http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.

Lormel, Dennis M . "The Challenges of Terrorist Financing in 2014 and Beyond." *ACAMS Today,* Dec. 2013 - Feb. 2014. http://www.acamstoday.org/wordpress/2013/12/18/the-challenges-of-terrorist-financing-in-2014-and-beyond/.

Murphy, Dan. "Hamas Assassination: Debit Cards Issued by Firm with Israeli Ties." *The Christian Science Monitor*, March 2, 2010. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAA&url=http%3A%2F%2Fwww.csmonitor.com%2FWorld%2FGlobal-News%2F2010%2F0302%2FHamas-assassination-Debit-cards-issued-by-firm-with-Israeli-ties&ei=5NcVVbyOONivoQTsv4KQBA&usg=AFQjCNHZNLktLyU9iH8XPOdobcu2ZG_g4w&sig2=CuRTRsCM0Hz9s-W7BnRk3Q.

Roth, John; Greenburg, Douglas; and Willie, Serena. "Monograph on Terrorist

Financing.” National Commission on Terrorist Attacks Upon the United States, July, 22, 2004, 2. http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf.