Congressional Testimony

The Next Terrorist Financiers: Stopping Them before They Start

John A. Cassara
Former U.S. Intelligence Officer
and Treasury Special Agent

Board of Advisors
FDD's Center on Sanctions and Illicit Finance

Hearing before the House Committee on Financial Services
Task Force to Investigate Terrorism Financing

Washington, DC
June 23, 2016

Chairman Fitzpatrick, Ranking Member Lynch and members of the Task Force to Investigate Terrorism Financing, thank you for the opportunity to testify today. It is an honor for me to be here.

On February 3, 2016, I was similarly honored to appear before this Task Force to testify on a topic of great concern – trade based money laundering and value transfer.[1]

I am pleased to note that as a result of the referenced hearing, there has been additional focus on trade-based money laundering (TBML) and its links to terror finance. I am also heartened that the Task Force has explored some of the recommendations in my testimony.

The focus of today's hearing is to summarize findings but also identify emerging terrorism financing threats so that we can act to mitigate coming dangers. So this morning, I would like to shift my focus away from TBML and take this opportunity to discuss another topic that I have also been concerned about for many years. It is already dramatically transforming financial services in areas of the world in which our adversaries operate.

. . . . . .

Exponential Growth

In 2008, I wrote an essay published by the Department of State titled "Mobile Payments – a Growing Threat."[2] Eight years later, the threat has materialized.

Mobile payments is actually an umbrella term that covers diverse high-tech money transfer systems such as digital precious metals, Internet payment services, prepaid calling cards, and M-payments (i.e., money and e-value transfer via the use of cell phones).

(Note: I am limiting my remarks to mobile network operators where transactions are generally processed over the operators' wireless network(s). I will not address mobile payment services offered by financial institutions or the mobile payment service provider model where the provider offers mobile payment capabilities to its service users which may include merchants.)

The growth of access to cellular devices is breathtaking. In 1990, there were approximately 11 million mobile phones worldwide.[3] In 2016, the number of mobile lines in service has surpassed the global population![4] By 2020, more people will have mobile phones than electricity and running water.[5]

The GSMA, an organization that represents the global mobile industry, estimates that there are now approximately 411 million mobile money accounts in the world. The total was increased by almost a third in 2015. There are approximately 270 mobile money services operating in 93 countries. More than one billion mobile money transactions were processed in December 2015.[6]

We should cheer these developments. The G-20 included "financial inclusion" on its priority agenda to help over two billion adults around the world who have limited access to financial

institutions.[7] As an example, only an estimated four percent of Mauritanian adults have bank accounts.[8]

I know many of Task Force members are international travelers. Many of you have traveled extensively in the developing world. Undoubtedly, you have observed how easy access to M-payments via the ubiquitous cell phone is transforming lives by providing a much needed link to contemporary financial services at a reasonable price. Users are not required to have a bank account or credit card. Countries without modern financial and communications infrastructure are able to "leapfrog" directly into cutting edge networks.

For example, in Tanzania only 12 percent of the population is engaged in the formal financial sector. Mobile banking services fill the gap and, as a result, are expanding rapidly. The Central Bank of Tanzania estimates that the equivalent of $650 million is transferred each month through mobile transfers. [9]

In Kenya, using 2013 data, an astounding 43 percent of Kenya's GDP flowed through M-Pesa, the country's leading mobile money service provider.[10] Twenty-three million Kenyans use M-Pesa or 90 percent of the adult population. There over 100,000 M-Pesa agents in Kenya.[11]

How it Works

The following is a very simple summary of how money moves via cell phone.

1. The subscriber/user gives cash to an M-payment outlet. Sometimes these are nothing more than a small "mom and pop" kiosk or a convenience store in a rural village or city street. The user pays a small fee generally based on the amount of money involved.

2. The M-payment center transfers the money electronically through the phone company to the receiver's cell phone.

3. The recipient receives a text message informing him/her that the transfer to his "electronic-wallet" is complete.

4. The recipient uses the credits.

M-payments allow the purchase of products, services, payment of bills, the transfer of money person to person (P2P), the facilitation of micro payments for low value repetitive goods such as mass transit, the settlement of utility bills, payment of taxes, school fees, health, and many other services. Salaries and government benefits can be credited to cellular devices. M-payments have empowered small business creation. Remittances from migrant workers are sent home via the use of cell phones.

Unfortunately, this wonderful development in financial services is also going to have dangerous side effects that I believe deserve the attention of this Task Force.

Money Laundering and Terror Finance Dangers

I spent a career traveling the world investigating financial crimes such as fraud, money laundering and terrorist finance. I firmly believe that unless we move quickly to engineer new forms of data collection and analytic tools in M-payment systems and also put in place regulatory and enforcement countermeasures we will pay a very heavy price. In fact, there are signs that the abuse of the mobile payment industry by criminal elements is already happening.

I would like to reference the three distinct stages of money laundering and explain how M-payments are used in all three.

The first stage of money laundering is **"placement"** of illicit cash into a financial institution. There are many ways this occurs. One of the most prevalent methods both in the United States and around the world is "structuring," sometimes also known as "smurfing." For example, a professional money launderer takes a large amount of drug dollars and divides it into small amounts. He gives the small sums of money to "runners" or "smurfs" to deposit. The transactions are done in ways that attempt to avoid government mandated financial transparency reporting requirements. Financial transparency equates to financial intelligence. To put things in context, in the United States approximately 17 million pieces of financial intelligence are forwarded to the Treasury's Financial Crimes Enforcement Network (FinCEN) every year. Financial intelligence helps analysts and law enforcement officers follow the money trail. Most countries have similar types of financial transparency countermeasures.

With M-payments criminals now have a new way to "place" the proceeds of crime into financial networks. For example, a professional money launderer recruits a number of runners and gives them the proceeds of criminal activity. Small street sales of drugs, stolen property, or even suspect charitable or terror financing contributions can be laundered in this manner. The runners then go to M-payment establishments and use the illicit funds to load up their cell phones with money or "e-value" under the maximum threshold level. At the end of the day, the runner will be directed to forward the mobile money credit to master accounts controlled by the money launderer. This technique has been labeled by the Asian Development Bank as "digital smurfing." In contrast to money laundering where cash is placed into traditional financial institutions and sometimes money service businesses (MSBs), these structured M-payment placements are not transparent. With few exceptions, financial intelligence is not generated. And practically speaking, as I describe below, digital smurfing in most countries of concern is immune to law enforcement counter measures.

The second stage of money laundering is **"layering."** Once the illicit funds are "placed" into a financial institution, the objective is to layer the dirty money by multiple transfers and transactions thereby confusing the paper trail and adding multiple levels of venue and jurisdiction. Layering makes it very difficult for criminal investigators to "follow the money."

With M-payments, layering will be taken to new levels. In most jurisdictions, mobile value can be transferred from account to account and then directed to a financial institution or MSB in the host country or perhaps wired to another country or even an offshore haven. Mobile value can even be credited to an on-line account or perhaps used to purchase virtual currencies in

cyberspace. A myriad of formal and informal money transfer systems such as hawala can also be added to the equation to further frustrate criminal investigators trying to follow the money trail. M-payments can also be used in hawala networks as a 21st century means of settling accounts between brokers. In short, layering schemes are only limited by the criminal's imagination.

The third stage of money laundering is defined as **"integration."** Once the dirty money is placed and layered, fronts for a criminal organization integrate the laundered money back into the economy. They might buy luxury vehicles and palatial homes or invest in shopping centers, the stock markets, and commercial enterprises of all sorts.

For example, the daughter of one of the worst kleptocrats in Africa has a net worth of billions of dollars. The country concerned has tremendous natural resources. The money controlled by the kleptocrat's family could be described as "fruits of corruption." In order to help "integrate" or legitimize the laundered ill-gotten gains, the kelptocrat's daughter has invested in cell phone carriers and M-payment providers in multiple countries.

In another example cited by the U.S. Department of State, in the West African country of Cote d'Ivoire funds are already being laundered via these M-payment techniques. In Uganda, also according to State Department reporting, "a significant portion of financial transactions … take place in the form of 'mobile money' payments and transfers, which could be abused by individuals and entities engaged in money laundering, terrorist financing, or other forms of financial crime … While the AMLA (financial intelligence unit/FIU) requires financial institutions to conduct comprehensive customer due diligence, it does not put the same requirements on mobile money transfers."[12]

While sub-Sahara Africa is the region where mobile money is most widely spread, South Asia, the Caribbean, Latin America, and the Middle East are also rapidly expanding mobile financial services. Per industry sources, the following are a few examples of some of the most successful examples of M-payments; the Philippines, Bangladesh, Pakistan, and Afghanistan.[13] Some of these countries already boast millions of M-payment users.

Unfortunately, these same countries also face terror finance challenges and likewise have extremely weak anti-money laundering/counter-terrorist finance (AML/CFT) enforcement. In all of the above examples, due diligence practiced by mandated reporting entities such as banks, money service businesses (MSBs), and designated non-financial businesses and professions is generally very weak. The FIUs are challenged – if not ineffectual – and law enforcement and prosecutors are hampered by a lack of expertise and capacity. To put things in perspective, in 2015 the Philippines had zero convictions for money laundering; Bangladesh had one conviction; Pakistan had zero convictions, and in 2014 (the last year statistics are available) Afghanistan reported only four money laundering convictions.

Realistically, there are no current tools to help law enforcement and intelligence officers identify and untangle suspicious M-payments in these and other countries where our adversaries operate. And as far as I am aware, none are on the horizon.

My point is that some skeptics might claim that there are few cases linking mobile payments with money laundering and terror finance. I am convinced that currently there are many incidents and that they will increase rapidly in the coming years. Cases are simply not recognized because the necessary technical infrastructures are not in place to trigger "red-flags." Moreover, there is a lack of understanding of the new M-payment threat and a corresponding lack of financial crimes investigative capacity in most of the countries concerned. There has been a rush by entrepreneurs and mobile payment carriers to develop the technology and deliver services while for the most part ignoring countermeasures that could be engineered into the systems to help thwart money laundering and terror financing.

Some countries are being careful. For example, M-payments in Lesotho are flourishing. So the Central Bank of Lesotho mandated that mobile money systems such Ecocash and M-Pesa must adhere to the Lesotho Money Laundering and Proceeds of Crime Act. The Central Bank issued guidance that was developed to conform to "international best practices and standards." M-payment providers are mandated to follow AML/CFT compliance programs. All transactions must be local and the amounts transferred have daily and monthly limits. In order to transfer higher amounts, know-your-customer (KYC) rules apply and subscribers are required to present their passport and proof of their sources of income. The system also has unusual behavior triggers which can lead to a suspicious transaction report (STR) being filed with the financial intelligence unit (FIU).[14]

The Lesotho model will help mitigate the digital smurfing risk. It will work for them because the size of the customer base is manageable. Lesotho has a population of two million. The real challenge will be to implement M-payment AML/CFT safeguards for large user communities.

For example, there are more mobile phones in Brazil than people, with approximately 275 million subscribers in a population of approximately 200 million – or approximately 100 times the population of Lesotho. Brazil is the fourth largest mobile market in the world. Yet despite the extensive mobile device penetration, mobile payments have been relatively slow to catch on. That will change soon.[15]

Action Taken by the United States

So what is the United States government doing? The short answer is not much. Eight years ago when I first wrote about "the growing threat of M-payments," the idea of money laundering and terror finance via cell phones was mostly theoretical. In the interim, Treasury's Financial Crimes Enforcement Network (FinCEN) was given the mandate to sort out the myriad of legal, regulatory, and enforcement issues. Little was done.

U.S. regulators did make clear that existing financial services regulations apply to mobile banking and mobile payments providers. FinCEN announced "that the acceptance and transmission of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location, by any means, constitutes money transmission" and is "subject to relevant FinCEN regulations for AML/CFT purposes, either as part of the requirements on banks applying to all of their products and services, or as part of the requirements on money transmitters, a subset of

regulated "money services businesses."[16] As such, mobile banking and mobile payment providers are required to register with FinCEN, be licensed in most of the states where they operate, and follow traditional financial intelligence reporting norms.

However, it gets complicated. According to the government's own data, FinCEN's MSB registration program has not been successful.[17] The diversity and accessibility of the MSB sector presents challenges for regulation and oversight.[18] Moreover, many of the businesses involved in the transfer of money through mobile devices aren't financial institutions. Some argue that companies involved in mobile payment systems that don't meet the established definition of providing banking services aren't subject to anti-money laundering enforcement scrutiny, regulation, or even consumer protection laws. Undoubtedly, more years will go by while industry pushes back against the requirements.

In addition, there doesn't seem to be a sense of urgency to deal with these issues. While the use of M-payments will continue to grow, we have a social-economic culture that includes very well-established electronic payments systems with numerous existing options to meet consumer needs outside of mobile. Moreover, some observers in the U.S. have voiced concerns about M-payment interoperability, security, availability, consumer protection, etc.

Yet in most jurisdictions overseas, these concerns do not dominate discussion. As noted, many countries are hampered by weak anti-money laundering controls, enforcement, lack of capacity and expertise, corruption, and the lack of political will to seriously confront money laundering. M-payments are thriving in these same areas and I believe they represent clear and present money laundering and terror finance dangers that will accelerate globally in the very near future for the simple reason that criminal networks always gravitate towards the weak link.

What Should be Done?

Similar to my earlier testimony on TBML, I am somewhat optimistic about engineering AML/CFT safeguards into M-payments. As with TBML, M-payments generate big data. Advanced analytics can be applied. For example, current fraud frameworks and security intelligence platforms are agile and can be adapted to various architectures and use cases. They are currently being used by both global banks and telecom companies for financial crime detection, public security and regulatory purposes. Technology enables identity management capabilities and risk scoring using rules, predictive models, anomaly detection, as well as link and association analysis. In short, "red-flags" can be engineered into M-payment systems that could automatically trigger alerts, suspend suspect transactions, and generate the filing of financial intelligence reports with the host country's FIU.

The worldwide growth of mobile money services does necessitate banking and telecom regulators to work together to allow mobile platforms to work. This type of cooperation is challenging. And while there will be some costs for the M-payment industry, I believe M-payment providers should welcome robust anti-fraud and AML/CFT safeguards because they cannot afford being labeled as facilitating financial crime.

Overseas, ready markets already exist for M-payment AML/CFT safeguards. I encourage U.S. data and analytics innovators to get involved. If government does not wish to take the lead, I would like to see industry or a neutral and well-respected organization or think-tank convene an open forum where concerned law enforcement representatives, regulators, representatives from mobile carriers, and big data and analytics companies can discuss both the challenges and the opportunities of engineering AML/CFT countermeasures into M-Payment systems. Perhaps an analytic solution could be developed and shared with interested mobile operating platforms and host country FIUs in the developing world. The safeguards could be made available in ways similar to the Egmont Group's "secure web" communications network and the United Nations Office on Drugs and Crime (UNODC) standard software system "GoAML" which is made available to FIUs around the world.

In addition, I believe that applicable law enforcement and intelligence agencies should heighten their awareness and reporting on the growing threat of M-payments.

As this Task Force understands, it's much easier and less expensive to take pro-active steps in the early stages of new financial threats rather than to wait and play "catch-up." We should not wait and react to a crisis if we can identify one in the making.

I appreciate the opportunity to appear before you today and I'm happy to answer any questions you may have.

---

[1] John Cassara, Testimony: "Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance;" available online at: http://democrats.financialservices.house.gov/uploadedfiles/02.03.2016_john_a._cassara_testimony.pdf

[2] 2008 International Narcotics Control Strategy Report (INCSR) Volume II on Money Laundering, U.S. Department of State; available online at: http://www.state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm

[3] "Electronic Finance: A New Approach to Financial Sector Development?" World Bank Discussion Paper 431

[4] David Runde, "M-Pesa and the Rise of the Global Mobile Money Market," August 12, 2015, *Forbes;* available online: http://www.forbes.com/sites/danielrunde/2015/08/12/m-pesa-and-the-rise-of-the-global-mobile-money-market/#663d74f723f5

[5] Roger Cheng, "By 2020, More People will Own a Phone than have Electricity," February 3, 2016, CNET; available online: http://www.cnet.com/news/by-2020-more-people-will-own-a-phone-than-have-electricity/

[6] Daniel Thomas, "Vodaphone Rings Up Record Growth on Mobile Money Platform," *Financial Times*, April 24, 2016; available online https://next.ft.com/content/0242219e-087f-11e6-b6d3-746f8e9cdd33

[7] "Advancing Financial Inclusion to Improve the Lives of the Poor," *CGAP*, available online at: http://www.cgap.org/topics/financial-inclusion

[8] 2014 International Narcotics Strategy Report (INCSR) Volume II on Money Laundering, U.S. Department of State; see entry under Mauritania

[9] 2016 State Department International Narcotics Control Strategy Report (INCSR), Volume II on Money Laundering; available online at: http://www.state.gov/documents/organization/258726.pdf

[10] Runde

[11] "The Future of Money," *60 Minutes*, November 22, 2015; available online via YouTube: https://www.youtube.com/watch?v=AHIgQttKajc&list=PL55ohbFcgaDMbY-iVxzP6cpJPDVMfDpV3

[12] 2016 INCSR

[13] Runde

[14] John Cassara, "Out of Africa – AML Compliance for Mobile Payments," June 12, 2015, *Mobile Payments Today;* available online: http://www.mobilepaymentstoday.com/articles/out-of-africa-aml-compliance-for-mobile-payments/
[15] Bethan Cowper, "Brazil is the Country to Watch for Mobile Payments," *Banking* 2015; available online at: http://www.paymentssource.com/news/paythink/brazil-is-the-country-to-watch-for-mobile-payments-3019867-1.html
[16] For more information, see "The Future of Money: Where do Mobile Payments Fit in the Current Regulatory Structure?": Hearing Before the Subcommittee on Financial Institutions and Consumer Credit, 112th Cong. (2012) (statement of James H. Freis, Jr., Director, Fin. Crimes Enforcement Network, U.S. Dept. of Treasury), available online at: http://financialservices.house.gov/uploadedfiles/james_freis_testimony.pdf
[17] 2007 National Money Laundering Strategy Report; available at: http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf
[18] Ibid