ACAMS

Combating the Proliferation of Mobile and Internet Payment Systems as Money Laundering Vehicles

Sean McCrossan, CAMS-FCI

Executive Summary

When was the last time you asked someone for directions? The last time you saw a payphone or mailed a handwritten letter to a friend? When was the last time you used the yellow book left on your doorstep for anything other than a doorstop? Actions and items woven into the daily life of the entire population have disappeared almost completely in the span of a decade or so. We saw it coming with the steady advance of technology, but just when we thought the newest advance was here, it was already behind us as innovation tends to go. Driven and funded by the promise of convenience and efficiency, from cordless phone to cell phone to smart phone, we now possess maps of everywhere, mail service, newspapers, catalogs and a seldom used telephone within arm's reach at all times. How did this all happen so fast? Did we realize it was happening at the time? Do we now?

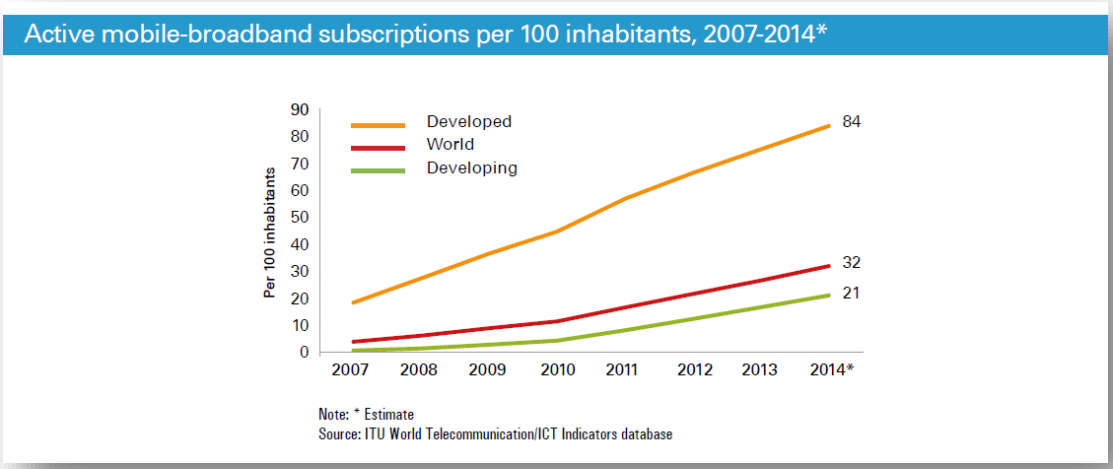
A sea change of money movement has occurred and like the tide has appeared suddenly at our feet; innovation in products and services related to mobile payments and digital currency has skyrocketed in recent years with no signs of stopping. Consumer adoption appears to be a matter of comfort; baby boomers are now comfortable with accessing financial statements and paying bills online, while their children fund tech startups and purchase digital currency from global exchanges, all from their tablets and smartphones. There is no shortage of mobile applications being developed for sending money or making payments and among the swiftest adopters of these new services are the bad actors seeking obscure avenues to launder illicit funds or finance acts of terror. How can financial institutions (FIs) and financial crimes investigators best position themselves to detect and deter misuse of these new mediums? This paper will discuss the proliferation of Mobile and Internet Payment Systems (MIPS) and the complications they present to banks and financial crimes investigators, as well as recommendations for combating their use as vehicles for money laundering and terrorist financing.

Landscape

Recent regulatory actions have caused financial institutions (FIs) to increase anti-money laundering and counter-terrorist financing (AML/CTF) staff and throw big money at software providers like never before.[i] While the analytic capabilities of AML targeted software improve in their ability to identify commonalities, transaction history and unusual flow of funds, it still remains that data presented by these systems needs to be reviewed by the careful eyes of AML investigators. The large numbers of newly minted AML analysts hired[ii] to remediate past deficiencies and avoid fresh ones require proper training, guidance and experience. Effective execution of a money laundering scheme by criminals can be difficult to spot for even the seasoned investigator. Add to that the unchartered waters presented by new payments products quickly deployed by companies looking to grab market share and AML programs may be left wondering if their view of the full transaction landscape is really that clear. The proliferation of MIPS is developing into an arms race, with telecoms and tech companies competing against FIs to bring payment systems to market. For the scope of this paper, MIPS refers to any number of Internet and mobile-based money movement channels, including peer-to-peer (P2P) mobile applications, online bill payment systems and digital currencies.

In 1998, Paypal, then Confinity, started devising mobile wallets "to enable money transfers solely on PDA's" to reduce the risk of cash being stolen, and in 2006 started allowing users to text money via mobile phone.[iii] While P2P money transfer applications have existed for some time, the global acceleration of mobile technologies has produced numerous entrants to the P2P transfer market to emerge in recent years (see Figure 1). Paypal has since been joined by the likes of Venmo, Dwolla, Square and Popmoney; even photo sharing application Snapchat has rolled out an offering for members to send money to friends. Almost all offer applications for mobile usage, some exclusively. A search of online startup site AngelList reveals a list of over 100 P2P money transfer startups alone. Part of the reason for this wave is to fill gaps in current financial product and service offerings, such as the avoidance of fees associated with sending small sums of money, convenience and financial inclusion. Investors looking to get more bang for their investment buck are also finding the meteoric rise of mobile usage a "can't miss" opportunity. The goal for these investors: the $1 trillion plus global P2P transfer and remittance market.

Figure 1-



Globally, mobile-broadband penetration will reach 32 percent (estimate) by end 2014—almost double the penetration rate just three years earlier (2011) and four times as high as five years earlier (2009). – ITU World Telecommunication

Digital currencies like Bitcoin and a legion of less familiar products are included here due to their use as an online currency and, in my view, their seemingly eventual use as a mainstream payment system. Digital currency wallet providers and exchanges, acting as money services businesses (MSBs), are the gateway to the global financial system, and users who want to avoid the risky option of meeting someone from an online ad in person to conduct a digital currency transfer, will both purchase and cash out using these providers. This is the vital point where the money trail can start or abruptly halt for financial crimes investigators and the relative anonymity of these products may prevent them from piecing together the scheme or seeing the full money laundering cycle.

The value of digital currencies for some is found in the innovation, with open source availability of transaction records and real-time settlement. Others tout these products due to their relative anonymity and decentralized nature, granting them freedom from price manipulation by banks or governments. Large scale adoption by consumers, however, has been limited, likely due to volatility and a lack of consumer protections. One indelible event in Bitcoin's short history is an example of both limitations. Customers of now defunct, Tokyo-based Bitcoin exchange, Mt. Gox, were left with no recourse after a large loss of Bitcoins as a result of cyber theft. Due to ongoing issues with U.S. regulators and the effects of the theft, coupled with problems of hubris and understaffing at the one-time largest Bitcoin exchange, the price of the fledgling currency experienced artificial inflation globally.[iv] A recent exploration by the Federal Reserve of digital currencies as a

possible component in improving the U.S. Payment System,[v] however, reveals digital currency may soon hold a more prominent place in banking and payments. Other developments including 1) the proposal of Bitcoin regulations by the NY State Department of Financial Services,[vi] 2) a Bitcoin panel at a recent NJ State Legislature hearing that saw business owners and legal experts pitch the Garden State as a development hub for the digital currency[vii] and 3) the opening of the first licensed U.S. Bitcoin exchange by online Bitcoin wallet provider Coinbase[viii] show the need for FIs and financial crimes investigators to embrace and understand digital currencies at more than a basic level.

Most FIs now offer an online service for their customers to pay service providers for standard monthly expenses. The use of these bill payment systems to transfer funds between individuals has become a common use of the system, where the payee is a third party instead of a service provider. This is significant to financial crimes investigators due to higher dollar limits in these systems compared to the P2P focused products being offered at FIs, as well as limits on many P2P mobile applications. Popular money transfer services like Western Union and MoneyGram offer this option both online and at agent locations. These systems are sometimes used by individuals to make cash payments on personal property with illicit cash, such as luxury vehicles obtained through a "straw" purchaser. These are examples of payment systems with defined, legitimate functions that may be exploited to move illicit funds.

Benefits

"Necessity is the mother of invention." This proliferation of MIPS would not be occurring without principal benefits to both user and provider. Gone are the days when employees raced to the bank branch before closing on a Friday to cash a check. Companies now avoid printing checks and their employees are saved a trip to the branch as their payroll is deposited directly into their account. Convenience is the most visible benefit of MIPS; our constant search for ways to save time coupled with technological advances have given us ever new and creative ways to achieve that goal. The evolution of convenience is continuous as friends now split bills for meals, parties and trips with one another, local organizations and school collections can manage fees and donations with applications like Cheddar Up,[ix] and companies of all sizes can pay affiliates, developers, freelancers and others with Payoneer.[x] Consumers have shown they want access to their money at all times and they want to move it both freely and with fewer associated costs. In *Business Spectator's* "What's Driving Digital Banking in 2015," Lucia Vuong states, "We live in the age of the 'entitled consumer.' These consumers expect more, trust their peers, are informed, have choices and have a voice."[xi]

The cost of sending funds has long been a hot button item for consumers and competition in the marketplace finally appears to be tilting in their favor with numerous mobile offerings

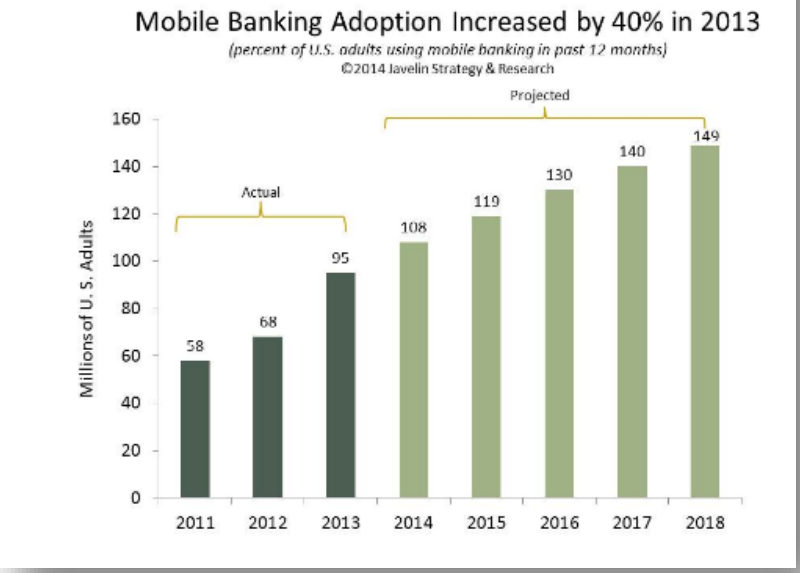
now available for sending money at no cost within the U.S. International remittances are an enormous business with many players vying for this large customer base. “Each year, an estimated 6 million households in the U.S. send billions to families, friends, and others abroad.”[xii] Exchange rates and differing fees make this market a complex one for consumers to navigate and, in recent years, some larger FIs have even rolled out targeted services to compete with well-known players Western Union and MoneyGram. Eager to keep up with the times, most international money transfer services offer their services online and some, like Skrill and others, operate a mobile platform.

Financial inclusion is quite possibly the largest reason for the global advance of mobile banking. “At least one in every 13 American households had no bank account in 2013; in households making less than $15,000 a year it was one in four.”[xiii] What almost everyone does possess, however, is a cell phone, and that technology is expanding financial services to the under and unbanked populations. The Board of Governors of the Federal Reserve System stated in a March 14, 2012, press release that, “the widespread use of mobile technology has the potential to expand access to financial services for previously underserved populations.”[xiv] This population is seeking easier ways to shop online and pay for products, while some look to avoid the risks associated with carrying or storing cash.

Risks

While the benefits of MIPS are clear, the risks are somewhat less perceptible and will vary based on a FI’s connections to products and services. The risk common to all, however, is the one presented by a lack of face-to-face interaction with the customer. In a June 2013 Guidance titled, “Risk Based Approach on Prepaid Cards, Mobile Payments and Internet-Based Payment Services,” referring to new payment products and services, the Financial Action Task Force (FATF) states, “the absence of face to face contact may indicate a higher ML/TF risk situation” and “an absence of Customer Due Diligence (CDD) increases the difficulty for the service provider to identify suspicious activity.”[xv] With each passing year, non-face-to-face interaction risk continues to heighten for FIs as the shift toward online and mobile banking steadily increases (see Figure 2).

Figure 2



Institutions using the direct banking model, known as online banks, do not operate

Figure 2 gives a view of the continued year over year increase in mobile banking in the U.S. An estimated 130 million U.S. adults will be banking via mobile in 2016, almost double the number from 2012. – Javelin Strategy & Research.

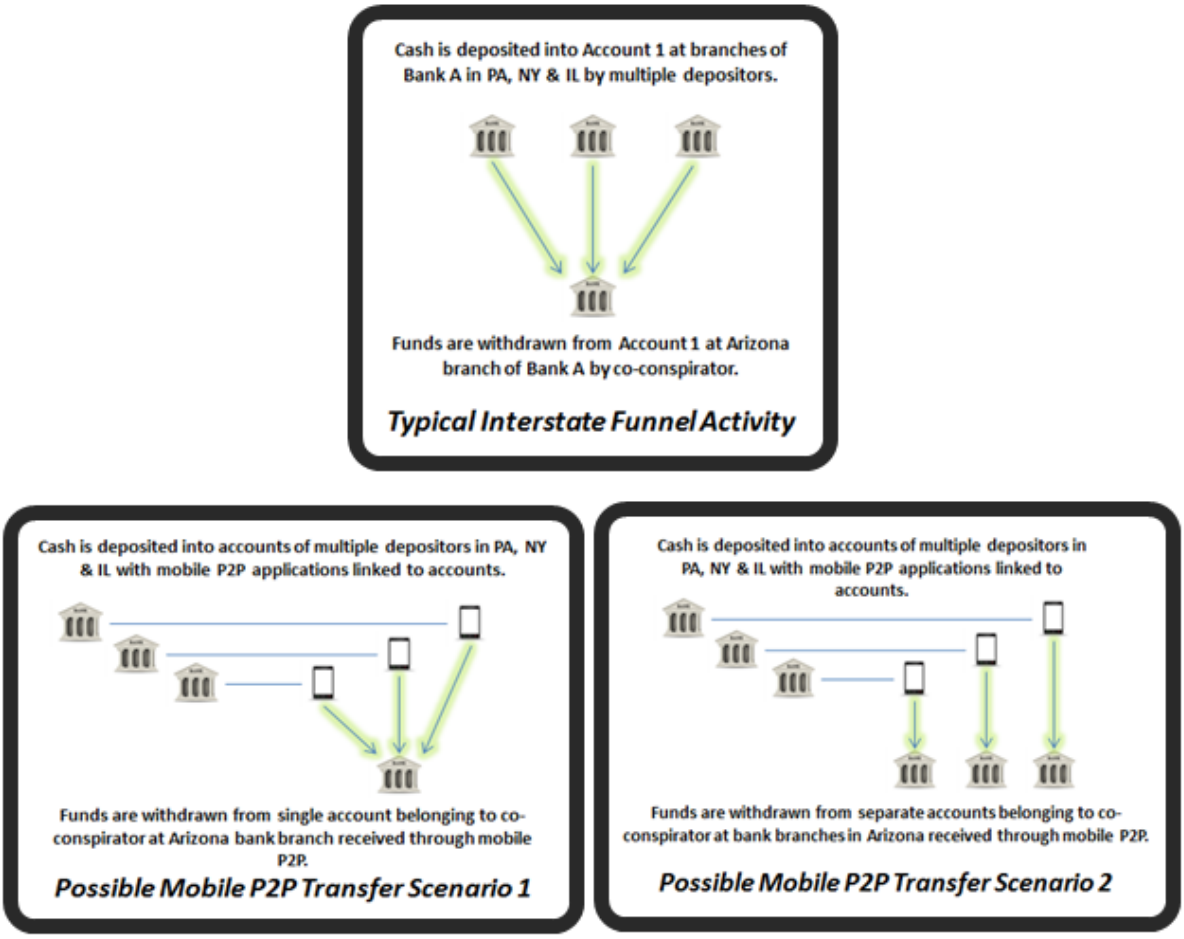
branches and are forced to place a larger focus on non-face-to-face interaction as they assess overall AML risk and implement controls. Their larger spotlight on this risk should place them in a better position to adapt to new MIPS. Some examples of the risks FIs will soon face include: 1) a mobile application set to move to market in the near future that may allow users to load a balance with cash at unmanned loading stations, avoiding the need to open a bank account; no information is available yet regarding controls, dollar limits or operation of the loading stations mentioned, [xvi] 2) a system said to allow cash payments at merchants that are converted into digital currency payments,[xvii] and 3) a mobile application for international remittances that pools funds, using a digital currency platform.[xviii] These products emphasize the potential for new risks within the fast moving MIPS space.

Criminals are rapidly embracing new products and technologies in order to further their schemes and launder their illicitly derived funds. This unintended consequence is often realized by many industries and is out of the control of innovators. The head of the Financial Crimes Enforcement Network (FinCEN) recently noted at a Foreign Affairs Forum her concern that terror group ISIS might be using Bitcoin as part of their funding,

also mentioning that, “many Bitcoin entrepreneurs, developers and startups underestimate the power of their platforms.” Another expert at the same Cryptocurrency Policy session stated, “the first adopters of new payment systems, without a doubt, are the criminals.”[xix] Whatever convenience or consumer need developers of new products seek to fill, bad actors are ready to seize a new opportunity, looking for a way to exploit and occupy territory for as long as possible before law enforcement catches on. Money laundering or terrorist financing schemes can continue long before law enforcement becomes aware or understands the scope of the problem. The recent cases of Liberty Reserve and The Silk Road online marketplace are prime examples of new technologies abused for the purposes of laundering illicit funds. In the case of Liberty Reserve, the Costa Rica-based global currency exchange created its own digital currency and employed a scheme wherein they did not accept deposits; customers instead utilized money exchangers worldwide to move funds to and from their Liberty Reserve accounts in the currency of their choice. The company is said to have laundered more than $6 billion before it was shut down.[xx] In the case of Silk Road, an online marketplace for drugs and other black market products and services accessed through the anonymous TOR Web browser, the technology of the currency and the location of the marketplace both relied on anonymity.[xxi]

The complexity of these schemes continues to increase due to the exploitation of new technologies; the previous examples should serve as a warning to financial crimes investigators to familiarize themselves with new and emerging technologies in banking and payments. The prosecution of culpable individuals and organizations, as well as further AML guidance put forth by governing bodies, starts with the identification of individual transactions and reporting of suspicious activity by astute investigators. Consider the possible evolution of funnel account activity, which incorporates mobile P2P applications; instead of cash being deposited into an account at branch locations in Philadelphia, Chicago and New York City, and subsequently withdrawn at a branch on the Southwest border in Arizona, the cash might now be deposited into multiple co-conspirator accounts and sent via mobile P2P app to multiple mobile identities controlled by one individual (see Figure 3). The geography and concentration of illicit in this scenario become difficult to identify. Identification of this and other possible future schemes involving MIPS will be the task of dedicated AML professionals.

Figure 3- Possible Variations of Interstate Funnel Activity through Mobile P2P



As banks start to restrict the deposit of cash into accounts by third parties, possible scenarios involving mobile P2P applications may be used by members of drug trafficking organizations and human trafficking/smuggling operations. In the scenarios above, accounts accepting or disbursing funds may belong to straw persons or have been opened fraudulently. Applications with the capability to send funds globally may also be used by terrorist organizations for funding.

The risk of cross-border movement of funds through MIPS varies by product; many online services exist for sending remittances and the movement of this feature to mobile platforms appears to be on the rise. The continent of Africa is currently the largest laboratory for the mobile money transfer experiment. Telecoms have taken the lead in the innovation of mobile services here, leading to large swaths of the continent skipping online banking (and personal banking in general for some) with the move straight to mobile payment platforms.[xxii] M-Pesa, an electronic payment and stored value system introduced in 2007, has revolutionized payments and money transfer in Africa. Many more applications with cross-border capabilities exist in Europe, likely due to the common

currency (eliminating the need for exchange rate algorithms) and proximity of the Eurozone countries. Few mobile P2P applications with cross-border capabilities can be found in the U.S. at this point, but that is sure to change with the scope of the global remittance business. Cross-border transfer capabilities are inherent with digital currencies; a factor that will need to be addressed with their almost inevitable integration into the mainstream banking and payments system.

Complications for Financial Crimes Investigators

MIPS pose problems for financial crimes investigators due to their increasing number and varied properties. A January 2014 post on *The Financial Services Blog* cites the renewed interest in AML (software) solutions is in part due to Internet and mobile banking technologies making the job of AML staff's more difficult and facilitating the laundering process due to increased velocity and volume of transactions, as well as the added complexity related to the transacting location.[xxiii] Financial crimes investigators are now confronted with tracking sources of funds through multiple payment channels and scores of different MIPS products. The sheer number of money transfer services can complicate financial crimes investigations; this will be exacerbated if investigators are unaware of these new products and methods. On the topic of illicit use of emerging payments systems, Michele Braun states, "Unfortunately, many of the features that provide value for legitimate transactors can also make them susceptible to misuse by individuals engaging in money laundering or terrorist financing." She notes speed of value transfer and anonymity as features making them attractive to misuse.[xxiv]

With regards to controls, online P2P services and mobile applications vary in sending/receiving limits, funding options, and personal information required to use the service; some applications even offer the option of linking one's Facebook profile as part of their verification process. In their Winter 2012 edition of Supervisory Insights, the FDIC cited possible mobile payment risks associated with record keeping, screening and reporting, and challenges satisfying AML/BSA/OFAC requirements when working with systems developed or managed by third party service providers.[xxv] While most products appear to be individually designed with basic AML compliance standards in mind, risks lie in the possible concurrent use of a wide array of products by launderers and their cohorts or their use with fraudulently opened accounts, a common tactic for launderers attempting to disguise money movement. The case of the Silk Road methamphetamine trafficking and money laundering ring, "Hammertime," charged in December 2013, revealed a combination of a fraudulently opened bank account and the use of multiple Paypal accounts, as well as Bitcoin and Western Union money transfers to move illicit funds related to their global operation.[xxvi]

Investigations involving MIPS can also be complicated by the lack of a robust transaction monitoring system or a reliance solely on basic or aged AML scenarios, especially for smaller institutions with limited budgets. Keeping track of new MIPS and understanding their potential for AML risk is a task requiring time and research. Does the institution have a touch point with the product? What are the product limits and can it store value?

Proposed Solution

My recommendation for combating the proliferation of MIPS and their current and future use as vehicles for money laundering and terrorist financing consists of the incorporation of three essential practices by AML professionals: Awareness, Dynamic Transaction Monitoring, and Enhanced KYC Processes.

- Awareness of Emerging Products, Possible Use and Associated Risks
- Foresight and Flexibility with respect to Transaction Monitoring
- Evaluation of Enhanced Processes for Online Account Opening and Customer Verification

Awareness

In the immortal words of Ferris Bueller, "Life moves pretty fast. If you don't stop and look around once in a while, you could miss it." In the cat and mouse game of financial crimes investigations, it is incumbent upon AML professionals to stay on top of emerging products and risks. Awareness is the single most important factor in battling the misuse of MIPS for laundering purposes. In the field of financial crimes investigations, the well-known security maxim holds true, "You have to know what is normal to know what is abnormal." Knowing which products and services exist, the risks they pose to your institution, and the general profile of consumers using MIPS products are key factors on which to focus. FATF Recommendation 15 on new technologies states, "Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products."[xxvii] Going forward, institutions of all sizes will need to maintain a constant and proactive approach to industry development of mobile banking and P2P transfer methods.

The formation of a team responsible for evaluation of emerging product technologies is the first step. This team, selected from within the AML ranks, would periodically research new products available in mobile and Internet banking to evaluate them for their potential risk. Risk rating should be conducted to identify overall ML/TF risk, as well as relevancy with respect to the institution's products, customers and services. For instance, an institution with credit card offerings might want to know that certain P2P mobile apps can

be loaded with a credit card to evaluate the risk of layering through their product. “Ask someone who knows.” The best place to start is usually with someone already involved in topic of research. It could be beneficial for the team to develop and maintain a relationship with the institution’s product development or user experience groups; these employees usually have both the knowledge and enthusiasm for market trends, and their finger on the pulse of the consumer. After an evaluation of products, the next step is a search of their use within the institution, followed by a sampling of customer accounts to gauge how the products are used. The periodic review by this team should conclude with recommendations to either continue with current transaction monitoring, conduct tuning to current scenarios to include newly identified activity, or explore the creation of new scenarios around products evaluated. This team’s creation will offer the institution the ability to move swiftly when risks associated with these products become elevated or with the presentation of regulatory guidance. This process will also display the proactive nature of the FI’s AML program to their regulators.

Dynamic Transaction Monitoring

Transaction monitoring conducted by institutions to properly identify potentially suspicious activity involves considerable effort and constant reevaluation. Regardless which of the myriad AML and Financial Crimes software solutions an institution employs, two crucial issues at stake are: (1) data identification and capture and (2) scenarios effectively designed to pinpoint transactions for review by investigators. Consolidation of transaction data from multiple source systems, whether in house or handled by third-party servicers, provides challenges for all institutions and the identification and capture of the proper data around MIPS is vital for appropriate monitoring. Periodic review and validation of this data is necessary to prevent gaps in monitoring. Input from investigators in the process is a valuable tool for operations groups as their research of and exposure to new MIPS may assist in the identification of transactions for inclusion into the data stream. The proper foresight and proactive approach to exploring emerging products and services will be wasted, however, if sharing between departments and implementation of data does not exist. Financial crimes investigators should also learn to interpret the data that accompanies the transactions they encounter, as data presented in new MIPS may differ from other transactions. New rules enacted by NACHA for 2015 regarding consistency in data transmission through the ACH network should assist in determining originator and beneficiary in transactions.[xxviii]

The continued release of new MIPS will require dynamic transaction monitoring on the part of FIs. Data analysis and flexibility are the keys here; the ability to evaluate the effectiveness of scenarios, thresholds and customer groupings repeatedly, and the willingness to abandon or overhaul scenarios will define the future effectiveness of AML departments. AML transaction monitoring scenarios must evolve alongside of mobile and

Internet banking technology. Analysis of standard use of MIPS by a customer base and the associated limits will be essential to creating and tuning scenarios. Scenarios based solely on dollar amount and transaction type will not be sufficient to monitor for laundering through MIPS. Items such as customer segmentation and initial threshold tuning should be explored to maximize impact; these topics are described by Protiviti in their paper, "Implementing AML Transaction Monitoring Systems: Critical Considerations."[xxix]

Carol M. Beaumier and Sujal Shah in their 2003 *ABA Bank Compliance* submission, "The Evolution of Anti-Money Laundering Compliance," state, "While transaction monitoring should be risk-based, the focus should not be on high risk transactions alone, particularly as money launderers are becoming more sophisticated and will seek ways to target an institution by using transactions that are least likely to be monitored. All transactions require a degree of monitoring and the exclusion of certain transactions from monitoring presents a risk to the financial institution."[xxx] This statement over a decade ago continues to hold true today and will hold true into the future as mobile and Internet technology changes the way money is transferred. Of specific concern is the fact that terrorist financing operations have shown to be low cost, and organizations like ISIS have recently exhibited surprising technological acumen, as shown by their use of social media platforms for recruiting and propaganda.[xxxi] Low dollar transactions involving mobile P2P that occur under thresholds requiring additional identity confirmation fit this pattern and are justification for employment of dynamic transaction monitoring.

Know Your Customer (KYC)

The third point of this multi-pronged approach to combating the proliferation of MIPS relates to established process of customer due diligence (CDD). It is the responsibility of FIs to know their customers, including collecting basic information at account opening as mandated by Title III, Section 326 of the USA PATRIOT Act[xxxii] and ongoing monitoring of higher risk accounts as recommended by the Basel Committee for Banking Supervision's *Customer Due Diligence for Banks.*[xxxiii] These directives published in October 2001 created a benchmark for account opening and customer identification programs and consistency among FIs. Opening of bank accounts online has existed since the late 1990s; however, Internet usage, and therefore volume of accounts opened in this manner, were low. That has changed though, and as non-face-to-face account openings and transactions become the norm in banking, the minimum requirements for all account openings may need to be reevaluated in the near future. Online account openings, in my opinion, warrant increased collection of personal identification. In light of the growing number of breaches of company systems involving the theft of customer information, including the most recent involving medical insurance administrator Anthem announced in January 2015, are FIs comfortable that customer acceptance processes are robust enough to thwart fraudulent account openings? Operation of fraudulent accounts is also a prime vehicle for money launderers and the possibility of large numbers of accounts opened with stolen identification used not to commit theft of funds, but solely to launder funds, may be difficult for fraud detection systems to sniff out. The risk of falling victim to such activity increases with each unsettling press release that details the increased amount of personal information pilfered from the systems of major corporations.

Collection of additional information from customers at account opening such as source of wealth, employment details and intended use of the account are very basic pieces of enhanced due diligence (EDD) that can significantly cut down on investigation time, specifically in cases that do not warrant a suspicious activity report (SAR) but otherwise are stretched out due to EDD searches to bolster support of the case disposition. Many institutions have already decided to implement requirements beyond minimums, and while this is a key factor in mitigating some of the risk associated with non-face-to-face transactions, other options should be evaluated for future implementation. With respect to ongoing monitoring of accounts, banks should know their customer individually and collectively. "An initial risk profile can only be based on customer self-reported information (e.g., expected volume, type of account, amount of business) but can be updated with information as the customer conducts banking transactions," states Volkov.[xxxiv]

A process of grouping customers into classes periodically should be evaluated to assist with dynamic transaction monitoring. Examples such as probationary periods after

opening, transaction volume levels, transaction classes and geographical activity will allow for more targeted scenarios around the use of MIPS. For business customers, FIs must also be aware of the use of business to person (B2P) payment systems like Payoneer,[xxxv] intended for the purpose of compensating employees, contractors or freelance contributors. Businesses are known to be targets of money launderers and the potential for misuse of MIPS by cash-intensive businesses or shell companies through fabricated payroll transactions is a possible risk.

Another unknown to consider as banking technology evolves is the profile of the digital currency user. Can we properly define this customer yet? How do we differentiate between speculator, enthusiast and online drug trafficker? With the negative news in recent years and the inherent product risk associated with digital currencies, if FIs are not

If FIs aren't currently monitoring for or exploring the creation of scenarios around digital currency, they are already behind the curve.

currently monitoring for or exploring the creation of scenarios around digital currency, they are already behind the curve. The intelligence gathered therein will be necessary in the future as those value transfer methods become mainstream and continue to adapt; now is the time to start collecting that data.

Other future possibilities to consider regarding customer identification at account opening and EDD might include the use of products that incorporate visual identification or further verification through matches on social media. Cloud biometrics company, BioID, offers multimodal biometrics authentication solutions for online login, transaction authorization and mobile payments.[xxxvi] We have already seen P2P applications start to verify account ownership through Facebook, and Open Identity Exchange's, "Investigating Challenges in Digital Identity" explored the possible use of mobile phone data and social media history as factors in establishing a digital identity for individuals with a low-level identity footprint.[xxxvii] As a society, we are increasingly identified by our online presence and in the not too distant future may find verification by these sources outpacing those of public records tools. Financial crimes investigators are already relying significantly on Internet search tools to corroborate customer employment and wealth and, as online sharing by customers increases, so will identification by digital profile. This is just the beginning of numerous changes to come in digital identification and verification.

Conclusion

The risk-based approach advocated by AML governing bodies and authorities worldwide for the mitigation of money laundering and terrorist financing is pragmatic and often the most efficient option for AML departments continually forced to do more with less. We need to recognize, however, that significant risks lie in the unknown, and both payments and money transfer systems continue to evolve as we attempt to contain yesterday's threat. Criminals and terrorist financiers are repeatedly modifying their techniques to stay ahead of law enforcement and are not afraid to utilize unique or experimental products and services. The drug trade, human trafficking, and cyber-based crimes are not abating, kleptocracy and tax avoidance schemes will undoubtedly continue, and new technologies involving money transfer, as well as the global acceptance of mobile and Internet banking, will facilitate the perpetuation of these crimes. Regulators will assuredly be interested in an institution's monitoring of MIPS before long and as FIs continue the shift toward mobile products and services or work with third parties that provide these, AML/CTF professionals must understand that the old way of looking at things will not last. Ardent and perpetual awareness of the ongoing changes in the mobile payments and money transfer landscape, a willingness to employ dynamic transaction monitoring, and re-evaluation of how customers are onboarded and verified are the roadmap to combating the proliferation of mobile and internet payment systems as money laundering and terrorist financing vehicles.

Works Cited

[i] "According to IDC Financial Insights, worldwide spending on risk and compliance technology will reach $79.2 billion in 2015. - See more at: http://www.pega.com/insights/articles/3-key-regulatory-trends-will-affect-your-it-investment-budget-2015#sthash.aW8ZyVId.dpuf" & "Transaction monitoring systems continue to represent the greatest area of AML spending" http://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf

[ii] http://www.complianceweek.com/blogs/scuttlebutt/hsbc-to-hire-thousands-more-compliance-employees# and http://www.wsj.com/articles/SB10001424052702304163604579531263107487566

[iii] https://www.paypal-media.com/history

[iv] http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228

[v] "Strategies for Improving the U.S. Payment System." Federal Reserve. 23 January 2015. Web. 26 January 2015.

[vi] http://www.coindesk.com/new-yorks-proposed-regulations-mean-bitcoin-businesses/

[vii] http://www.innovationnj.net/innovation-news/bitcoin-panel-seeks-new-take-on-regulation-at-new-jersey-hearing

[viii] http://www.wsj.com/articles/first-u-s-bitcoin-exchange-set-to-open-1422221641

[ix] http://www.cheddarup.com/

[x] http://www.payoneer.com/

[xi] http://www.businessspectator.com.au/article/2015/1/13/technology/whats-driving-digital-banking-2015

[xii] www.consumer Reports.org/cro/2012/03/the-best-way-to-send-money- abroad/index.htm

[xiii] http://www.economist.com/news/briefing/21632441-worlds-poor-need-stability-and-security-banks-have-traditionally-offered

[xiv] http://www.federalreserve.gov/newsevents/press/other/20120314b.htm

[xv] "Guidance for a Risk Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services." Financial Action Task Force (FATF). June 2013.

[xvi] http://www.myecheck.com/services/mobile-services/

[xvii] http://www.coindesk.com/ripple-labs-now-taking-cash-payments-zipzap-snapswap/

[xviii] http://www.zipzapinc.com/zed/

[xix] http://bitcoinexaminer.org/us-treasury-fears-islamic-state-using-bitcoin-fund-terrorist-activities/

[xx] http://www.insightcrime.org/news-analysis/liberty-reserve-case-exposes-new-frontiers-in-laundering-digital-cash

[xxi] http://www.insightcrime.org/news-analysis/liberty-reserve-case-exposes-new-frontiers-in-laundering-digital-cash

[xxii] http://recode.net/2014/07/24/disrupting-payments-africa-style/

[xxiii] https://blogs.oracle.com/financialservices/entry/aml_the_next_frontier

[xxiv] "Understanding Risk Management in Emerging Retail Payments." Michele Braun. 25 August 2008.

[xxv] "Mobile Payments: An Evolving Landscape." Federal Deposit Insurance Corporation (FDIC). Supervisory Insights. Winter 2012. https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/SIwinter12.pdf

[xxvi] http://www.deepdotweb.com/2013/12/19/silk-road-vendor-hammertime-busted/ and http://www.golocalpdx.com/news/portland-is-a-hub-for-online-drug-dealers

[xxvii] "The FATF Recommendations." Financial Action Task Force (FATF). February 2012. Recommendation 15. Pg. 16.

[xxviii] "Person-to-Person Payments via ACH." NACHA. https://www.nacha.org/rules/person-person-payments-ach

[xxix] "Implementing AML Transaction Monitoring Systems: Critical Considerations." Protiviti. 11 January 2013. Pg. 4.

[xxx] "The Evolution of Anti-Money Laundering Compliance." Carol M. Beaumier and Sujal Shah. Pg. 17. http://www.aba.com/products/bankcompliance/documents/septoct03coverstory2.pdf

[xxxi] http://www.nytimes.com/2014/08/31/world/middleeast/isis-displaying-a-deft-command-of-varied-media.html

[xxxii] http://www.fincen.gov/statutes_regs/patriot/index.html?r=1&id=326#326

[xxxiii] "Customer Due Diligence for Banks." Basel Committee on Banking Supervision. October 2001.
[xxxiv] "AML Transaction Monitoring- Corruption, Crime & Compliance." Michael Volkov. Blog. 13 June 2013.
[xxxv] http://www.payoneer.com/
[xxxvi] https://www.bioid.com/Solutions/Mobile-Payment
[xxxvii] "Investigating Challenges in Digital Identity." The Open Identity Exchange (OIX). 2 July 2014.