Taking a Proactive Approach to Monitoring and Investigating Emerging Threats in Money Laundering

By: Zachary C. Miller, CAMS

CAMS-FCI Advanced Certification White Paper

August 2014
Executive Summary

The volatile world of anti-money laundering (AML) and combating financial terrorism (CFT) is ever-changing, and the “bad guys” are always at least one step ahead of law enforcement and compliance professionals’ efforts. With each passing day, it is evident that payment channels, legal interpretations and other factors create opportunities for money launderers and financiers of terrorism to get creative with their movement of funds. As AML professionals, what steps can we take to be more proactive in monitoring and reporting emerging types of suspicious activity and threats to our financial system?

Those in the AML/CFT landscape understand criminal activity is ever-evolving and usually ahead of the curve compared to everyone else. As financial institutions struggle with meeting regulatory requirements and expectations while juggling a large and increasing workload, sometimes with minimal resources, and levels of support from senior management that vary greatly, they should still take the time to monitor and investigate new money laundering threats and methods, even when formal regulations have not been established or enacted. After all, many AML professionals have seen that adaptability is possibly the most important trait that a BSA officer or investigator can possess in the post-9/11 world.

The purpose of this white paper is to provide financial crimes investigators in financial institutions insight into some emerging trends and help them understand the importance of being proactive in monitoring and investigating new types of potentially suspicious activities even before any or minimal official regulatory rules or guidance is available. This paper will focus specifically on virtual currency and interstate funnel accounts as two areas of current concern provoking discussion. The goal is for investigators to understand how to gain new insights into emerging threats and the activities related to those threats as trends in the world of financial crimes change and develop monitoring thresholds, focusing on red flags. Making these adjustments will also create preparedness when regulations eventually lay out the requirements for monitoring these areas.

After all, many AML professionals have seen that adaptability is possibly the most important trait that a BSA officer or investigator can possess in the post-9/11 world.

Background

First, this paper will examine some of the new and current primary areas of concern for AML/CFT, keeping in mind that the issues change from year to year. Obviously, it would be
impossible to cover every threat or scenario, and each institution will have a different level of risk associated with the different topics being discussed.

In the interest of time, the focus is primarily on two major areas all financial institutions should be concerned about presently: virtual currency and interstate funnel account activity. Both of these examples represent potential threats for money laundering and terrorist financing, and we have already seen how both have been used to carry out the work of individuals and organizations involved in drug trafficking. Both have also received significant attention from news outlets and FinCEN, which indicates that financial institutions should be taking notice. The level of attention institutions give to these areas may vary depending on size, scope and risk appetite. Nevertheless, all institutions will have some level of responsibility to understand and manage the risks associated with both virtual currency and funnel accounts.

**Virtual Currency**

Regardless of the name being used, whether it is digital currency, virtual currency, or any other forms of those words, one thing remains clear: These crypto-currencies represent perhaps one of the most polarizing issues in the financial world today, and certainly one of the biggest issues AML professionals are currently facing. In speaking with AML professionals about what virtual currency is and for what purposes it can be used, one will hear a variety of opinions. Some think that virtual currency is the most innovative and greatest thing to happen in payment methods since the invention of paper money. Others see it as the downfall of today’s banking system. The fact is that virtual currency is here, and as the industry adapts with how to use and handle it, more and more consumers and businesses will seek to use it to facilitate both legitimate and illicit transactions. It will be the responsibility of AML professionals to take this payment channel and any funds flowing through it into account when determining best practices for their suspicious activity monitoring programs.

Although multiple names and definitions are used to discuss virtual currency, generally speaking, it is a form of electronic money that is not backed by any legal tender. Therefore, “it covers the digital representation of value that can be traded and functions as a medium of exchange, store of value or unit of account but does not have legal tender status” (IOM Today, 2014). The value of most virtual currencies, including Bitcoin, which is perhaps the most popular and well known, is perceived by its users and is typically assigned based on
mathematical equations and the number of units in circulation. Others have entered the market with varying degrees of success and values including Litecoin, Dogecoin, and Darkcoin, as have those especially designed to handle the flow of funds for marijuana-related businesses in the U.S. such as Potcoin and Dopecoin. With each passing year, more and more types of virtual currencies are being introduced. While there have been many success stories and seemingly endless possibilities for positive use of virtual currency, one need look no further than the U.S. Justice Department’s money laundering cases against Liberty Reserve (DOJ-Criminal Division, 2013) and the Silk Road (Greenberg, 2014), as well as the hacking and subsequent bankruptcy filing of Mt. Gox (Maglich, 2014) to understand that the risks and potential for illegal activity is equally great.

Speaking first to U.S. centric regulations, the Federal Financial Institutions Examination Council BSA/AML Examination Manual (FFIEC exam manual) was last updated formally in 2010 and therefore does not specifically reference virtual currency. However, it does cover an overview and examination procedures for electronic cash or e-cash. The exam manual describes e-cash as “a digital representation of money,” which “comes in several forms, including computer-based, mobile telephone-based, and prepaid cards.” The closest item related to virtual currency is probably computer-based e-cash, which is described in the exam manual as being “accessed through personal computer hard disks via modem or stored in an online repository” (FFIEC, 2010). This mostly fits the description of Bitcoin and other virtual currencies, which require the creation of a digital wallet to store the represented value. As such, there is an obligation to take a risk-based approach to monitor e-cash in any form, but the recommendations are a bit open-ended and not specific to virtual currencies in the sense being discussed in this paper.

FinCEN has taken a stance to identify and mitigate some of the risks associated with virtual currency by issuing guidance aimed at how institutions, at least in the U.S., should handle individuals or businesses engaged in money transmitting services associated with Bitcoin and other virtual currencies. This is helpful as it defines users, exchangers and administrators. It also outlines what financial institutions might do to ensure that their customers who may be acting as exchangers or administrators are properly registered as money transmitters or give them the option to stay out of that line of business, similar to how many financial institutions have moved away from banking money services businesses (MSBs) in recent years. This also depends on the state, as each state may have different rules or regulations related to money transmitters. In terms of actually monitoring transactions and reporting suspicious activity related to Bitcoin or others, the regulators have not yet provided the exact roadmap that AML professionals are supposed to follow.

Internationally speaking, the Financial Action Task Force (FATF) has indicated they are only in the early stages of developing international standards and recommendations to handle the
emerging payment method. The nature of virtual currency makes it a global issue—one that must be addressed at the level of the FATF before it can be truly tackled at the individual country level, in terms of regulatory best practices. However, each individual country seems to be handling Bitcoin and others in their own way, whether it is banning their use in countries like Iceland and Vietnam, or developing rules related to taxation and regulation. This clearly shows how the rapid changes in the virtual currency realm makes it nearly impossible to establish formalized guidance across the board at this time and that includes guidance that should be applied first on a worldwide level, then within a country, and finally within individual institutions.

**Interstate Funnel Accounts**

As of the time of this writing, interstate funnel accounts, or simply funnel accounts, present a large concern for FinCEN in the U.S., as evidenced by the advisory FIN-2014-A005 made public on May 28, 2014. Funnel accounts are used to conduct rapid movement of funds by making deposits in one geographic region followed by withdrawals initiated by a different individual in a different geographic region. According to the advisory, actions taken by the Mexican and U.S. governments during 2010 to restrict U.S. currency flowing through the Mexican financial system have popularized the use of funnel accounts as a method to launder proceeds from illicit activities, such as narcotics trafficking, human smuggling and trade-based money laundering (TBML). This shows that the criminal factions are mixing both earlier money laundering schemes with the newer methods through the use of structuring and third-party actors and although this issue is primarily a problem for the U.S. and Mexico, it could be for other regions as well.

FinCEN has done an effective job issuing communication related to this situation and has detailed the method, along with examples of how it may be employed. Due to this communication, AML professionals have a better sense of the types of red flags they should be looking for, the various offenses that may be committed, and the types of institutions and situations that may have the biggest risks associated with this method of money laundering. The scheme involves drug trafficking organizations from both the U.S. and Mexico and their use of “straw” account holders and structuring to keep their activities under the radar as much as possible. Structuring plays a major part in the activity. With the FinCEN information, AML professionals have been provided the tools they need to begin more proactively monitoring; however, it is still a subject that is not addressed in the FFIEC exam manual. Many automated and manual monitoring systems need to be updated to accommodate scenarios or behavior based rules to adequately capture this activity.
Challenges

These two examples represent (1) a situation where minimal official guidance is available and (2) a situation where enough communication has been delivered to begin work immediately. In both cases, however, challenges in proactively creating monitoring thresholds and applications still exist. Issues exist in managing overall workload, resources allocated to AML compliance, varying levels of support from senior management depending on the institution and managing any underlying regulatory expectations. It is important for each financial institution to analyze each of these challenges to determine if any need to be addressed in greater detail.

Workload

Most AML professionals with several years of experience would agree that their workload has increased from the time of their introduction into the AML realm and continues to trend upward. With so much scrutiny being placed on compliance departments and their ability to effectively and accurately maintain their AML programs, it may be perceived that adding new layers to an already (hopefully) robust suspicious activity monitoring program is more trouble than it might be worth. This becomes especially challenging considering the speed with which changes in the world of money movement and criminal enterprise are taking place in an increasingly digital age. Specific to workload, some challenges of developing and monitoring for suspicious activities conducted through virtual currency and funnel accounts may include:

- The complexity of cases involving new trends – There is inherently less knowledge and experience dealing with the red flags associated with virtual currency and funnel accounts.

- Number of affected accounts – This is an unknown piece of information at the beginning of the process and will have a direct impact on the amount of work that will be necessary.

- The inability to easily identify the appropriate parties that need to be investigated – With the anonymous nature of Bitcoin and many other virtual currencies and the various parties used to facilitate funnel account activity, simply finding a subject for investigation presents a significant challenge.

Resources

Hand in hand with workload is the issue of having sufficient resources in compliance departments. The ability to handle the workload, which includes filing CTRs, administering a suspicious activity monitoring program, risk reporting, high-risk customer monitoring, OFAC
monitoring and various other responsibilities depending on institution size and scope, is immediately effected by the amount of resources that can be given to that area. Budget constraints are always a concern in today’s economic landscape, but departments that can attract and retain enough quality talent, invest in systems, and spend time and money in training and development will have a better chance to manage the workload in a way that creates the opportunity to consistently enhance and improve upon the already existing processes. Resource challenges may include:

- Number of staff dedicated to investigations – The complexity of cases and the number of accounts impacted may facilitate the need to hire additional investigators.

- Dedicated individual(s) with adequate technology/application support expertise to build and maintain ongoing reports – Qualified personnel will need to search for specific word strings in transactions, transactions occurring across multiple jurisdictions and transactions involving multiple or unidentifiable conductors.

- Training – New and existing staff will require advanced training to be able to understand how virtual currency works including how to set up virtual wallets, exchange funds and convert back and forth between virtual and real currency. Investigators in both small and large institutions will need to be trained to understand the inner workings of funnel account usage and how the activity may be facilitated in any institution regardless of size.

_Senior Management Support_

Resources will be directly impacted by the level of support from senior management and the board of directors. Developing a compliance culture within the institution from the top down and recognizing the need to provide the appropriate resources to AML can keep the institution running smoothly as regulatory pressures mount. This becomes especially clear considering the sheer number of consent orders and the size of the civil money penalties levied since the beginning of the financial crisis in the U.S. More often than not, the management of financial institutions that have already been through the burden of remediation or paid penalties is now acutely aware of just how important their compliance efforts are and that their support can mean the difference between the ship sinking or staying afloat. Remember: When speaking to senior management about resources allocated to AML, point out that while it may be seen as a cost, AML compliance keeps hard earned money in the institution by saving the institution from paying legal fees, consulting fees and penalties. Also, and perhaps more importantly, senior management should recognize the value of the partnership between the money making lines of business and compliance-related functions based on the compliance department.
management’s ability to show them that while challenges may be present, they are not impossible to overcome (Cocheo, 2014). Education for senior management/board of directors will be required so that they can understand the schemes at a high level and be aware of the compliance area’s needs to adequately address them.

Also, and perhaps more importantly, senior management should recognize the value of the partnership between the money making lines of business and compliance related functions based on the compliance department management’s ability to show them that while challenges may be present, they are not impossible to overcome.

**Regulatory Expectations**

Regulatory expectations may be directly attributed to formalized guidance or advisories, or may be somewhat indirect and based on current trends and typologies. From a regulatory perspective, AML professionals are in fact expected to remain abreast of new developments in financial crime, payment methods and money laundering schemes. Of course, these expectations should drive the institution’s board and senior management to make available the appropriate resources to help manage the workload associated with AML compliance. To this end, the challenges presented may appear independent, but they are directly related to one another and each piece of the puzzle must be present in order to begin to develop a proactive approach to emerging threats in money laundering for the financial institution.

**Solution – How to be Proactive**

**Evaluate, Identify**

Periodically evaluating the existing model and identifying areas of concern is the first step to establishing an up-to-date and forward moving suspicious activity monitoring program that continually addresses new and emerging threats. The thresholds for defining what makes a review “periodic” differs from institution to institution based on a variety of factors and considerations. Decide if the best course of action is to review annually, semi-annually, monthly, on an as needed basis, or some combination of these. This may involve several items of interest including, but not limited to:

- Analysis of institution-specific activities and customer base that is also used to update the risk assessment. This may include reviewing new products and services for their money laundering vulnerabilities, even after they have been risk rated and
implemented. What products or services may be used to facilitate virtual currency transactions and will the institution allow it?

- Up-to-date management of high-risk customer types, including methodologies for determining new types of customers to be added.

- Continuous monitoring and enhancements to the institution’s list of high-risk geographies, both within and outside of the country of operations. Which regions within the financial institution’s footprint are more likely to be targeted by funnel account users?

- Utilizing communication from regulators, law enforcement, financial intelligence units (FIUs), and the news media to identify areas of growing concern as they are recognized. Leverage information like FinCEN’s guidance on funnel accounts to begin building a monitoring plan (FinCEN, 2014).

- Recognizing emerging trends within the institution’s footprint or customer base through comprehensive analysis of the results of suspicious activity monitoring programs and high risk customer monitoring.

In addition to these and other factors, the importance of maintaining a risk-based approach is critical to success. Consider the size and footprint of the organization, the customer base, products and services offered and the level of capability in the compliance department to take on additional monitoring. Essentially, consider the risk assessment and what valuable information it can offer regarding what is being done currently, and where the institution’s AML risk profile may be headed. The current risk assessment may need to be updated to address concerns regarding virtual currency and funnel accounts and how the compliance area will begin their monitoring process and report findings.

Determine what guidance is or is not available on the topics of concern. Specifically referencing virtual currency and funnel accounts, it is obvious that there are varying levels of communication from regulators regarding how these issues should be handled. For example, the FFIEC exam manually lists risk factors for e-cash, which can be a starting point for placing monitoring controls around virtual currency:

- Funds may be transferred to or from an unknown third party.

- Customers may be able to avoid border restrictions as the transactions can become mobile and may not be subject to jurisdictional restrictions.
• Transactions may be instantaneous.

• The customer may perceive the transactions as less transparent (FFIEC, 2010).

Using these risk factors as a preliminary roadmap, the additional risk factors should become more clear by conducting further due diligence on the topic, outside of the exam manual. In the case of funnel accounts, no FFIEC guidance is yet available, but the FinCEN advisory and communications has clearly outlined what kinds of red flags and risk factors the agency has already seen and what they expect the activity to look like at this point and in the immediate future. Consider which aspects of the activity relate to previously identified methods of money laundering, so that the new and innovative parts of the schemes become clearer. Take note of international standards first, look at standards specific to country/region, followed by regulatory rules/expectations, and then develop internal policies and procedures around these considerations.

Specifically referencing virtual currency and funnel accounts, it is obvious that there are varying levels of communication from regulators regarding how these issues should be handled.

Update, Create, Implement

After taking the time to evaluate and determine the areas of concern to be added to the existing suspicious activity monitoring program, a number of key considerations come into play. Focus on the specific threats and determine what is already in place that may help capture the information needed. If the existing resources cannot adequately accomplish the objective, look for new options within the constraints of the program’s current workload and resource level.

• What systems are currently in place? Many shops have moved to a model with some combination of manual and automated transaction monitoring. Larger institutions may be mostly automated while small to mid-sized shops may still be working on a primarily manual system. Can either system search for a string of key words or phrases within the transaction information, or does it simply identify dollar amounts and transaction types?

• Are systems and thresholds current enough to catch suspicious activity? Regardless of the institution’s systems being automated, manual, or a combination, they need to be kept up to date and periodically validated to ensure that data integrity and quality in the results is being taken into account. Automated systems may or may not possess the
ability to add new rules or scenarios that would specifically identify new areas of concerns. Are appropriate thresholds in place to identify conductors of transactions and is that information easily obtainable? For example, when examining funnel account activity, has the institution taken steps to collect information on the conductors of cash deposits, even if they are below the CTR reporting threshold? Many institutions may decide to collect cash conductor information for any cash transactions above $3,000. Others may choose to do so for any cash transaction of any amount. The institution should make a risk-based evaluation of the effectiveness of their threshold and determine if it may need to be revised. With funnel account activity, it may be prudent to examine lowering conductor thresholds to more accurately identify responsible parties. In other words, do the systems have the capacity to be updated to address new and emerging threats?

- Who is responsible for developing rules or monitoring thresholds? Many AML professionals wear multiple hats. Depending on the workload and resources allocated to the AML program, it may be beneficial to designate an individual(s) who is solely responsible for data, systems and technology. This type of individual is the perfect candidate to also assist the BSA officer or manager with data analytics and program governance. Using that knowledge base and always considering the risk assessment, a person in this capacity will be acutely aware of all of the data that is accumulated and processed for AML monitoring and should be able to pinpoint effective starting thresholds and testing methodologies to maximize the output of any new monitoring tools.

- What rules or scenarios need to be updated or created and how they will be monitored? Consider transaction types and payment methods that should be included. Examine accounts with activity that hits multiple geographic jurisdictions, as well as accounts where “classic” red flags such as structuring or unusual wire transfers are taking place. It is important to take into account what is happening on the front line as new account relationships are established and institutions have the opportunity to risk rate customers at onboarding. Implementing account opening questions focusing on expected activity which can be compared to actual activity should provide valuable knowledge to supplement the rules based or behavior based transaction monitoring systems being used.

- How should training be addressed so that investigators understand new and emerging threats and how to investigate them? The importance of ongoing training and
development of AML staff cannot be understated. An AML training plan should be developed and executed across the institution to address all levels of staff and updated on an annual basis at the very least. The training should target the specific audience and how each area of the institution comes into play when addressing compliance. A variety of sources should be used to develop the training information, and AML professionals should leverage their partnerships with law enforcement to try to obtain quality intelligence that is as current as possible.

- How does staff keep up with the challenges? Provided that the institution has a strong level of support from senior management and the appropriate resources, the goal is to attract and retain a team of people who are innovative, adaptable and relatively tech savvy. These traits need to be supported by critical and analytical thinking, and a mind for investigating both the obvious and more hidden aspects of transactional activity. As the profession of AML compliance gains more and more attention in the wake of the increasingly strict regulatory world, the field will become more specialized with long time AML practitioners and individuals with backgrounds in criminal justice, law enforcement, statistics and data analytics differentiating themselves as the most desirable team members. As time passes, individuals with previous experience working with payment systems specifically related to virtual currency may become increasingly attractive to compliance teams.

**The Benefits of Being Proactive**

Regulatory expectations drive the majority of the work performed in AML compliance departments or their equivalents throughout the country and the world. This is especially true in the growing number of institutions that have already remediated deficiencies in their programs as identified in enforcement actions. Staying a few steps ahead by implementing monitoring controls of emerging money laundering and terror financing threats will usually illicit a desirable response from examiners who like to see that the institution is not just resting on its laurels when its core program has already been deemed sufficient. As a general rule, identifying these areas will cut down on the number of items an auditor or examiner will list for areas of improvement in their final report letting senior management know that all of their support was properly placed.

However, it is important to never lose sight of this primary objective: supporting the efforts of law enforcement in an attempt to protect the financial system. This may be segregated, based on country, but is ultimately a worldwide issue. Time and time again, FinCEN and law enforcement agencies tout the importance of suspicious activity reporting and how beneficial the information is for their efforts. Proactively monitoring and reporting suspicious activity
related to newer and emerging trends in money laundering gives law enforcement the opportunity to leverage the invaluable data financial institutions can make available. AML professionals should be making a point to develop communication and partnerships with law enforcement professionals, especially within their institution’s footprint. This will allow for a greater understanding for both parties on the activities requiring immediate attention, and those that represent a gradual, yet meaningful change in previously identified issues. With law enforcement feedback, the quality and usefulness of suspicious activity reports can be optimized for the benefit of both parties.

**AML professionals should be making a point to develop communication and partnerships with law enforcement professionals, especially within their institution’s footprint.**

**Conclusion**

The challenges faced by AML professionals are many, and that in itself is not a novel concept. However, illicit actors remain on the cutting edge of new schemes and are exceptionally adept at utilizing new methods to accomplish their goals. As such, it is incumbent upon all financial crimes investigators to assess the issues, identify opportunities to enhance existing programs, leverage support to gain the resources to manage the workload and establish the partnerships with law enforcement to provide the most meaningful assistance possible. We must take advantage of our skill sets and be as adaptable and innovative as possible if we have any hope of keeping up with those whose greed and lust for personal gain is far greater than one’s own. At the end of the day, proactively monitoring emerging threats in money laundering and terror financing is one of the AML professional’s contributions to the fight against financial crime.

**At the end of the day, proactively monitoring emerging threats in money laundering and terror financing is one of the AML professional’s contributions to the fight against financial crime.**
Works Cited

http://www.ababj.com/component/k2/item/4709-you-can-t-be-dr-no-anymore/4709-you-can-t-be-dr-no-anymore


