Journal of Strategic Security

Volume 6
Number 5 *Fall 2013 Supplement: Ninth Annual IAFIE Conference: Expanding the Frontiers of Intelligence Education*

Article 30

Red Flags and Black Markets: Trends in Financial Crime and the Global Banking Response

Barry Peterson
Wells Fargo Bank - Global Financial Institutions

pp. 298-308

Red Flags and Black Markets: Trends in Financial Crime and the Global Banking Response

Barry Peterson

Introduction

In the broad spectrum of issues within the field of intelligence and national security, perhaps no single issue is less well understood or focused upon than finance. The international banking and financial systems play a key role in every aspect of terrorist financing, money laundering, embezzlement, corruption and illicit trade. However, given the nature of globalization, international markets and multilateral jurisdictions, countering these threats cannot be left up to national security establishments and agencies alone. Rather, these agencies rely heavily on the banking and financial services community itself. In this respect, the private sector bankers, financial analysts, risk managers and so forth work every day on the front line against money laundering, terrorist financing and other white collar crimes.

This report will focus on only a few key factors which are most commonly addressed within the non-governmental anti-money laundering (AML) and counter-terrorism financing (CTF) operations. First, a general overview of the issues will be presented including brief descriptions of some of the most historically popular methods and means by which illicit funds are transferred around the world for criminal intents. Second, a more in depth analysis will be presented on what private sector actors (banks) currently do and what tools are at their disposal for conducting proper AML/CTF research and analysis. Finally, we will address a number of new concerns, issues which are predicted to present new challenges to AML/CTF and present ideas as to how these new threats may be countered in the future.

While it may be logical to demonstrate the separations between AML and CTF, the reality is that the two issues are irrefutably linked to one another. Although the two do not necessarily overlap in all cases, the means by which the two interact and benefit each other are demonstrable. Money laundering may take the form of embezzlement to hide proceeds of corruption, introducing funds from criminal enterprises into legitimate banking, or simply the transferring of funds to or from parties on known criminal or terror watch lists.

Illicit funds flow daily to and from points all over the world. The purposes of these funds vary as widely as the individuals and organizations taking part. Classic perpetrators of these illicit transfers are transnational criminal organizations (TCO), corrupt government officials, terrorist organizations, and individuals seeking to disguise the proceeds of illegal activities such as embezzlement. Wire fraud may be one of the most common methods by which these illicit transfers are conducted, but they are by no means the only. Credit card fraud, paper instrument fraud (travelers checks, money orders), over- and under-paying for goods and services and trading in hard commodities are all effective ways of injecting illicit funds into the licit financial system.

Wire Transfers

The most obvious and well-documented means by which this is accomplished is through processing of wire transfers. As recent history has shown, wire transfers have become a preferred method for moving illicit funds both internationally and internationally. Globalization has allowed wire transfers to be sent and received instantaneously by more and more individuals and business entities. As access to the international banking system increases, so too has the ability to utilize these wire transfers for illicit means. Migrations and worldwide travel have led to increased remittance payments to home countries, increased payments for goods and services and increased threat of laundered money. The very nature of wire transfers is what makes them both economically efficient as well as amenable to money laundering, making them desirable for both legitimate and illegitimate users.

Money-laundering by wire transfer is one of the most common types of money laundering, owing to the relative ease and speed with which these transactions can be completed. The immediacy of these transfers also makes tracking them after the fact exceedingly difficult. As a result, pre-emptive actions must be relied upon in order to attempt to catch illicit transfers before they can be sent. In order to do so, bank employees including AML and compliance departments as well as bankers and even customer-facing tellers must be trained to recognize suspicious activity and to be knowledgeable in how to report that activity.

A number of red flags are often spotted in wire transfer data which should be key indicators of suspicious activity. These red flags may include transfers between business entities in wholly unrelated industries with no legitimate reason for conducting transactions, transactions for unusually large dollar amounts, transfers to high-risk countries, transactions involving off-shore banks or tax havens, and transfers involving downstream banking activity. The most obvious red flags that should be spotted in wire transfer data involve the entered data itself. Missing data, empty data fields, unusual entries, repeated suspicious transactions, repeat occurrences of suspicious names, inclusion of references to cash payments and transactions involving industries previously known to be utilized for money laundering should all be noted.

When a particular industry or customer base is better known, another key indicator may be the apparent over- or under-payment for goods and services. For example, if a particular company has been known historically to process $1 million in wires to another party for a set amount of goods, analysts should be especially mindful of the occasion in which that payment suddenly jumps to $2 million, or $5 million or some other drastically increased value with no obvious purpose. This may be evidence of overpaying for goods which will then be sold in legal markets, thereby reintroducing those funds into the licit market.

AML professionals have noted a number of key industries in which money laundering seems to be most popular. These industries are widely varied and seemingly innocuous. Example include used car imports and exporters, flower shops, precious metals companies, real estate, recycling and industries historically involved in predominantly cash based transactions such as bars, nightclubs and casinos.[1] One of the most pressing concerns for AML work today involves currency exchange house, currency brokers, and illegal conversion markets for local currencies into U.S. dollars. Money laundering through Mexican *casas de cambio* involved *peso* deposits

[1] Diana Valdez Washington, "Drug cash fuels money laundering," *El Paso Times*, August 5, 2012.

http://scholarcommons.usf.edu/jss/vol6/iss5/30
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.28

followed by transfers into bank accounts denominated in dollars. From a U.S. perspective, this problem has been especially evident along the southern border, where cash from the drug trade moves more freely southward into Mexico to be injected into the banking system there.[2]

Though most banks which process wire transfers do have some semblance of due diligence procedures applied to customers opening accounts and wishing to send wire transfers, these procedures are susceptible to the fact that they, at the most basic level, rely on human interaction. As a result, a bank employee must rely on the information provided by potential customers at the time of account opening, i.e. proper identification provided. Even the most seasoned and professional employee is not immune to being duped by a false identification card or number, as has been seen and recognized throughout history. Human fallibility is perhaps the most preyed upon vulnerability surrounding wire fraud.

Assuming a customer is able to establish an originating account (that is one from which illicit funds will be wired from), the wire itself is susceptible to fraud at every other stage of its transit. Intermediary banks which forward wires to beneficiary banks rely on accurate information from the sender in order to route the funds accordingly. At the ultimate beneficial end, the beneficiary (individual or business entity) receiving the funds may not be required to provide as much detailed identifying information as the originator.

Removing identifying information from wire data, known as "scrubbing" or "stripping" is evidence of nefarious intentions by some party involved in the transfer. However, unlike the issue of false identification of originators or beneficiaries, scrubbing is most often noted as being perpetrated by the banks involved. Again, this is an activity that relies on human interaction to be accomplished, not automated software or systems. At some point in the transfer process, information that may identify a party as being on a watch list (such as OFAC) is simply deleted from the transfer data. This may be as simple as removing the party's address.

The most effective means of countering scrubbing is to maintain robust and efficient AML systems within financial institutions at every level, as scrubbing requires, at some point, that an individual (likely a bank employee) take the action of removing identifying information from the wire data. Recent actions taken against HSBC Bank included fines for scrubbing of wire data by "affiliates" of the bank in order to circumvent U.S. sanctions against money transfers to Iran.[3] The unfortunate actuality of instances such as this is that all too often individuals fall victim to pressure from superiors or other outside influences and succumb to such pressure to "play along" with these activities. As a result, activities are allowed to carry on and continue to transfer illicit funds even when, in hindsight, the illegality of transfers seems blatantly obvious.[4]

What must be remembered, however, is that while a wire transfer may be missing key identifying data such as a party's address, that is not necessarily evidence of illicit activity. Reporting systems and systems used to input customer data varies greatly from bank to bank and

[2] Turner, Jonathan E., *Money Laundering Prevention: Deterring, Detecting and Resolving Financial Fraud* (Hoboken: Wiley; 2011).
[3] Andrea Seabrook, "HSBC Accused of Letting Cartels Launder Money," *NPR*, July 17, 2012, available at: *http://www.npr.org/2012/07/17/156933069/hsbc-accused-of-letting-cartels-launder-money*.
[4] Ibid.

country to country. In addition, the entering of this data is done by a person who may or may not be properly trained in how to do so. As a result, it is not uncommon to see wire transfer data which is missing country data, full address, personal identification numbers (where required) or other such identifying information. These human errors may be less indicative of illicit activity as they are indicative of lax training and employment standards on a bank-by-bank basis. Such issues should be addressed by the bank itself, correspondent banks and the proper regulatory authorities of the country or region.

Another issue with wires is structuring or "smurfing;" the processing of wires in smaller monetary denominations so as to avoid crossing regulatory thresholds, such as those in place for reporting transactions over $10,000, for example. In order to bypass the $10,000 reporting threshold, an individual may choose to send slightly less ($9,950 for example), or break the $10,000 into two or three smaller transfers. These smaller transfers will not trigger automatic reporting and are often not recognized by bank automated monitoring software as being suspicious. It is as this point that human interaction by AML professionals is of utmost importance, as the trained human eye is often better at spotting patterns and activity that computer systems simply aren't able to do.[5]

Structuring is likely the most common method by which illicit funds are transferred via wires. As the global banking system has come to rely more heavily on interconnected computer networks, however, these types of fraudulent transactions have become more susceptible to being identified and counteracted. Newer, more detailed AML systems and better-trained compliance and AML professionals will play a key role in future efforts to meet this threat head-on as well as aid in the development of future AML standards and practices.

Other Instruments

Although wire transfers have become one of the most common methods of money laundering, it is by no means the only such method. Computer gurus of the past have long predicted the so-called "paperless office," in which all necessary information would be stored and transmitted electronically, with no further need for actual paper records and items. The global financial system has moved somewhat towards that end, but still holds firm to the need for physical monetary instruments for numerous transaction types. These instruments are in the easily-recognized form of checks, money orders, traveler's checks, stock and bond certificates and of course physical currency (bank notes).

From an AML standpoint, each of these instruments presents its own unique challenges. Among these challenges are forged checks, counterfeit bank notes and "washed" checks (in which information is physically scrubbed from checks and new information written in). Even when the instruments themselves are physical unaltered, legal and legitimate, the purposes for their use may not be. Unlike wire transfers, these instruments, especially traveler's checks and money

[5] Note: structuring is not found only in wire transfers, but is also seen widely in paper instrument fraud. Payments over reporting thresholds may avoid reporting via instruments denominated in smaller amounts. The $10,000 example may be broken into two or three personal checks for amounts well under the reporting limit, and therefore would not trigger automatic reporting. Identifying these fraudulent instruments and transactions requires analysts trained not only in AML but also document analysis.

http://scholarcommons.usf.edu/jss/vol6/iss5/30
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.28

orders, do not always include any identifying information with regards to the individual purchasing or cashing/depositing the item. This inherent anonymity provides opportunity for quick and easy transportation and transfer of funds between individuals.[6]

The U.S. Financial Crimes Enforcement Network has created the "Money Laundering Prevention: A Money Services Business Guide" in order to provide a primer on detecting and countering money laundering activity perpetrated via money orders, traveler's checks, check cashing, currency dealing or exchange and stored value items. This guide, while not exhaustive, most importantly includes directions on when the money service business or bank must file a Suspicious Activity Report (SAR) with the government. These SARs must be filed under certain circumstances including purchase of traveler's checks totaling over $3,000, and currency transaction over $10,000 and any time a transaction is "both suspicious, *and* $2,000 or more."[7]

Recent activity involving fraudulent use of traveler's checks was noted in the 2012 scandal surrounding HSBC. In that case, the bank was accused of clearing large numbers of traveler's checks around the world. Despite evidence of money laundering activity, HSBC cleared an estimated $290 million worth of these checks through a correspondent bank in Japan. Sequentially numbered traveler's checks were being deposited at the bank in bulk, often involving as much as a half a million dollars in sequentially numbered checks. Despite this unusual and suspicious activity, HSBC failed to report the activity. Later investigations revealed that most of the checks were being purchased in Russia, a key high-risk jurisdiction for money laundering.[8]

Another major issue is that involving foreign exchange markets dealing in U.S. dollars. The legitimate, white market exchange in dollars is present in most countries and jurisdictions worldwide, with a few exceptions, and in various forms including private-sponsored and state-controlled. Countries like Venezuela regulate the trade between local currency (Bolivars) and foreign currencies, especially U.S. dollars. Venezuela provides legitimate currency exchange through two parallel systems, the Complimentary System of Foreign Currency Adjustment (Sicad) and the Foreign Exchange Administration Commission (Cadivi). The newly-created Sicad system is meant to compliment Cadivi in an attempt to eliminate or, at the very least, offer a more enticing alternative to the booming black market currency exchange system in the country.[9]

However, these systems are victims of their own bureaucracy and allegations of corruption and thus face an uphill battle towards greater acceptance. The greatest challenge facing the legitimate exchanges are the restrictions placed on the legitimate trade, which can be frustrating

[6] Carrick Mollenkamp and Brett Wolf "U.S. probing money laundering in check processing;" *Reuters*, April 23, 2012, available at: *http://www.reuters.com/article/2012/04/23/us-financial-banks-laundering-idUSBRE83M1DG20120423*.
[7] U.S. Department of the Treasury, "Money Laundering Prevention: A Money Services Business Guide," *Financial Crimes Enforcement Network, 2013,* available at: *http://www.fincen.gov/financial_institutions/msb/materials/en/prevention_guide.html*.
[8] "HSBC money laundering report: Key findings," *BBC*, December 11, 2012, available at: *http://www.bbc.co.uk/news/business-18880269*.
[9] Tamara Pearson, "Venezuela Government Announces New Currency Exchange System," *venezuelanalysis.com*, March 19, 2013, available at: *http://venezuelanalysis.com/news/8288*.

to customers while equally easy to circumvent via black markets. Restrictions include limits on how many dollars may be trade for, limits on number of exchange transactions per day as well as different rates and rules for individuals using the exchange system and companies using the same. As of February 2013, the Venezuelan government has devalued the Bolivar to trade at 6.3/dollar.[10] Meanwhile the exchange rate on local black markets is closer to 23/dollar. This is a considerably less favorably exchange rate, but when combined with no restrictions and no requirements for reporting or recording transactions, the rate is acceptable and the black market thrives.

One of the most pressing examples of foreign exchange markets facing the U.S. banking system in particular is the cross-border cash movement activity relating to the international drug trade. As illegal drugs flow north from Mexico into the United States, the proceeds from these sales must be inserted into the legal banking system at some point. These funds enter the system by means of deposit either into U.S. accounts or by being physically smuggled out of the country to be deposited in accounts overseas.

A common means of moving funds across the border involves depositing funds in an account in the U.S. and then simply wiring them to accounts in Mexico. As a result, enhanced due diligence is now being applied to banks along the border, which often deal with a high volume of customers with ties to Mexico. Extra attention is being paid to structured payments, large cash deposits, payments from a single account to multiple accounts for identical amounts and other such red flags.

High-Risk Jurisdictions, Tax Havens and Off-Shore Banking

As commerce and banking expand geographically, the issues discussed previously are also expanding into areas that are considered high-risk jurisdictions. These countries and municipalities may be considered high-risk for a number of reasons. The three highest risk countries are Cuba, North Korea and Iran; banking activity involving parties in any of these countries is red flagged based on international sanctions against them for security or political reasons.

Other high-risk countries may not be quite so obvious, but are considered so due to lax banking laws, strict banking privacy laws, favorable tax laws or general concerns about the state of banking within them. Countries on this list include political hot-spots such as Pakistan and Afghanistan, countries with histories of corruption such as Russia, tax havens in the Caribbean such as British Virgin Islands or Turks and Caicos, and others including Belize, Panama, Cyprus, Latvia, the United Arab Emirates and the Channel Islands.

Off-shore banking has also increased in the recent past, as the ease with which money is transferred to and from banks outside of a person's or company's home jurisdiction has increased. Add to this the desire to avoid more stringent local currency and currency conversion laws, and the popularity of off-shore banking can only be expected to increase. Off-shore banking has become something of the norm in countries such as Panama, where countless

[10] Matthew Boesler, "Venezuela Devalues Its Currency;" *Business Insider,* February 8, 2013, available at: *http://www.businessinsider.com/venezuela-bolivar-currency-devaluation-2013-2*.

http://scholarcommons.usf.edu/jss/vol6/iss5/30
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.28

customers from neighboring countries have opened accounts to take advantage of Panama's favorable banking system.

Finally, the real threat posed by shell companies has expanded. Shell companies may be acting as fronts for illicit trade or money laundering. The anonymity offered by shell companies allows investors and ultimate beneficial owners to keep their names off most official records for the company. In order to do this, a shell company is created in the name of a single partner, often a lawyer or law firm in a country like British Virgin Islands. This individual will be listed as the Chairman of the Board of the company, for example, and will have power of authority to execute the company's affairs. However, it is not uncommon to research a dozen shell companies and find that they all share a common address and common board members. When it is found that a single individual is listed as Chairman of a number of different companies at a common address, red flags fly. This type of entity has gained so much popularity that having a company in the British Virgin Islands has become something of a status symbol for wealthy Chinese business, which have begun to form hundreds of shell companies, which have come to be known colloquially in China as "BVIs."[11]

Regulatory Concerns

As more and more banks worldwide have begun to adhere to stricter guidelines regarding Know Your Customer (KYC) standards, as well as adopting more stringent standards along the lines of the U.S. Bank Secrecy Act, more and more attention is paid to the customers themselves. Enhanced due diligence is expected for costumers considered to be of higher risk, customers in certain key high-risk jurisdictions (whether local to those jurisdictions or conducting business therein), and those involved in particular industries.

Former Wachovia employee and British National Crime Squad detective Martin Woods discussed the importance of robust KYC procedures as key to improving the banking systems of high-risk countries, in particular Mexico. Increased KYC focus aids not only in identifying potential threats to the banking system, but also allows legitimate businesses and individuals to operate more freely and under less threat from corruption. "KYC is about transparency and the ability to see into and through relationships, which is what enables businesses, including banks, to identify and manage risks."[12]

In its July 2012 report, the U.S. Senate Permanent Subcommittee on Investigations also addressed a number of shortcomings within the U.S. Office of the Comptroller of the Currency (OCC). The Senate report recommended systematic changes to the ways in which OCC addressed bank regulations, particular with regard to identifying compliance concerns and OCC's practice of forgoing statutory violations when a bank's AML programs does not meet one or more of four pre-established minimum statutory requirements. Most notable, perhaps, was addressing OCC's lax regulatory actions when a bank hit a pre-set threshold for the number of

[11]Shaxson, Nick; "Why do Chinese companies flock to the BVI?" *Treasure Island Books,* Mary 23, 2011, available at: *http://treasureislands.org/why-chinese-companies-flock-to-the-bvi/.*
[12] Martin Woods "A Robust Know Your Customer (KYC) Program is Good for Mexico," *Thomson Reuters white paper*, available at: *http://www.world-check.com/sites/default/files/white-pappers/L-373149_US_KYC_Is_Good_for_Mexico_WhitePaper.pdf.*

AML statutory violations or "Matters Requiring Attention." Though these thresholds and limits have been in place for some time, OCC enforcement was at the discretion of the individual conducting the investigations. [13]

To an extent, however, KYC is only as effective and reliable as the individuals conducting the research, investigations and analysis of customer activity. In cases such as HSBC, a "pervasive, polluted" culture of acceptance of the illicit activity permeated certain departments, in which employees were expected to turn a blind eye to suspicious activity and allow that activity to proceed normally.[14] In addition, lax enforcement of existing statutes combined with insufficient manpower and resources required by regulatory agencies only compounds the issue and makes potential threats more difficult to identify and address effectively.

Future Concerns

Future trends in financial crimes are always difficult to predict. However, a few key issues are worth noting here. These issues are the rise of Hawala networks, increased remittances from workers abroad, and the somewhat curious advent of so-called "virtual currencies." Each poses a unique potential threat to global banking, and likewise may require unique actions and intelligence to counteract.

The first two issues, Hawala networks and foreign remittances are somewhat tied to one another. As globalization has led to increased demand for foreign workers, the prevalence of remittances to home countries has increased as a corollary. Individuals sending money back home have, in the past, suffered from "underbanking," or lack of access to the global banking system, often as a result of inability to open accounts in the countries in which they find themselves working. Lack of government issued identification prevents many from opening accounts and using standard money transfer services provided by banks. As a result, many have relied heavily on legitimate remittance networks and money service providers such as Western Union to conduct their transfers.

Alongside these legitimate networks has been the rise of new and far-reaching Hawala networks. Hawala networks operate in much the same way standard remittance networks do, but have a more focused target market. Hawala networks, while officially illegal in many places, owe much of their success to the simple trust put in the network operators, or *Hawaladars*. A person wishing to send money to another simply negotiates terms with the *hawaladar* (usually at better rates than standard remittance services), pays a small fee and the *hawaladar* handles the rest of the service. In general, a *hawaladar* on the other end of the transaction takes up the responsibility of giving the money to the intended recipient, also for a fee. However, in Hawala transfers, no money actually moves. Instead, the *hawaladars* make arrangements to pay each other's commitments to the deal by other means. This is often done by adding or subtracting the

[13] United States Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Government Affairs, "U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History," U.S. Senate, July 17, 2012 Hearing.
[14] Alastair Jamieson, "Report: HSBC allowed money laundering that likely funded terror, drugs;" *NBC News online*, available at: *http://www.nbcnews.com/business/report-hsbc-allowed-money-laundering-likely-funded-terror-drugs-889170.*

http://scholarcommons.usf.edu/jss/vol6/iss5/30
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.28

amounts being sent from otherwise legitimate business expenses such as invoices due or pending payments.

The most important aspect of any Hawala network is the underlying trust in all parties involved. As a result, many of these networks have sprung up within immigrant communities and often revolve around a single individual or small number of individuals in whom the community has some level of trust. This may be a local business owner, a community religious leader or even a tribal head.

Threats posed by Hawala networks are relatively small in number, but considerable in scope. First, Hawala networks rely on anonymity. Users of these networks are often individuals who are not able to use traditional banking methods due to lack of identification, legal immigration status, or other issue which prevents them from opening and maintain conventional accounts with financial institutions. Second, *hawladars* often combine numerous remittances into single, large dollar value payments. As a result, otherwise innocuous transfers of funds (though illegal, nonetheless), may be intermixed with proceeds from illicit activity. Money gained from the sale of contraband items, illegal drugs and the like would be combined with funds earned legitimately. This comingling of funds creates enormous difficulty in tracking illicit funds and separating commonplace remittances from attempts at laundering money.

A somewhat new and unquestionably unique new threat facing global banking is that posed by virtual currencies. Virtual currencies are those that exist only in a truly digital marketplace, but are backed by hard currencies at some point in their transactional processes. The most common of these, and the one that has gained the most general acceptability, is Bitcoin. Bitcoins are essentially virtual credits which users can buy at varying rates, depending on market value (which has been shown to fluctuate wildly). Online merchants have begun accepting Bitcoins much more frequently in the past few years. The trouble faced by currencies such as Bitcoin is that they are, in the most basic definition, commodities. In much the same way gold or precious metals may be traded for goods and services, yet have no single national currency backing, they may be victims of volatile markets. Recent prices for Bitcoin went from $1.00 to $30.00 to $2.00 per Bitcoin within a matter of months. Current trading has the exchange rate as high as $235.00.[15]

In addition, as a tradable commodity at the mercy of the marketplace, Bitcoins are susceptible to sudden and irrevocable market collapses. The recent collapse of a single trader, Bitfloor, resulted in the loss of hundreds of thousands of real dollars. While this is not a substantial amount relative to the global economy, the potential for this type of collapse is best for demonstrating volatility. Worse yet, weeks before Bitfloor's collapse, hackers allegedly stole an additional quarter million dollars of real money by simple hacking in and syphoning the virtual funds.[16]

[15] Jason Dorrier, "Bitcoin blows up, exchange rate jumps ten-fold in recent weeks," *www.singularityhub.com*, April 9, 2013, available at: *http://singularityhub.com/2013/04/09/bitcoin-blows-up-exchange-rate-jumps-ten-fold-in-recent-weeks/.*

[16] Timothy Lee, "Weeks after shutdown, Bitcoin exchange customers still wait for refunds," *Ars Technica*, May 6, 2013, available at: *http://arstechnica.com/tech-policy/2013/05/weeks-after-shutdown-bitcoin-exchange-customers-still-wait-for-refunds/.*

Bitcoin may be the most visible virtual currency, but it is hardly the only. One of the most interesting and unique virtual currency threats emerging today revolves around online video games. The Massively Multi-Player Online Role Playing Games (MMORPG) often includes in-game shops in which players can trade virtual currency for game-based goods. Virtual currencies in-game are funded via purchase with hard currency by means of credit card, pre-paid game cards or other systems. Once added to the game, these funds can be transferred to other players any country around the world with an internet connection and a place to receive the funds. Funds may be deposited with legitimate processors such as PayPal or Moneybookers, which are then distributed to by check, direct deposit to other accounts, or in some cases, cash.

As the threat of virtual currencies expand, the possibilities for their use in money laundering and the illegal movement of money increases also. By relying on virtual networks and the inherent anonymity which exists in the online realm, money launderers have a vast new system to exploit for their own goals. Current regulatory processes are incapable and ill-equipped for countering this type of threat. As the banking system and law enforcement catch on and create new countermeasures, the virtual users stay a step ahead.

Conclusion

When faced with such daunting threats and the realities of the changing landscape of global banking and the changing face of financial crime, a few points must be noted with consistency and vigor. The basic threats posed involve complex networks and interconnectedness of those networks. Globalization in the legitimate business world has grown at an exponential rate and can only be expected to continue along a similar course. Global banking must continue to grow alongside it, in order to keep the world moving forward at "the speed of banking." Meanwhile, robust anti-money laundering and counterterrorist financing measures must continue to be created and implemented uniformly and consistently.

Reliance on automated systems, computer screenings and algorithmically-created watch lists are highly effective, but all suffer the same fatal flaw: lack of human interaction. By increasing the number of effectively trained AML professionals, as well as improving AML training for individuals at various stages within the banking system, banks will be able to offer better counteractions to new threats. Keep in mind that all of the threats discussed here are predicated on the actions of a person or persons choosing to omit identifying data, choosing to bypass standards, choosing to engage in black market exchanges, and so forth. Red flags are present and identifiable at every stage of these illicit actions, waiting to be spotted by analysts and dealt with accordingly.

Perhaps most importantly for the global banking industry is the need to re-establish and maintain the levels of public and customer trust that erodes with ever new report or government filing against a financial institution for violations (by commission or omission) of banking laws. It is vital that the global banking community establish public relations in order to assure not only their customers but also regulators, government entities, law enforcement, other agencies and even other banks that the systems in place are effective. Mistakes have been made, and will continue to be made; each of which offers AML professionals new information on how to better face the next round of threats. Global banking must make it known and understood that these

http://scholarcommons.usf.edu/jss/vol6/iss5/30
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.28

threats are being faced and countered every day, in every corner of the world, and at every stage of transactions.