You Think You Know, But You Have No Idea:
Effective Oversight in the Era of Increasing Facelessness, Is it Possible?

By: Shanique Smith
# Table of Content

*Executive Summary* 2

*Methods and Motives to this Madness (Types)* 3
  - Virtual Currency 3
  - Prepaid Cards 4

*Where it Could Go Wrong (Risks)* 5
  - Virtual Currency 6
  - Prepaid Cards 7
  - Audit 10

*If You Play, What You Are Expected to Pay (Oversight Expectations)* 10
  - How Should Audit Use This Information 14

*Likely On the Horizon (Going Forward)* 15
  - Virtual Currency 16
  - Prepaid Cards 16

*Is Effective Oversight Possible? (Conclusion)* 17

*Resources* 19
Executive Summary

The selection or range of products providing elevated anonymity is vastly increasing and will only continue to expand, as these products will be required to keep pace with providing continued convenience and variety while remaining innovative. However, because of the faceless aspects of these products, people are more inclined to be their true selves since they would not have to worry about committing a crime directly in front of someone or possibly being identified by law enforcement—and that is where additional risk comes into play.

Money laundering exploits payment system vulnerabilities that provide criminals the opportunity to disguise both themselves and the nature of their transactions. Banking fraud groups and other criminals, as they always do, have found and begun to abuse weak links in the chains of security and oversight surrounding products with a great deal of anonymity.

This discussion will focus on two types of faceless products: virtual currencies and prepaid cards.

It was only a few years ago that virtual currencies were hardly known outside of the online gaming community. Fast forward to today, the total market value of these currencies exceeds $9 billion. Virtual currencies offer consumers an alternative choice of payment method and at the same time are fostering significant national and international investments in new payment technologies that have the potential to create additional options for consumers and investors in the future. However, there is limited regulation and oversight applied to the players and transactions in this marketplace. This means that consumers and investors who use this currency and institutions that process these transactions, or are in any way connected to those in this arena, are exposed to significant risks.

Additionally, prepaid card programs have become an attractive alternative for traditional solutions such as payroll payments, cross-border remittances, government assistance programs and numerous other payment applications.

Prepaid cards sometimes offer lower fees than traditional checking accounts and have become attractive to law abiding citizens and criminals alike. They provide methods for delivering financial services to the unbanked and underserved segments of society, which has contributed to excessive growth in the utilization of these products. Unfortunately, many criminals have learned the art of exploiting this payment form to facilitate money laundering using the same features that make prepaid cards such a positive payment innovation.

While virtual currencies offer the potential for continued advancement in the payments industry, a number of big issues have yet to be resolved, some of which are critical. Actually, some of these issues are much like those with prepaid cards that have yet to be completely resolved. In fact, credentials used to transact in the virtual currency bitcoin are functionally similar to prepaid cards. However, bitcoin transactions are not covered by the consumer protections associated
with debit card and payroll card transactions, which will likely extend to prepaid card transactions.

This white paper will discuss the systemic risks associated with faceless products, primarily virtual currency systems and prepaid cards; along with potential approaches to managing these risks; and how the auditing function should be expanded to include these items.

Methods and Motives to this Madness

Let us start by discussing the products that provide an avenue for facelessness. Building a foundation of how they work in order to understand the associated potential anti-money laundering/counter-terrorist financing (AML/CTF) risks.

Virtual Currency

Virtual currencies are a type of electronic money. When you purchase virtual currency, instead of receiving an actual coin or bill that you can physically hold in your hand, you receive electronic units, and unlike regular money it is not issued or backed by any government or central bank. To work, virtual currency, like bitcoin, depend on the processing power of vast networks of unidentified, private computers around the world, which maintain and update a public ledger called the “blockchain.” It functions much like a public spreadsheet.

Since virtual currencies are not kept in banks or credit unions, in order to use them, they need to be stored in “digital wallets,” which are identified by the user’s "public keys." To access the virtual currency in a digital wallet, owners use "private keys" that are random sequences of 64 letters and numbers that are kept secret; however, public keys are corresponding letter and number sequences that everyone can see on the blockchain.

Two basic forms of virtual currency:

- **Convertible** – has a value in real currency and can be exchanged back-and-forth for real currency.
- **Nonconvertible** – intended to be specific to a particular virtual domain or world, and cannot be exchanged for real currency.

Convertible virtual currency can be either: centralized (having a single administrating authority) or decentralized (having no central administrating authority and no central monitoring or oversight). By default, all nonconvertible virtual currency is centralized.

There are numerous types of virtual currency; however, bitcoin is currently the longest standing, most popular and most widely used. Over 60,000 bitcoin transactions can occur in a 24-hour period and over 21,000 bitcoins can be sent somewhere every hour, which equates to approximately $7.5 million as of the October 28, 2014 price per bitcoin. However, bitcoin values have historically fluctuated significantly as the value is based on user demand. This
specific virtual currency system has been created, so that it becomes progressively more difficult to mine bitcoins and there will be no more than 21 million bitcoins issued.

The Players:

- **Exchangers** – person or entity engaged in the business of exchanging virtual currency for real currency, funds, or other forms of virtual currency, or precious metals, and vice versa, for a fee.
- **Administrators** – person or entity engaged in the business of issuing centralized virtual currency, establishing rules for its use, maintaining a central payment ledger, and has authority to redeem this currency.
- **Miners** – individual or entity that participates in a decentralized virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners can also be exchangers, or even users if they self-generate for their own purposes.²

The legitimate use of virtual currencies offers many benefits, such as increased payment efficiency and lower transaction costs. Virtual currencies facilitate international payments and have the potential to provide payment services to populations that do not have access, or have limited access to regular banking services. Also, virtual currency, notably bitcoin, may be held for investment purposes.

**Prepaid Cards**

A prepaid card is merely a device that allows consumers to access funds held at a financial institution. Technically, the monetary value is tied to an account associated with the prepaid card.

There are two basic types of prepaid cards:

- **Non-reloadable cards**: Gift cards, like Starbucks and Home Depot cards, and other similar cards found on the racks at checkout counters. Usually, they are sold in small, preset denominations of $25, $50, or $100, and the key thing about these cards is that they can only be used until the balance is depleted. There is no due diligence on the customer, so they can be purchased with cash and therefore have significant anonymity.

- **Reloadable cards**: Network-branded prepaid cards. The balance can be drawn down, but topped off at any time, as long as the account is open. These reloadable cards usually do have know your customer (KYC) requirements, so the customer’s identification is obtained and registered. It is much like opening a credit card or bank account. These cards can be reloaded from multiple sources online or sometimes from ATMs. They can also be used at ATMs, so they work
just like a credit or debit card, except that the balance draws down when you use it.

In theory, the risk controls on reloadable cards make them less risk than non-reloadable cards. However, a number of recent attacks actually involve reloadable cards due to the fact that they can be used at ATMs, unlike anonymous non-reloadable cards.

Prepaid cards have changed the way consumers, businesses and even government agencies handle money. For instance, companies like Wal-Mart use prepaid cards to distribute payroll; government agencies use them to provide benefits such as food assistance; migrant workers use them to send money to their home countries; and individuals who do not have bank accounts use them as a low-cost, bare-bones checking account. Consumers can purchase a prepaid card at a drugstore for a nominal fee, use it as a debit card to purchase goods, add funds via cash or check, and even pay bills electronically from the account. The cards offer an avenue of flexibility and privacy.

**Where it Could Go Wrong**

As if trying to determine and verify someone’s identify is not already hard enough, there are applications that have been built to separate out connections to someone’s identity and provide or create more anonymity.

For example, TOR, a software program that allows one to remain completely anonymous online through its peer-to-peer setup. TOR was previously referred to as The Onion Router because on the way, an IP address is ripped off before getting to its ultimate destination using so many layers that it is almost impossible to determine the originator’s IP address.

Then there is the Google-like imitation search engine, Grams:

**Grams Darknet Market Search Engine** – Google of the dark net, Cross marketplace search and TOR sites. Find the information, product, vendor or service you are looking for with blazing speed,
Programs like Grams are considered amoral like a hammer, since they can be used for both good and bad. The bad is conducted via hidden services where Web servers can be set up on each machine, which can prevent someone from being able to see the physical location of the Web server. The primary concern with these anonymous tools is that they grant the ability to remove most dangers of being caught or identified as associated with most crimes. One could commit, purchase, or solicit all kinds of illegal acts, from purchasing fraudulent documents to hiring a hit-man without ever having to leave the comfort of their home.

For the types of products cloaked in anonymity specifically discussed in this paper, the risks are as follows.

**Virtual Currency**

Because bitcoin is both convertible and decentralized, two of the most risky features of virtual currency, risks as they relate to virtual currency will be primarily focused on those associated with bitcoin.

Nowadays, bitcoins can be used to purchase cocktails in Manhattan, a Tesla car, tickets and concessions for a Sacramento Kings basketball game, or anything from Overstock.com; just as easy as they can be used to obtain stolen credit card numbers, illegal drugs, guns and pretty much anything else with questionable legality bought and sold online. As such, they are highly prone to be used for money laundering. The Bitcoin network is not completely anonymous, in fact it is more pseudonymous, as it is possible to see every transaction, but not where the transaction came from or where it is going unless someone acknowledges their ownership of a specific 16-digit account number. However, the risk of elevated anonymity is still there because, honestly, how many criminals will voluntarily provide identifying information when committing a crime? Hence, the heightened concern of risk associated with bitcoin.

Unfortunately, Bitcoin is a market full of risk-taking speculators that is not tied to any monetary policy or oversight, which is why it is subject to boom and bust. The value of bitcoin has jumped as high as $1,130 and as of October 28, 2014 is down to $357. In 2013, Bitcoin’s price fell as much as 61 percent in a single day, while in 2014, the one-day price drop has been as big as 80 percent.

One can get money into virtual currency systems completely anonymously, if so desired, because some virtual currency exchanges, such as Bitcoin, do not identify their owners, their phone numbers and addresses, or even the countries where they are located. Criminals can easily obfuscate their digital identity by simply spoofing their IP address or using another individual’s account, and this essentially makes their activities difficult to trace. Additionally, the public ledger, or blockchain, is maintained by vast unidentified private computer networks spread all over the world. It is even possible that participants in these networks could abuse the power that is associated with maintaining the ledger, for example, by undoing transactions that are thought to be finalized.
When you consider the added layer of convertible currencies that are decentralized, like with bitcoins, there is even more risk. For instance, not only do bitcoin addresses have no names or other customer identification attached, but the system has no central server or service provider. The bitcoin protocol does not require or provide identification and verification of participants, and therefore, does not generate transaction histories associated with specific transactors. There is no central oversight body and currently there are no AML software programs able to effectively monitor and identify suspicious transactions.\(^5\) Thus, the risk of not ever being able to identify who is actually out there transacting in bitcoin and where the transactions are going is immense.

Global reach also increases the risks of money laundering or terrorist financing. Virtual currency systems can be accessed via the Internet from anywhere in the world and can be used to make cross-border payments and funds transfers. They also commonly rely on complex infrastructures involving several entities that are usually spread across multiple countries, to transfer funds or execute payments. This segmentation of services often makes the responsibility for AML or CFT compliance and supervision unclear. Moreover, because customer and transaction records are usually held by different entities in different jurisdictions, it is difficult for law enforcement and regulators to access this information.

These risks are further exacerbated by the rapidly evolving nature of decentralized virtual currency technology and business models, including the changing number and types of participants providing services in virtual currency payments systems.

Why would this all be of concern? I am glad you asked. To put it a bit in perspective: It took less than $20,000 to blow up the U.S. Embassy in Tanzania in 1998; and less than $200,000 to enact the tragic events of 9/11; yet there can be anonymous transactions as high as $500,000 that occur at any given minute via the bitcoin program. Therefore, risks associated with bitcoin activities are of significant concern given the high level of anonymity on both sides of the transaction and the fact that there is no government involvement or oversight.

**Prepaid Cards**

Then there are prepaid cards, which also provide a great deal of anonymity.

Cash loaded on prepaid cards have become an attractive alternative for today’s criminals. Many types can be used anonymously and to get them does not always require a bank account. Risk posed by the anonymity of prepaid cards can occur throughout every phase (i.e. when purchased, registered, loaded, reloaded, or used by the customer). Cards have actually become the preferred means of paying couriers who transport illicit drugs. In fact, it is unclear how big a role prepaid cards actually play in moving the estimated $20 billion in drug proceeds that crosses from the U.S. to Mexico every year. However, while anyone crossing this border with $10,000 or more in cash must declare it, prepaid cards are currently legally exempt.\(^6\)
The two primary features of prepaid cards that create risk are their transportability and anonymity; making them more susceptible to potential abuse than established payment methods such as debit and credit cards. Money laundering risk associated with prepaid cards lies in their easy transportability and the relative ease of moving and potentially accessing monetary value anonymously. These risks are only amplified by the fact that, as with virtual currencies, prepaid card transactions can involve nonbank, unregulated parties.

Criminals can reload prepaid cards without having to reveal their identity using sources such as cash, moneygrams, or various online payment services that provide for a higher degree of anonymity. Or, they can purchase multiple gift cards, typically at the highest dollar value allowed, from a U.S. retail chain that has stores outside the U.S. and send the cards to an accomplice in another country where the cards will likely be sold for local currency. For example, Virtual Money Inc., a Dallas-based company, provided prepaid cards that were used to help Colombian drug traffickers move at least $7 million to Medellin over a three-month period in 2006. The money moved digitally and bypassed bank accounts, making it hard to detect its digital footprint.6

What makes prepaid card programs different from traditional credit and debit card programs is the involvement of third parties, such as program managers and distributors (including money services businesses [MSBs]). While these third-party firms play a critical role in the business model for network-branded prepaid cards, their participation poses additional risk to the card-issuing institution. Regardless of the third-party sponsors or distributors the card issuer is ultimately liable. If an institution has lax underwriting standards or does not carefully monitor activity, it may be vulnerable to rogue third-party players.

It is also important to be mindful that if a prepaid card portfolio is outsourced, this adds an additional risk to consider. While institutions are generally good at enterprise information security and maybe even securing card management platforms, ensuring security of hyper-extended enterprises usually poses a challenge. This includes the data center, as well as the networks and data centers of partners who are connected to them, which includes prepaid card management service providers if that function is outsourced. Hence, when a service provider is connected to an institution, the institution has to identify and consider risks within the partner’s networks, thereby expanding the institution’s risk exposure.

Prepaid card programs that provide access to cash at ATMs or incorporate offshore card issuers have the greatest risk for abuse by money launderers. Fraudsters can use compromised online banking accounts to quickly and easily buy a prepaid card under a stolen identification, load it with cash and then use it to launder funds.

Two primary types of attacks:

1. A card management platform, or back-office platform, that is being run by an institution issuing prepaid cards, is attacked. Prepaid cards are then issued using
counterfeit cards to launder money with a strategy known as unlimited operation as it involves taking the limits off of the prepaid card account.

*How it works:* Criminals hack into a card management platform, steal card numbers and associated PINs and change credit limits, so that they are inflated. They take the card data and encode it onto a handful of plastic cards, then rush to an ATM and withdraw funds and the laundering of cash then ensues. Most of these attacks likely take place over several months and are not detected right away. For example, hackers in the Bank of Iman case actually stayed connected to the card management platform in real-time while the money was being withdrawn from the ATMs, and they watched what was going on as a way to keep an eye on things as cash out activity occurred in different countries.

2. Money mules are hired to launder proceeds of an online banking attack. They are usually recruited by a work-at-home scheme. Often the individuals who work-at-home do not know that they are serving as a money mule.

*How it works:* Prepaid cards are attached to an online banking account that has been breached, as part of the breach, identity theft has occurred, which allows fraudsters to obtain a prepaid card in the name of the victim and then simply get prepaid cards, load them with cash and use them to launder money.

Therefore, prepaid card programs that do not require strict forms of customer identification or include rigorous monitoring of suspicious activity have a heightened potential for unknowingly facilitating money laundering or terrorist financing.

In fact it was bank and wire-transfer records that enabled law enforcement to identify the 9/11 hijackers and their overseas cells. According to a U.S. Treasury Department report, “Had the 9/11 terrorists used prepaid (stored-value) cards to cover their expenses, none of these financial footprints would have been available.”

So, the primary risks to consider are that these faceless products involve:

- Non-face-to-face relationships
- Extensive geographical reach (to the extent they can be used globally for making payments or transferring funds)
- Anonymous methods of funding (e.g., cash or another payment service that does not identify the customer)
- Access to funds through international ATMs
- Several segmentations of services (i.e., several parties involved in the overall process, especially when spread across several countries)
Audit

If getting into either or both of these types of products that are shrouded in anonymity there is also the risk that the audit function may not be robust enough to fully test and evaluate the functions being implemented to monitor and oversee these activities. This risk primarily stems from the possibility of not having a qualified independent audit party or one that has the expertise or knowledge of how to assess and evaluate these specialized products. As such, pertinent management information systems being relied upon to enable these anonymous transactions and any related risk management controls may not be effectively evaluated. Therefore, the board will not be able to rely on the audit as an adequate tool to aide in the identification of areas of weakness or in need of improvement. The likelihood that there will be undetected risk exposures and threats is only elevated in the event a qualified audit program is not put in place.

If You Play, What You Are Expected to Pay

Bankers and financial institution executives uniformly say they want to do the right thing in protection of their country; yet many struggle with how and why to implement a program to comply with a BSA regime they feel is both extreme and unpredictable.

Largely, the BSA expects institutions to make every effort to identify the source, volume and transit points of funds moving in and out of the institution that may be related to money laundering and identify the persons associated with such movement—and that is unchanging.

Given the number of methods and products that can be exploited to launder money anonymously, oversight efforts should be focused on how to address the risk associated with these products and their varying structures and features. Not only should an institution ensure an effective day-to-day oversight program is in place, but an adequate audit should be implemented as well. The audit should periodically test the controls being performed and identify oversight weaknesses or areas that need improvement, so that it is not a surprise when regulators come in and point out such weaknesses.

While some institutions are reluctant to take on Bitcoin start-ups given the perception that they have a high potential for money laundering, maintaining these account relationships is not forbidden. However, to mitigate AML risk, institutions that are banking merchants active in the field of virtual currencies or prepaid card programs should subject them to strict due diligence, and verify that they are fully compliant with laws and regulations, and appropriately adhere to AML- and KYC-related programs and policies.

Due Diligence
For starters, an institution should know if their customer serves as an exchanger, administrator, or miner of virtual currency, or deals in prepaid cards. Adequate due diligence should be performed to determine if a customer is considered a money transmitter or otherwise subjected to FinCEN registration and oversight requirements. In the past, some government agencies have stated that there is no intersection at all between bitcoin and banks; however, not all regulators agree. Applications such as ZipZap provide an avenue for consumers to able to use cash to load money onto their digital wallets at thousands of participating merchants; however, if these merchants are customers of the institution, this activity can easily affect the institution through its indirect connection with virtual currency. And for those thinking that bitcoin, or any virtual currency, exchange accounts are never directly linked to traditional bank accounts, think again. Some exchanges require linkage of an existing traditional bank account to the exchange account to transfer funds between the two, typically via the Automated Clearing House (ACH) transfer system. Therefore, performing adequate due diligence is critical as banks and money transmitters can be used to facilitate the movement of large sums money whether legal or illegal. As was the case with:

**Liberty Reserve:**

The largest online laundering case in history, this was a Costa Rica-based money transmitter, operating an unregistered money transmitter business and money laundering to facilitate the movement of more than $6 billion in illicit proceeds. The company was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking and child pornography by enabling them to conduct anonymous and untraceable financial transactions. It had its own virtual currency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency (or US dollars). 5

**Western Express International:**

A money transfer firm that was indicted for operating an illegal check cashing and money transmittal business. This company used its bank accounts to convert funds from sources in Eastern Europe to prepaid cards for which it served as a load location and distributor. The cards were then distributed to various individuals in the U.S. as well as mailed abroad, which allowed millions of dollars to be moved into and out of the U.S. (8)

Providers of prepaid cards are required to register with FinCEN just as exchangers and administrators of virtual currency. Though prepaid card sellers do not have to register with FinCEN, they, along with those required to register, are required to implement an AML program, report suspicious transactions and maintain records on individuals purchasing large amounts of gift cards for five years if their products meet FinCEN’s criteria. (9x2)
There are, however, several exemptions to these rules; for instance:

- Prepaid access products of $1,000 or less and pay roll products if they cannot be used internationally, do not permit transfers among users, and cannot be reloaded from a non-depository source;
- Closed loop prepaid access products sold in amounts of $2,000 or less; and
- Government funded and pre-tax flexible spending for health and dependent care funded prepaid access programs.  

Also, virtual currency exchangers and/or administrators may need to be licensed with their applicable state as money transmitters. Part of the enhanced due diligence (EDD) and monitoring process should require checking with the applicable state’s financial regulators to make sure that an exchange is licensed, if required. The registration with FinCEN or the applicable state does not, on its own, mean that the customer is trustworthy. Adequate relationship management of any of these businesses would require periodically obtaining, reviewing and assessing their AML program.

**Monitoring for Suspicious Activity**

Even if the administrator, exchanger, program manager and other participants in these faceless programs are legitimate, there is always the risk that individuals can use virtual currency or prepaid cards to commit illegal acts undetected if the institution, administrator, exchanger, or program manager does not monitor transactions for suspicious behavior.

Institutions are expected to have and implement monitoring systems that detect patterns and anomalies. Once these detection systems kick in, and do what they are designed to do, mule activities are generally identified. The unfortunate part of this is that because criminals are also aware of these automated detection systems and the need to constantly replace and recruit new mules; there is starting to be an increasing shift towards criminal use of faceless, less traceable products to get around these obstacles. Therefore, appropriate transaction monitoring is necessary.

Institutions should ensure strategies to monitor and detect patterns that identify suspicious or high-risk transactions that might suggest money laundering activity at the virtual currency administrator and exchanger, and prepaid card-issuing and program management levels. Detecting money laundering requires a very different set of filtering criteria and as such, traditional payment fraud solutions are not likely to identify money laundering activity.

For example, in the case of Moola Zoola, funds were loaded onto one prepaid card, transferred to another, and then removed soon after at an ATM. Standard software designed to detect payment fraud would not have identified these suspicious activities. Therefore, institutions should obtain and run active, real-time transaction monitoring systems that are equipped to adequately monitor for money laundering activity. While monitoring and reporting mechanisms can be put in place
to identify suspicious activity, absence of proper due diligence increases the difficulty of actually being able to do so appropriately.

**Protection Against Risk of Security Breach**

It is best to address risks of misuse or a security breach prior to getting into any product or service instead of waiting until after an incident has occurred. Institutions are expected to put due care into the development and management of products and services that pose elevated risk and have experts involved in the design and implementation from the start, so that security and protective measures are imbedded into the related systems. It is in the DNA of the product and not added more expensively later as an afterthought. Though cost and convenience reasons may cause reluctance to do this, given that criminal usage and cyber-attacks are on the upswing, it is likely that institutions will be expected to incorporate elevated security into these types of products and services. The demise of Mt. Gox—formerly the largest bitcoin exchange by volume that ultimately failed due to repeated security breaches and inadequate internal accounting controls, is a prime example of how payment systems risks that are not identified and properly managed can lead to an unforeseen, abrupt dissolution of the company.

A risk-based approach should be implemented when establishing a risk appetite for participating in any product or service that poses elevated risk, and when determining what mitigating controls and limits will be put in place to reduce the risk of money laundering or terrorist financing as outlined in the FATF June 2013 – Guidance for a Risk-Based Approach – Prepaid Cards, Mobile Payments and Internet-Based Payment Services.

A risk assessment should be completed that guides the determination of monitoring and oversight procedures and risk limits to be applied. Generally, risk limits for prepaid cards should be established regarding:

- Daily Cash Withdrawal Limits
- Load Types
- Cash Load Limits
- Card Value Limits
- Geographic Limits

Due to the uptick in criminal hackers’ exploitation of card systems, it is necessary to ensure adequate controls to prevent back-office systems from being manipulated to facilitate fraud. The breach that took place in late 2012 that targeted the prepaid card processors for two banks in the Middle East resulted in a $45 million ATM fraud that was coordinated across several countries and took place in the space of only a few hours.

Operators of card platforms should also consider it best practice to implement the following safeguards in addition to the standard expectations (i.e., running a robust cybersecurity program,
performing a risk assessment, practice good Web application security and hardening service site systems against default passwords):

- Improving detection and response capabilities;
- Conducting penetration testing
- Using data mining and predictive analytics tools
- Establishing an incident management program
- Controlling for insider threats

**Periodic testing of third-party CIP and verification procedures**

CIP is usually not verified initially on general purpose cards. First, loads are usually limited to a certain amount and then CIP information is typically required when trying to reload the prepaid card. This is assumed to mitigate fraudulent card purchases; however, this information is usually obtained by the program manager and not the institution ultimately liable, and a number of these third-party program managers often do not implement adequate CIP verification measures. Institutions should perform periodic tests of all third-party CIP verification procedures to ensure processes being relied upon to confirm prepaid card customer’s identity are sufficient.

It may very well be impossible to identify all fraudulent or compromised identification used to open accounts. For instance, prepaid cards were used by suspected Israeli agents to cover their tracks when they assassinated a commander of the Palestinian militant group Hamas in the Persian Gulf state. The card was issued by MetaBank, an Iowa-based institution that said it did its due diligence but was dealing with customers who used fraudulent passports. However, it is important to make every effort to not only identify each customer, but the activities they are engaged in.

All of these systems and safe-guards are only as good as what is put into them. Therefore, adequate expertise need to be on-hand or consultants who possess the necessary expertise should be obtained to ensure proper effective oversight. And whatever policies and procedures are implemented should be independently reviewed and tested through the audit program.

**How Should Audit Use This Information**

Though audit coverage will vary depending on the complexity, scope and risk profile of activities; there are several general features that should always be included. For starters, to be truly effective, the audit must be performed by persons who are not involved in the function being tested, qualified to properly review the subject area and knowledgeable of how to assess the aforementioned preventative measures for adequacy.\(^{(11)}\)

Each audit should be risk-based and evaluate risk management processes of all operations. This requires a broader and more in-depth assessment of functions related to products such as virtual currency and prepaid cards to appropriately account for the exposure posed by these activities.
with elevated risk. The audit should determine if the degree to which an institution participates in activities that are highly prone to anonymity and money laundering are adequately incorporated into the overall BSA/AML compliance program and risk assessment.

If the risk assessment is determined to be reliable and identifies all areas of risk and elevated concern, then the audit should utilize the risk assessment to help dictate the scope and determine where to focus efforts during the review.

An assessment of the process for identifying and reporting suspicious activity related to virtual currency and prepaid cards, to include a review of the effectiveness of both manual and automated suspicious activity monitoring systems, should be performed during the audit. To test for and evaluate the effectiveness of oversight and suspicious activity monitoring associated with products that are highly anonymous and exhibit elevated risk, such as virtual currency and prepaid cards, the audit should analyze reports and procedures regarding:

- Suspicious activity monitoring reports (to include warning indicators of load, withdrawal, or geographic activity)
- Funds transfers
- Large balance fluctuations
- Account relationships

Such reports should be tested for accuracy along with management’s procedures for reviewing and implementing any investigative or follow-up procedures, when necessary.

The audit should also assess if adequate training regarding the risk features of these faceless products and proper oversight, has been provided to all applicable employees. As well as, validate procedures for managing and verifying third-party procedures as they relate to the institution’s customers. For example, as previously stated, an institution should periodically perform tests to validate third-party CIP verification procedures, and validate this process and determine its adequacy.

These actions performed effectively should provide assistance in determining areas of weaknesses or in need of enhanced controls and oversight, which should be used as a road map to develop and implement corrective oversight measures.

**Likely On the Horizon**

As you can expect with this amount of risk and increasing amounts of exposure, there will likely be increased government scrutiny and oversight.

**Virtual Currency**
Going forward, virtual currency will likely continue to become more widely used and accepted as a method of payment, which inevitably means that there will be continued incidents of abuse. In fact, as a result of this rising risk exposure, the New York Department of Financial Services issued the first bitcoin regulation in July 2014, which requires virtual currency exchanges, issuers and administrators to conduct an initial risk assessment and tailor a program around their legal, compliance, financial and reputational risks. Furthermore, virtual currency firms must take steps to identify and verify their customers and apply EDD steps to customers who exhibit higher risk and maintain records on each transaction. For some virtual currency firms, identifying either or both parties in a transaction will prove to be difficult, as some virtual currencies are built around platforms meant to ensure users remain completely anonymous. Businesses will also be required to file suspicious activity reports (SARs) on transactions that might signify money laundering, tax evasion or other illegal or criminal activity, and report transactions by any customer exceeding $10,000 in aggregate over a 24-hour period.12 Though this regulation currently only covers businesses operating in New York, there will likely be similar regulations for other territories in the near future.

Then there is Ripple's ascension in the shadow of bitcoin, which could very well be the preview of a step away from digital currency, towards the foreign exchange market. Ripple charges little to no fees and transaction confirmations take only seconds as opposed to the 10 or more minutes with bitcoin. Ripple requires a more exclusive arrangement than bitcoin, as institutions are to sign up as gateways on the network in order to participate. However, Ripple is also a decentralized network that does the work of the middleman and is similar to bitcoin and other virtual currencies in that its member computers work off of a common set of software-driven rules to confirm transactions.13

It is also believed that virtual currencies will eventually help creditworthy, but overlooked customers to gain access to affordable loans. Since virtual currencies have common, public ledgers that log all transactions, they can offer lenders a clear view into an individual’s payment history as revealed by a public wallet address. Underwriters may soon be able to evaluate public wallet addresses for insight into cash-flow and bill payment history.14 While virtual currencies may eventually be used to allow lenders to view individual’s payment history, institutions will have to be aware of fraudsters and/or hackers ability to manipulate these systems, if in fact they are being relied upon to make credit decisions. In addition, this will only prove helpful if individuals openly identify themselves and disclose all of their transactions and not just those that reflect favorably on them.

Prepaid Cards

FinCEN has been, and is still, working on creating a rule that will require travelers to tell customs officials if they are carrying more than $10,000 on a prepaid card. Currently, travelers are only required to declare cash and travelers checks above that amount. Despite the fact that criminals use the cards to travel undetected with huge sums of money, there are a number of
people that openly speak out against establishing such requirements. For example, regulatory
counsel of the Network Branded Prepaid Card Association (NBPCA) stated that, “Nobody takes
your ATM card to find out what is in your bank account when you go through customs. If you
have got a huge line of credit on your credit card—no one asks to see it. Why should prepaid
cards be any different?” Some even argue that, given some of the demographic segments that
are more likely to rely on prepaid cards, not treating consumers traveling with prepaid cards
similar to those traveling with credit or debit cards could lead to a perception of increased
consumer profiling.

Nevertheless, you can rest assure that as the popularity of prepaid gift cards continues to grow
along with identified cases of abuse, regulators will likely continue to try to develop and issue
additional rules to combat the use of prepaid gift cards in money laundering schemes. And, the
Consumer Financial Protection Bureau is scrutinizing prepaid cards and is expected to issue new
guidelines by the end of 2014 or early 2015. The agency said in July 2014 it would start
accepting consumer complaints about prepaid cards.

Is Effective Oversight Possible?

Yes! It is possible to establish and implement effective oversight; after all there are no bad
products or technologies, just bad people using them to do bad things.

More and more companies are thinking of strategies to address providing services to the under-
banked market, and like it or not, products with high levels of anonymity risk such as virtual
currency and prepaid cards offer this possibility. Many believe there is a huge potential to apply
the unique properties of some virtual currencies to build products for the nearly 80 million
Americans who are least served by the existing financial system. This population spends $90
billion a year on alternative services such as check cashers, payday loans, auto loans and more.

As with any major gap that exists and presents the opportunity to make large sums of money,
there is likely to be a growing shift of participation in these products, especially for those who
are focused on remaining competitive. Believe it or not, the regulatory community does not
necessarily want to stand in the way of this. Regulators would be happy with a balance of
providing information needed to combat money laundering and terrorist financing while still
providing a means for innovation and legitimate usage of these faceless products. However, there
are always precautionary measures that must be taken, and having adequate controls in place and
a quality audit program are essential.

While some institutions believe that regulators have gone beyond what is reasonable when it
comes to AML enforcement, please know that there is much reason for this rhyme. No institution
wants to receive a surprise visit by law enforcement only to find out that, unknowingly, it has in
any way facilitated fraudulent transactions that have caused harm to victims of identity theft like
in the case of Moola Zoola, or even that it has a company like Silk Road, the underground illicit
online bazaar, in its customer base.
Efforts to combat money laundering remain a high priority for law enforcement, the regulatory community and the financial services industry. Despite these efforts, criminals continue to find ways to use payment systems to move and hide their illicit funds. Historically, criminals have often been one step ahead of those trying to prevent crime and currently, virtual currencies provide an avenue for criminals, terrorist financiers, or sanctions evaders to move and store illicit funds beyond the reach of law enforcement or any authoritative body. That being said, it is likely and necessary that regulators and the payment industry make the abuse of payment products as difficult as possible without stifling legitimate use and continued innovation.

To establish the necessary regulations, make them work most successfully and prevent misuse of products with inherent anonymity, it will require collaboration. Open communication and collaboration between industry, regulators and law enforcement is needed to enable better understanding of how these products work, how they can be misused and what is needed to mitigate associated risks.

**Resources**

(2) FIN-2013-G001 – Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies – March 18, 2013


(4) Consumer Advisory – Risks to Consumers Posed by Virtual Currencies – August 2014


(7) Information Security Media Group – Prepaid Cards’ Role in Fraud By: Megan Goldschmidt – April 1, 2014


(11) FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual


