White Paper

Understanding the new payment methods, their risks, and opportunities

April 2014

LexisNexis®

Risk Solutions

Understanding the new payment methods, their risks, and opportunities

Authors: Ana L. Pereira and Ana Maria H. de Alba

As global competition increases, organizations are looking to introduce new payment products and services to the financial marketplace. Prepaid cards, e-payments, b2b, mobile banking, mobile payment services, virtual currencies, and Internet-based payment services are some examples. Most of these new payment methods address a specific domestic economy (mainly in developing economies) or have been developed for electronic commerce. Each has its own unique application and settlement process, language and currency support, and is subject to domestic rules and regulations. Along with these technological advancements come accessibility, convenience, speed, but also an increase in risk. The growing number of ways to make noncash payments has changed the financial landscape and the regulatory environment. An institution's understanding of the risks inherent in these payment methods, and how to mitigate them, should be a crucial part of its compliance strategy.

The introduction of these products to the marketplace, given they are not fully understood or fully regulated has made it quite difficult to track transactions, lending itself to the illegal use of these technologies. As a result they can become attractive for criminal behavior such as money laundering and terrorist financing. This has caused an increased attention by the regulators worldwide. Efforts are being placed to close regulatory loopholes and to get tough on the unlawful use of these systems.

Several regulatory agencies have made advancements closing these loopholes:

- March 2013, the Financial Crimes Enforcement Network (FinCEN) advised that traditional money-laundering rules would apply to virtual currencies in the United States.
- June 2013, the Financial Action Task Force (FATF) issued Updated Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments, and Internet-Based Payment Services (FATF June 2013 Guidance), which provides recommendations for the countries and the private sector on how to apply a risk-based approach to implementing anti-money laundering and counter-terrorist financing measures.
- August 2013, the New York State Department of Financial Services (NYS DFS) issued a notice of inquiry into virtual currencies.
- January 2014, the Financial Crimes Enforcement Network (FinCEN), to further interpret the March 2013 ruling, published two administrative rulings, providing additional information on whether a person's conduct related to convertible virtual currency brings them within the Bank Secrecy Act's (BSA) definition of a money transmitter. The first ruling states that, to the extent a user creates or "mines" a convertible virtual currency solely for a user's own purposes, the user is not a money transmitter under the BSA. The second states that a company purchasing and selling convertible virtual currency as an investment exclusively for the company's benefit is not a money transmitter.

Let's consider Virtual Currency, which is currency that exists in electronic form and commonly referred to as digital cash. It is not physical, such as paper money or coins. Examples of virtual currencies are Bitcoin, Ripple, Litecoin, Peercoin, Dogecoin, and Namecoin.

Over time civilization has moved away from currency backed by gold, and are progressively moving to completely electronic currencies. Most national currencies today exist in both physical and electronic form. If current trends continue, there may come a day when physical currencies are no longer used. Some people do not use physical money at all; for instance, in the U.S. many people receive their paychecks through direct deposit, move money with electronic fund transfers, make payments such as utilities and to other suppliers through online bill pay, and spend money with credit and debit cards. While physical currency still has advantages in certain situations, its role has gradually diminished. There are four main types of online interfaces that use virtual currency:

- **Online Gaming**
- **Social Networking.** A few examples are Facebook, MySpace, Flickr, YouTube
- **Virtual Worlds.** Users interact in a simulated environment through the use of avatars
- **Online Communities.** Are a group of people that interact with others in that community through mediums other than face to face such as instant messages, email, newsletters etc.

Although use of virtual currencies are commonly associated to internet transactions and now with purchases in Overstock.com or Amazon.com, to name a few of the more than 21,000 online merchants accepting Bitcoin as payment, a recent surge in brick and mortar stores accepting Bitcoin as a form of payment has sprouted from eateries to public relations agencies in Manhattan and over 26 businesses in London, proudly announcing they accept this new method of payment to demonstrate their forward thinking and attract a new wave of 21st century customers.

Some risks associated with virtual currencies:

- High volatility
- Misuse for criminal activities (Money laundering, drug trafficking and exploitation of children)
- Acceptance is uncertain
- Convertibility into legal tender
- Information security
- Consumer protection

At a minimum, risk mitigation should be focused on:

- Placing limits on transaction size, frequency, or volume per customer or group of customers and users,
- Monitoring of licensed money service businesses executing transfers and exchanges, and
- Customer or user identification

Buying virtual currency allows users to make online transactions without using credit card or bank account information. Once users have transferred real money into virtual currency, their virtual currency is no longer associated with bank accounts or credits cards, making it possibly less vulnerable to hacking and theft. One compliance concern is that the source of funds becomes difficult to confirm when cashing in or converting them into legal tender.

In the March 2013 FinCEN Guidance exempted "de-centralized virtual currencies," such as Bitcoin, from AML regulations unless they have been traded for real currencies or goods. Businesses exchanging Bitcoins are coming to terms with the fact that they need to get licensed as money transmitters in 48 U.S. states, a process requiring in-person interviews in each state.

Lets take a look at a recent money laundering case that involved virtual currencies. Federal law enforcement charged Liberty Reserve, a digital currency provider, with running a $6 billion digital money-laundering scheme. Prosecutors called it possibly the biggest money-laundering case in US history. Liberty Reserve, a centralized digital currency service based in San José Costa Rica, was similar in function to PayPal, it allowed users to register and transfer money to other users with only a name, e-mail address, and birth date. No efforts were made by the site to verify identities of its users, which attracted much illegal activity. Users had a traditional bank wire money to a third party exchanger, which were usually unlicensed money-transmitting businesses without significant government oversight or regulation. The exchanger then converted the money to digital currency, untraceable from its original source. That digital currency was then deposited into a Liberty Reserve account. No limits were placed on transaction sizes.

Liberty Reserve charged 1% service fee on each transfer and offered shopping cart functionality. All the transactions were 100% irrevocable.

Liberty Reserve was, in effect, a bank that issued its own digital currency. The key to Liberty's system was that it never actually received deposits, but instead used a series of middlemen, or money exchangers, who bought the currency in bulk and then sold smaller portions to people looking to convert money into the digital currency. The shutdown of their website, and new federal rules around money laundering that aim to make digital currencies compliant sends a clear message that US law enforcement has digital currencies top of mind.

Another payment method that is rapidly becoming a standard practice, especially for small amounts, is Mobile Payments (m-payments). Generally, customers exchange cash for virtual value that goes into their cellular phones, essentially turning those devices into an electronic wallet, personal ATM, or stored value card. It is estimated that only one in five of the world's 7 billion people have direct access to banks and financial services, but there are approximately 5 billion cell phones that can be used as virtual wallets. Some experts predict that by 2020 there will be 50 billion connected devices, and mobile payments will become the standard form of banking in much of Africa, Asia, and LatinAmerica, which are regions known to be heavily dependent on informal economies and have weak laws and/or enforcement against money laundering and terrorism financing.

There are three different types of mobile payment options:

- **Digital Wallets.** Users link their bank accounts, debit cards and credit cards directly to one online account. Some examples include PayPal, Payzen, Google Wallet. Digital wallets have all of the users' payment information conveniently available in one place. This provides extra security in that the vendor they are buying from never receives their credit card information.
- **Mobile Wallets.** Offer the same security and convenience of digital wallets. Users must first create a digital wallet with one of the providers then activate their mobile wallet on their mobile device by downloading the provider's corresponding app. This allows users to use their smartphones to make payments at any merchant with a near-field communication reader available at checkout.
- **Mobile Credit Card Payments.** There are many mobile credit card readers that attach directly to a smartphone and work just like in-store credit card machines, but are portable and require only a corresponding app. iZettle, Square, PayWave, and PayPass are some examples.

Various risks have been associated to Mobile Payments, including:

- **BSA/AML.** Resulting in failure to satisfy recordkeeping, screening and reporting requirements are common
- **Credit/Liquidity.** Resulting in possible loss from a failure to collect on a credit obligation or otherwise meet a payments-related contractual commitment
- **Fraud.** As a result of failure to prevent or deter unauthorized transactions, the interception of confidential information, or other fraudulent activity
- **Compliance.** As a result from failure to comply with applicable consumer protection laws, disclosure requirements, and supervisory guidance

In emerging markets forms of mobile money are quickly growing and helping financial inclusion to the unbanked population. It is creating unprecedented opportunities for poor people in developing countries to more actively participate in the economy. Customers can also derive significant benefits from these new payment methods. The speed and convenience of a financial transaction can create real savings for people in these emerging markets. They can pay bills without waiting in line at cash centers, which might otherwise take up to two hours plus travel time, where in some cases the entire trip can result in half a day's salary.

Security is another benefit. Carrying cash can be dangerous in many countries. The threat of robbery limits an individuals' ability to carry cash to either deposit or withdraw money, or pay bills. With mobile money, that threat is eliminated. A mobile wallet allows for the safe storage of money.

Several risk factors exist for these new payment products and services. One risk factor is that they have the potential of being used for money laundering or terrorist financing because they can allow for non face-to-face business relationships, and certain local practices could provide cover for the true initiator and recipient of a transaction (elusiveness or traceability of the transactions.) Also, depending on the type of product, funds can quickly move around the world (velocity), and with the absence of face-to-face contact (anonymity) stronger mitigating controls need to be in place to ensure that the customer identification program addresses risks such as identity theft.

How the product is funded could pose a risk. For example, does it allow cash funding? Or anonymous funding? Is it reloadable? Other risks include incomplete or fictitious information, structured or recurring, non-reportable transactions, and high velocity or frequency of transactions. These problems are not necessarily new; they might be the same inherent problem that might occur quicker or in a larger scale.

To mitigate some of the risks associated with mobile payments, at a minimum, organizations should consider implementing controls such as:

- Placing specific limits on funding
- Specifying the parties and methods authorized to fund the accounts
- Placing limits on funding
- Specifying the nature of the legal tender used to fund the accounts
- Monitoring the frequency of loads to the account
- Applying enhanced and ongoing due diligence on merchants, and monitoring for their compliance with regulatory obligations (i.e. use mystery shoppers)

Depending on the levels of fraud losses, an institution can determine whether the benefits outweigh the risks. The mere fact that fraud losses are low does not necessarily mean the risk is low, it might be that some weaknesses have not yet been discovered or that current controls are mitigating some of the risk. In certain parts of Africa and in Latin America m-payments have been used to launder fake currencies, to bribe corrupt officials, and to facilitate kidnapping and extortion, among other crimes. As organizations begins to experiment with an emerging payment method, the potential for fraud, money laundering and operational risk must be at the forefront.

We have only begun to tap into the possibilities of these new technologies. As we venture into these new payment methods several compliance opportunities are created:

- Re-examine the purpose of businesses and its controls, eliminating those that no longer seem sensible and rebuilding/creating ones that do
- Strengthen governance, structures, processes, and controls
- Be proactive in responding to the new regulatory landscape quicker than competitors

As payment methods continue to evolve and the use of virtual currencies gain momentum as a legitimate means of payment, it is increasingly important for compliance professionals to understand the nature, risks and opportunities associated with these products. The ultimate success will depend on their ability to control risk.

About the authors

Ana Maria H. de Alba is the President & CEO of CSMB, a risk management and banking consultancy headquartered in Miami, Florida and offices in Panamá, Republic of Panamá. Her experience spans more than 28 years in the financial services and consulting industries leading projects in financial crime investigations, risk and risk mitigation, due diligence in support of mergers and acquisitions, and independent evaluations of internal controls, as well as a broad range of employee and Board of Director training. As a former senior banking officer, Ms. de Alba worked in both domestic and international banking. As a consultant she has led and participated in multiple engagements, providing her services to internationally recognized business intelligence and security firms, in a wide range of business sectors that include the financial services industry as well as government entities throughout the USA, Latin America, and the Caribbean. Ms. de Alba is a recognized and frequent speaker at numerous international conferences, where she has exposed on issues related to risk mitigation and internal controls.

Ana L. Pereira is a Senior Vice President and Senior Consultant at CSMB specializing in compliance matters. As former senior compliance professional with Visa, Inc., Mrs. Pereira brings over 16 years of significant experience in Ethics programs, Anti-bribery and Corruption, and Information Security Management. Mrs. Pereira is a professional known for leading high performance teams, mitigating potential compliance and regulatory risk, influencing key organizational stakeholders, and spearheading process improvement endeavors. Her expertise is in Legal & Regulatory Compliance (AML, GLBA, Privacy), Anti-Bribery & Corruption (FCPA, UK Bribery Act), and Code of Business Conduct and Ethics (Dodd-Frank Act, Conflicts of Interest, Whistleblower Protection Act.)

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.