New Payment Products and Systems: Mitigating the Risks of Finance's New "Wild West"

I. INTRODUCTION

A. New Payment Products and Services are Changing the Financial Landscape

Increasing global competition, coupled with technical progress, has led to the rapid introduction of new payment products and services ("NPPS") to the financial marketplace. Prepaid cards, mobile banking, mobile payment services, and Internet-based payment services are manifestations of this trend. The growing number of ways to make noncash payments in electronic form has markedly changed the financial landscape, with NPPS adding speed and convenience to transactions previously conducted via slower traditional channels. These products have expanded financial inclusion to previously unbanked market segments. However, the introduction of these new products has not come without cost. Because of their recent introduction to the marketplace, some NPPS are not fully understood or fully regulated. Further, it is often difficult to track NPPS transactions, clouding the ability to distinguish between the legal and illegal use of these technologies. As a result, NPPS can become an attractive venue for criminal behavior, including money laundering, terrorist financing, the sale of illicit drugs, weapons, and commercial child sexual exploitation.

B. NPPS Draw Increasing Regulatory Attention

NPPS have drawn the increased attention of regulators worldwide, who are heightening their efforts to close regulatory loopholes and to crack down on the illicit use of these systems. In March 2013, the Financial Crimes Enforcement Network ("FinCEN") advised that traditional money-laundering rules would apply to virtual currencies in the United States. Shortly after this advisory was released, the Department of Homeland Security seized an account tied to the world's largest e-currency trading exchange, Mt. Gox, for failing to register as a money service business. By late June 2013, Mt. Gox moved to comply with the Treasury's requirements by registering with FinCEN.[1]

FinCEN is not alone in its attempts to regulate NPPS. In 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 ("AML")

CONTACTS »

Ellen Zimiles
Managing Director, Head of Global Investigations & Compliance
212.554.2602
ellen.zimiles@navigant.com

Alma Angotti
Director
202.481.8398
alma.angotti@navigant.com

Claire Slagis
Consultant
202.973.6551
claire.slagis@navigant.com

navigant.com

and counter-terrorist financing ("CFT") measures. Two months later, in August 2013, the New York State Department of Financial Services ("NYS DFS") issued a notice of inquiry into virtual currencies. Concerned that virtual currencies are becoming a 'Wild West' for narcotraffickers and other criminals, NYS DFS announced its intent to establish appropriate regulatory guidelines for NPPS.[2] In response to growing regulatory attention, representatives of Bitcoin, a form of virtual currency, are in the early stages of creating a self-regulatory organization. Backed by several prominent members of the Bitcoin community, including Tony Gallipi, the CEO of payment processor BitPay, the Committee for the Establishment of Digital Asset Transfer Authority, or DATA, as it is known, was launched in July 2013. The group's mission is "work proactively with regulatory and policymakers to adapt their requirements to our technologies and business models." Among other goals, DATA purports that it will develop best practice AML standards for virtual currency firms.[3]

C. NPPS – A Double-Edged Sword

While the introduction of NPPS can give traditional financial institutions a competitive edge by providing convenience for their customers, private sector institutions should be aware of the heightened risks and challenges involved in ensuring that such products and services are not used for illicit purposes. 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.

II. UNDERSTANDING NPPS

FATF June 2013 Guidance defines NPPS as "new and innovative products and services that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as product that do not rely on the traditional financial systems to transfer value between individuals or organizations."[4] The three most prevalent types of NPPS are prepaid cards, mobile banking (and mobile payment services), and Internet-based payment services. Brief overviews of these NPPS, the risks associated with them, and a list of red flags indicating that they may be being used for money-laundering and terrorist financing are provided below.

A. Prepaid Cards

FinCEN's 2011 Prepaid Access Final Rule[5] defines prepaid cards and other prepaid devices (including key fobs) as "mechanisms that provide a portal to funds that have been paid for in advance and are retrieval and transferable." Prepaid cards can be categorized as "closed loop" cards,[6] which can generally be redeemed only at locations belonging to the issuer (for example, a retail store gift card for a Starbucks), or "open loop cards," which can be redeemed at numerous locations. Small value closed loop prepaid cards are considered less-risky than their open loop counterparts. As such, closed loop cards with limits of USD 2,000 and under are exempt from FinCEN's prepaid access final rule.[7] Uses of "open loop" cards include online shipping, bill payment, and other traditional banking functions.[8] Some cards can be reloaded and some cards are one-time use only.

Many governments have adopted prepaid cards as a mechanism for making benefits payments to consumers. In fact, in March 2013, the United States government stopped issuing federal payments—including Social Security Supplemental Security Income, veterans' benefits, and retirement benefit payments for federal employees—in traditional paper check form. Recipients of United States' federal payments must now choose between receiving payments via direct deposit or via a United States' government-issued prepaid card known as the Direct Express Card.

B. Mobile Banking and Mobile Payment Services

According to Federal Deposit Insurance Corporation (FDIC) Guidance, mobile banking is the use of a mo-

bile device (i.e. a cell phone or a tablet computer) to conduct traditional banking transactions remotely using wireless communications.[9] Many financial institutions provide mobile banking services; these services operate under existing financial regulation. Rather than paying with hard currency or a check, a mobile banking customer can use his or her mobile phone to pay for goods and services.

Mobile payments, though also facilitated by mobile devices, are not specific to financial institutions. Mobile payments are defined as the use of a mobile device—most commonly a smartphone—to initiate a funds transfer between people or businesses.[10] Mobile payments can be made at point of sale (POS) or can be used to facilitate person-to-person payments (P2P), person-to-business (P2B), and government-to-person (G2P transactions). According to an FDIC report, by the end of 2012, over 87 percent of the United States population had access to a mobile phone, more than half of which are equipped with the smartphone technology necessary to facilitate mobile payments.[11]

Mobile payment technology is particularly popular in the developing world, which has broad access to mobile technology but limited access to traditional financial institutions. Mobile banking has the greatest number of users in Africa, where mobile banking in various forms exists in 33 countries. Kenya has emerged as a leader in mobile payments through the company Safaricom. The company, Vodafone's Kenyan affiliate, launched M-PESA, a small-value electronic payment and store of value system accessible from mobile phones, in mid-2007. Today, M-PESA boasts over 15 million users across Africa.[12] A 2012 survey of 78 mobile payment providers conducted by the Groupe Spéciale Mobile Association (GSMA) found that over 70 percent of the world's registered 81.8 million mobile payments customers are located in sub-Saharan Africa.[13]

FATF June 2013 Guidance describes two common mobile payment models: the bank-central mobile payment model and the mobile network operator (MNO) model. In a bank-centric mobile payment model, customers are account holders of the financial institution offering the mobile payment services. Under the MNO-centric mobile payment model, MNOs use mobile payment services to add value for their customers. In this model, customer funds are generally held in a prepaid account by the MNO itself or by a MNO subsidiary.[14]

At present, most mobile payments are still funded and settled via established retail payment channels, including automated clearing house (ACH), credit/debit networks, and electronic funds transfers.

C. Internet-Based Payment Services

FATF June 2013 Guidance defines Internet-based payment services as "mechanisms for customers to access, via the Internet, pre-funded accounts which can be used to transfer the electronic money or value held in those accounts to other individuals or businesses which hold accounts with the same provider."[15] Funds can be withdrawn through transfer to a traditional bank account or prepaid card, or via a value transfer service. Internet-based payment services appear in a variety of forms and are typically referred to as digital wallets, digital currency, e-currency, virtual currencies, or electronic money. A user can send digital currency to anyone with a web connection, either through a third-party website or by storing the currency on a computer hard drive.

Some common types of Internet-based payment services are pre-funded accounts used for online auction payments; digital currency providers that sell a digital representation of precious metals online; and digital currency providers allowing third parties to exchange national currencies with electronic ones. One popular virtual currency is Bitcoin (BTC), a unit of currency established in 2009. In July 2013, Cameron and Tyler Winkle-

voss, the twins made famous for their dispute with Facebook founder Mark Zuckerberg, filed a proposal with the United States Securities Exchange Commission ("SEC") to establish a Bitcoin exchange-traded fund that would buy Bitcoins for investors and store them securely. The proposed Winklevoss Bitcoin Trust, if it survives the SEC vetting process, will provide a platform for BTC to move from the world of computer programmers and Internet entrepreneurs into the domain of retail investors.[16]

Speaking in September 2013, Tyler Winklevoss claimed that "the next step for Bitcoin is potentially becoming the currency of a country."[17] While this might be a bit of a leap, some countries are beginning to recognize Bitcoin as a legitimate unit of currency. In August 2013, the German Finance Ministry recognized Bitcoin as a currency unit known as private money, a move which subjects Bitcoin to Germany's tax laws, including value-added tax on sales and income tax on profits earned from Bitcoin-related business.[18]

Even as Bitcoin is embraced by mainstream investors, two lawsuits recently filed in the United States underscore Bitcoin's attraction to criminals and other illicit users. In October 2013, United States law enforcement officials shut down Silk Road, an online international marketplace which required users to conduct all transaction in Bitcoin to protect user privacy. The shutdown follows a criminal complaint filed on September 23, 2013 by the United States' Attorney's Office for the Southern District of New York against Ross William Ulbricht, Silk Road's alleged owner, charging him with federal crimes in connection with the website. Shortly thereafter, on October 1, 2013, the U.S. Attorney's Office for District of Maryland filed a superseding grand jury indictment against Ulbricht. The two indictments paint a dark picture of just how easily Bitcoin can be manipulated for criminal means: according to the indictments, largely due to the of the blanket of anonymity Silk Road provided users, the website had become a haven for traffic in controlled substances. In addition to shutting down the website, federal prosecutors charged Ulbricht (who operated under the pseudonym "Dread Pirate Roberts") with narcotics trafficking conspiracy, computer hacking conspiracy, and money laundering conspiracy. The Maryland indictment further alleges that in March 2013, Ulbricht attempted to arrange the murder of a former employee who had been cooperating with federal authorities. According to the criminal indictment filed in New York, Ulbricht "deliberately set out to establish an online criminal marketplace outside the reach of law enforcement or governmental regulation." The lawsuits against Ulbricht are currently ongoing.

D. Risks Associated with New Payment Products

Every NPPS presents a variety of risks, though financial institutions can take comfort in the fact that these risks are not entirely different from risks faced by traditional payment methods. Research indicates that NPPS are subject to the same operational, legal, fraud, and illicit use risks as traditional payment products, with a key difference being the potential speed and scale at which crimes can be committed.[19]

The primary area of concern for regulators is the opportunity for NPPS to be exploited for illicit use. The same qualities that make NPPS attractive for consumers, including the speed at which transactions can be processed, ease of interface, and transportability of value, are qualities that make NPPS enticing to criminals, money launderers and terrorist financers. The speed at which transactions can occur often make it difficult to spot and prevent illicit transactions. The high degree of privacy provided by most platforms and the lack of transparency associated with them further augments their attraction to illicit users. Such users often become early adopters of these technologies as they attempt to exploit the new systems for their nefarious purposes.[20]

E. NPPS Red Flags

The following red flags, which can be similar to those for cash and other more traditional payment systems, may indicate that a NPPS is being used for money laundering or terrorist-financing purposes:[21]

1. General Red Flags
    a. Currency is deposited or withdrawn in amounts just below identification or reporting thresholds
    b. Customer makes multiple and frequent currency deposits to various accounts that are appear unrelated
    c. Unusually high level of transactions initiated over the Internet
    d. Customer makes high-value transactions not commensurate with the customer's known incomes
    e. Customers providing insufficient or suspicious information
    f. Customers making efforts to avoid reporting or recordkeeping requirements
2. Prepaid Card Red Flags
    a. Customer purchases a number of open-end prepaid cards for large amounts
    b. Purchases of prepaid cards are not commensurate with normal business activities
3. Funds Transfer Red Flags
    a. Funds transfer activity is unexplained, repetitive, or shows unusual patterns
    b. Customer receives large and frequent deposits from online payments systems yet has no apparent online business
    c. Many funds transfers are sent in large, round dollar amounts
    d. Large-value, automated clearing house (ACH) transactions are frequently initiated through third-party service providers (TPSP) by originators that are not financial institution customers
    e. There are multiple layers of TPSPs that appear to be unnecessarily involved in transactions
    f. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected
    g. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected
4. International Activity Red Flags
    a. Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations
    b. Funds are sent or received via international transfers from or to higher-risk locations
    c. Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason
    d. Many small, incoming transfers of funds are received and then almost immediately sent to another country in a manner inconsistent with the customer's behavioral history

III. FATF JUNE 2013 GUIDANCE[22]

In June 2013, in response to growing concern regarding NPPS, FATF updated its report on *Money Laundering Using New Payment Methods* to provide additional guidance for private sector firms regarding these products. The guidance explains different types of NPPS and

outlines which entities in a NPPS supply chain are covered by FATF Recommendations. The guidance also offers NPPS risk-mitigation measures.

A. Entities Covered by FATF Recommendations

Due to the complicated nature of NPPS, FATF recognizes that it can be difficult to determine which entity in an NPPS supply chain is responsible for implementation of AML/CFT compliance measures. While traditional financial institutions are already responsible for AML/CFT measures, FATF states that NPPS providers also fall within the definition of financial institution if they engage in "conducting money or value transfer services" or if they "[issue] and [manage] a means of a payment." They are therefore subject to AML/CFT preventative measures as required by FATF, including, but not necessarily limited to, customer due diligence, record keeping, and suspicious activity reporting.

Further, NPPS providers deemed as falling within the definition of money value or transfer services ("MVTS")[23] are required to be licensed and are subject to monitoring. This was the crux of the Mt. Gox case discussed in the introduction: FinCEN

Providers of Prepaid Cards	Providers of Mobile Payment Services	Providers of Internet-based Payment Services
» In circumstances where the prepaid card program is run by a program manager who provides payment services under contract to the prepaid card issuer, and where the issuer is responsible only for managing customers' funds, the program manager is considered subject to AML/CFT regulations when the program manager maintains relationships with customers. » In circumstances when the prepaid card issuer acts as the program manager and maintains relationships with customers and monitors the use of cards, the card issuer is subject to AML/CFT regulations. » When a prepaid card provider uses a distributor or agent, FATF Guidance indicates that the prepaid card provider is considered liable for any non-compliance with AML/CFT obligations on the part of the distributor.	» Mobile payment services that allow P2P transfers are subject to AML/CFT measures, including licensing and registration requirements. » Mobile payment services that provide for P2B transfers are subject to AML/CFT measures but are not subject to FATF licensing or registration requirements, unless required by country law. » Under the bank-centric mobile payment model, the bank which manages the customer relationships and funds is subject to AML/CFT requirements. » Under the MNO-centric mobile payment model, the MNO or its subsidiary is considered a financial institution for the purpose of FATF Recommendations and is subject to AML/CFT requirements. » When a prepaid card provider uses a distributor or agent (for example when an agent is used for loading prepaid money into a prepaid account), the provider is considered liable for any non-compliance with AML/CFT obligations on the part of the distributor or agent.	» FATF Guidance defines the provider of an Internet-based payment service as the entity that accepts funds, currency, or form a value from the customer and transfers the funds to another location using the Internet to transmit the payment message or issues an electronic currency that can be used for making transfers or payments. » Internet-based payment services that allow P2P transfers are subject to AML/CFT compliance regulations, including licensing and registration requirements. » Internet-based payment services that issue electronic currency as a means of payment for goods and services and do not allow P2P transfers are subject to AML/CFT measures but are not subject to FATF licensing or registration requirements, unless required by country law. » In Internet-based payment models, when the customer holds a claim to funds against the entity and the Internet-based payment service provider manages a relationship with the customer, the Internet-based service provider is responsible for AML/CFT obligations.

ruled that the company had acted as a money transfer service and was subject to the licensing requirements as a money service business.

B. Determining AML/CFT Compliance Responsibility When Multiple Entities Are Involved

When there are multiple entities involved in the provision of NPPS, FATF suggests that the following factors should be considered in determining whether a party is subject to AML/CFT compliance requirements:

1. The entity which has visibility and management of the NPPS
2. The entity which maintains customer relationships
3. The entity which accepts customer funds
4. The entity against which the customer has a claim for funds

In its 2011 Final Rule on Prepaid Access, FinCEN provides additional guidance on compliance responsibility for prepaid access programs. FinCEN defines prepaid programs as arrangements "of one or more persons acting together to provide prepaid access."[24] The arrangements are formed between providers and sellers, where prepaid program providers are "designated by agreement among the participants in the program or are determined by their degree of oversight and control over the program, including organizing, offering, and administering the program." Prepaid access devices are distributed by sellers, the "retailers of prepaid access devices." While prepaid program providers are required to register with FinCEN, sellers are not.[25]

C. Factors for Determining Whether Your Institution May Be Subject to AML/CFT Compliance Requirements for NPPS

Based on the FAFT June 2013 guidance, the below chart outlines circumstances in which institutions and NPPS providers may be considered subject to AML/CFT measures for NPPS products:

D. FATF Guidance Risk-Mitigation Measures

FATF suggests that financial institutions should identify and assess money laundering and terrorist financing risks posed by the development and introduction of NPPS. The 2013 Guidance offers financial institutions the following methods for NPPS AML/CFT risk mitigation:

1. Take a risk-based approach to due diligence, in which customer due diligence ("CDD") measures taken are contingent upon the level of risk posed by the NPPS
2. Use NPPS transaction monitoring and suspicious activity reporting
3. For NPPS products distributed by a network of agents or distributors, consider having the agents and distributors undertake CDD during face-to-face transactions
4. For NPPS products distributed by a network of agents or distributors, include conduct appropriate due diligence on their distributors and agents, hold the distributors and agents accountable to the financial institutions' respective AML/CFT programs, and monitor their compliance with AML/CFT measures
5. Consider limiting NPPS use by setting geographical or reloading limitations on NPPS
6. Consider limiting the functionality of an NPPS product to a certain geographical area or for the purchase of certain goods and services
7. Consider establishing individual tiers of service provided to customers, as such thresholds can ensure that NPPS remain lower risk and allow them for simplified CDD processes
8. Consider placing limits on person-to-person funds transfers
9. Consider combining transfer limits with loading or withdrawal limits

10. Consider restricting the source of NPPS funding, as anonymous sources of funding increase AML/CFT risk
11. Consider imposing identification verification requirements for NPPS
12. Be vigilant in maintaining transaction and CDD records

IV. PRACTICAL STEPS FINANCIAL INSTITUTIONS CAN TAKE TO MITIGATE NPPS-RELATED RISKS

While the risks associated with NPPS present significant challenges, they can be limited and contained by a sound AML compliance program. Such a program will include an assessment and risk ranking of AML risks posed by NPPS, an effective NPPS transaction monitoring system, customer due diligence requirements, record keeping requirements, ongoing training, and oversight.

A. NPPS Risk Assessment and Risk Ranking

The foundation of successful NPPS risk-mitigation begins with an assessment of the risks each NPPS poses to a financial institution. Financial institutions should work to understand the risks presented by such products as well as the types of customers utilizing them. Conducting a risk assessment enables financial institutions to systematically assess money laundering and terrorist financing risks and vulnerabilities as well as to identify, measure, and mitigate these risks. A properly conducted risk assessment will enable a financial institution to make effective choices about the allocation of compliance resources as it concurrently reduces the risk of a wide range of losses, from lost time spent on problem resolution to reputational and financial damage.

There is no such thing as a "standard risk assessment," as each risk assessment will be as unique as the financial institution utilizing it. However, there are standard elements that should be included to ensure that such an assessment is comprehensive. A proper risk assessment will be based on a standard methodology inclusive of a standardized rating guide. It will also include a strategy for risk identification and continued validation as it assesses AML and CFT risks across all business lines. The risk assessment is not a "one-off" process; rather, it should be conducted on a periodic and recurring basis.

In its risk assessment, a financial institution will need to determine whether the NPPS itself as well as the customers, entities, and areas using the products are more susceptible to abuse by potential money launderers, terrorists, and other criminals. Appropriate red flags related to the NPPS products (please refer to Section II for a starter list of red flags) need to be identified.

After these steps have been taken, the financial institution should "risk rank" the areas of its operations accordingly. When risks have been identified and ranked, a financial institution can properly mold its AML program to mitigate them.

Because the technology behind most NPPS is continuously evolving, with new products being developed and current products being adapted, this risk assessment should be evaluated on an ongoing basis to determine whether the NPPS products in use and the financial institution's exposures to them have not changed. The risk assessment should also be factored into new product development, so that emerging payments are properly controlled from the outset rather than being taken into consideration only after they have caused compliance concerns.

B. Monitoring NPPS Transactions

Ongoing monitoring of all NPPS transactions is an essential component of any financial institution's AML program. NPPS transactions normally leave an electronic audit trail that can be subject to analysis. NPPS transaction monitoring should include transaction monitoring, ongoing due diligence of customers and business partners, investigation and suspicious activity reporting as appropriate. Monitoring should be ideally conducted on multiple levels: it should be done on transactions on an individual level for irregularities, on sets of transactions for unusual patterns, on historical transactions for behavioral patterns, and on linked transactions for networking patterns.[26]

C. Due Diligence

A financial institution can further minimize NPPS-related risks by limiting access to such payment networks to vetted users that have undergone adequate due diligence. Such due diligence should not be limited to customers and should also include business partners in the case of intermediated products. According to FATF June 2013 Guidance, a risk-based approach to due diligence should be undertaken, in which CDD measures are based upon the level of risk posed by the NPPS. A good CDD program will require customer identification and verification measures. Customer identities should be verified prior to onboarding; post-onboarding, ongoing CDD into the customer should be periodically conducted. Customers should also be vetted for criminal background, political background, and other factors including geographical risks and the nature of the customer's business. For online transactions, the identities of both the originator and beneficiary need to be determined, as remains true for any other type of third-party payment.[27]

D. Recordkeeping

A sound AML program will include checks to verify whether all appropriate NPPS-related data requiring monitoring is captured and maintained. In addition, all CDD files should be maintained and periodically refreshed. For NPPS involving segmented services, it is especially important to maintain records on the various parties involved, including issuers, distributors, and agents. Such record keeping will allow for better detection of unusual activities. While financial institutions must collect and maintain information that is required by regulation, good risk mitigation and compliance practices may require that it collect and maintain certain information not specifically required by regulation or not required at lower transaction levels.

E. Training

A financial institution must have an adequate and knowledgeable staff to review NPPS-related transactions. All financial employees in contact with various NPPS should be trained on their nuances and AML-related risks. A financial institution should strive to conduct training regularly, including initial training and refresher training, and should provide specialized NPPS-training courses for employees working in areas of higher risk.

To ensure that such training is embedded, a financial institution should consider conducted assessments upon training course completion. Such training should also be tracked for employee attendance, penalties for non-compliance with AML policies and training procedures must be established and enforced.

F. Governance

The backbone of any successful AML program starts with having the appropriate "tone at the top." Financial institutions should provide training to board members as well as senior management

on the importance of AML and CFT compliance. A financial institution's senior management should be actively involved in establishing a control environment that emphasizes institution's compliance message, encourages the reporting of unusual activity, and promotes integrity and ethical behavior. The main aim of this control environment should be to embed an institution-wide compliance culture that promotes a collective attitude towards AML and CFT compliance. Senior management should also be involved in proactively reviewing the financial institution's risk profile and in evolving its compliance program as appropriate.

V. SUMMARY

Utilizing NPPS can provide financial institutions with a competitive edge, though the products do not come without risk. NPPS have drawn increasing regulatory attention because of their ability to be exploited by potential money launderers, terrorists, and other criminals. Financial institutions should consider taking appropriate AML risk mitigation measures, inclusive of a risk assessment, transaction monitoring, customer due diligence, record keeping, training, and governance. A strong AML compliance program will mitigate the risks of finance's new "Wild West" and allow financial institutions to employ the products to their benefit.

NOTES

1. According to FinCEN's website, *www.fincen.gov*, Mt. Gox's initial registration was received on June 27, 2013. The company's MSB registration number was reported as 3100029348132.
2. *Notice of Inquiry on Virtual Currencies*: New York State Department of Financial Services (August 12, 2013).
3. Bradbury, Danny. "Bitcoin Industry Leaders Launch DATA." *Coindesk.com* (July 30, 2013). *http://www.coindesk.com/bitcoin-industry-leaders-launch-data-a-self-regulatory-body/*
4. *Updated Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments, and Internet-Based Payment Services*: Financial Action Task Force (June 2013).
5. The Prepaid Access Final Rule establishes suspicious activity reporting requirements as well as customer and transactional information collection requirements on providers and sellers of certain types of prepaid access.
6. FinCEN's Final Rule on Prepaid Access exempts closed loop prepaid access products sold in amounts less than USD 2,000.
7. Please note that this exception is not without caveats. FinCEN states that "no more than USD 2,000 can be associated with each closed loop prepaid access device or vehicle in one day. Accordingly, if the closed loop prepaid access arrangement permits either individual reloads of more than USD 2,000 per device, or cumulative reloads per device that total more than USD 2,000 in one day, the arrangement no longer qualifies for the 'closed loop prepaid access' exception from the definition of a prepaid program under the Rule." http://www.fincen.gov/news_room/nr/html/20111102.html
8. "Mobile Payments: An Evolving Landscape." *Supervisory Insights*: Federal Deposit Institution Corporation (Winter 2012).
9. *Ibid.*
10. This does not include financial institution-sponsored online bill payment services.
11. *Mobile Payments*: FDIC (2012).
12. "Timeline." Safaricom. http://www.safaricom.co.ke/mpesa_timeline/timeline.html
13. *State of the Industry 2012: Results from the 2012 Global Mobile Money Adoption Survey*. GSMA: February 27, 2013.
14. *Updated Guidance*: FATF (June 2013).
15. *Ibid*.

NOTES

16. Lattman, Peter and Popper, Nathaniel. "Winklevoss Twins Plan First Fund for Bitcoins." *The New York Times DealBook* (July 1, 2013).
17. "Winklevoss Twins Say Bitcoin Could Become a Country's Currency." *Reuters* (September 17, 2013).
18. Schmeller, Johanna. "Germany Lends Real Value to Bitcoin Virtual Money." *Deutsche Welle* (August 22, 2013).
19. Braun, Michele, et al. "Understanding Risk Management in Emerging Retail Payments." *FRBNY Economic Policy Review* (September 2008).
20. *Ibid*.
21. This list is adapted from the Federal Financial Institutions Examination Counsel's *Bank Secrecy Act AML Examination Manual* (2010).
22. This white paper does not purport to address every aspect of the FATF June 2013 Guidance.
23. According to FATF June 2013 Guidance, MVTS "refers to financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including hawala, hundi, and fei-chen."
24. *The Prepaid Access Final Rule*: Financial Crime Enforcement Network. July 29, 2011.
25. However, sellers must maintain an anti-money laundering program if one of the following conditions is met: 1) if the prepaid access program offered is covered by FinCEN's Final Rule on Prepaid Access; 2) if the prepaid access card can be used without a later activation process that includes customer identification; or 3) if a retailer sells prepaid access products providing access to funds "that exceeds $10,000 to any person during any one day."
26. Nadig, Sowmya and Murthy, Anand. "Anti-money laundering principles for alternate payment methods." *Infosys Viewpoint* (2013).
27. *Ibid*.