Statement of James H. Freis, Jr., Director
Financial Crimes Enforcement Network
United States Department of the Treasury

Before the United States House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

JUNE 29, 2012

Chairwoman Capito, Ranking Member Maloney, and distinguished Members of the Subcommittee, I am Jim Freis, Director of the Financial Crimes Enforcement Network (FinCEN), and I appreciate the opportunity to appear before you today to discuss FinCEN's ongoing role in the Administration's efforts to establish a meaningful regulatory framework for new payment methods entering into the financial system. We appreciate the Subcommittee's interest in this important issue, and your continued support of our efforts to help prevent criminal abuse of the financial system and to mitigate the risk that criminals could exploit potential gaps in our regulatory structure as technological advances create new and innovative ways to move money.

FinCEN's mission is to enhance the integrity of financial systems by facilitating the detection and deterrence of financial crime. FinCEN works to achieve its mission through a broad range of interrelated strategies, including:

- Implementing, administering, and enforcing the Bank Secrecy Act (BSA) - the United States' primary anti-money laundering (AML)/counter-terrorist financing (CFT) regulatory regime;
- Supporting law enforcement, intelligence, and regulatory agencies through the sharing and analysis of financial intelligence; and,
- Building global cooperation and technical expertise among financial intelligence units throughout the world.

To accomplish these activities, FinCEN employs a team comprised of approximately 300 dedicated employees, including analysts, regulatory specialists, international specialists, technology experts, lawyers, administrators, managers, and Federal agents.

FinCEN's main goal in administering the BSA is to increase the transparency of the U.S. financial system so that money laundering, terrorist financing, and other economic crime can be detected, investigated, prosecuted, and ultimately prevented. Our ability to work closely with our regulatory, law enforcement, international, and industry partners promotes consistency across our regulatory regime and better protects the U.S. financial system.

There are three generally understood stages of money laundering – placement, layering, and integration – and FinCEN's rules for prepaid access, including mobile payments, are specifically designed to make this more difficult to occur in significant amounts without leaving a trail and with obligations on the industry to alert FinCEN of red flags. The customer identification process addresses integration, and we see reflected in the AML policies of many financial service providers controls to limit the dollar value available to single individuals both through thresholds and tracking to prevent a single individual from purchasing multiple access devices to

avoid the thresholds. Part of the monitoring process that is a component of an AML program would generally include classic money laundering indicators, and this is where a knowledgeable institution will often be able to distinguish between legitimate and illicit activity, which may trigger a suspicious activity report that the government uses to determine if this is indeed an aspect of criminal activity. A careful monitoring of the links between emerging payment technologies and traditional financial services helps in mitigating the risks of all three stages of money laundering.

At the outset, I would like to confirm our understanding of the differences between mobile banking and mobile payments. While mobile banking involves communication and direction from an account holder about their account at a depository institution, mobile payments essentially involve the direction of funds outside of a bank account to effect payments or other transfers. In its seminal study about mobile phone-based financial services,[1] the World Bank categorized mobile banking and mobile payment activity into four different types:

- Mobile phone-based access to information about balances and transactions conducted through a financial institution (mobile banking).
- Mobile phone-based access to an account established at a financial institution, to order such financial institution to conduct payments out of the established account (mobile banking).

[1] Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing, The International Bank for Reconstruction and Development/The World Bank, 2008. http://www.wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2008/09/17/000333038_20080917011913/Rendered/PDF/443840REVISED01ne01010200801PUBLIC1.pdf.

- Mobile phone-based access to an account established at a telecommunications provider, which might or might not be a financial institution, and where the account may be funded in advance or in arrears (mobile payments); note that this model exists in some foreign jurisdictions, but presently does not appear to be gaining popularity in the United States.
- Mobile phone-based access to an account established at a telecommunications provider, where prepaid phone minutes themselves are used as a virtual currency (mobile payments).

Let me emphasize that each of the foregoing are subject to relevant FinCEN regulations for AML/CFT purposes, either as part of the requirements on banks applying to all of their products and services, or as part of the requirements on money transmitters, a subset of regulated "money services businesses." While payment systems are evolving rapidly, often making leaps in functionality and connectivity within a matter of months, the aforementioned World Bank study still provides a valuable map to track the regulatory approach to the different roles mobile technology may play in the context of financial transactions. Although the World Bank study focuses on mobile financial services specifically, the same characterizations outlined above can apply with respect to mobile phones, key fobs and specialized readers, computer login over the internet, or any other means used to establish electronic communication with respect to, or to gain access to, funds. FinCEN's regulations take a comprehensive approach in this area, focusing more on the activity at issue as opposed to the particular electronic communication vehicle. For example, with respect to the first two characterizations listed above, FinCEN has already made clear that services that only provide connectivity between a customer and the financial institution where the customer account is maintained are not separately covered by

FinCEN's regulation. Responsibility under the regulations implementing the Bank Secrecy Act falls squarely on the financial institution where the account or analogous customer relationship is located, be it a bank, a securities company, or a money services business.[2]

With respect to the second two characterizations, FinCEN's regulations also have made it clear that the acceptance and transmission of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location, by any means, constitutes money transmission, and that any person wherever located doing business wholly or in substantial part within the United States engaging in money transmission, regardless of any other business lines the person is engaged in – such as the provision of telecommunication services – would likely be a money services business under FinCEN's regulations, and as such must register and comply with all the reporting, recordkeeping, and monitoring requirements applicable to a money transmitter.[3] Note that there is no de minimis exception for money transmitters to be subject to regulation as a money services business; this is sometimes referred to as a "zero dollar threshold." Finally, FinCEN also has determined the obligations under its regulations that would apply to any person who sets up an arrangement involving one or more parties under a program to provide access to funds that have been paid in advance and can be retrieved or transferred through an electronic device, and to any person that participates in such prepaid access program as a Provider of prepaid access.

As FinCEN's more extensive regulation of prepaid access providers and sellers is relatively recent, and some of its details and characteristics might not be familiar to all members of this

[2] FIN-2009-R001 – "FinCEN Issues Ruling (FIN-2009-R001) on Whether Certain Operations of a Service Provider to Prepaid Stored Value Program Participants is a Money Services Business" - 03/10/2009.
[3] *See* 31 CFR 1010.100(ff).

Committee yet, let me concentrate on a brief description of the evolution of prepaid access regulation, from its inception as stored value, and its application to certain business models that might be employed by mobile payment providers.

Mitigating Money Laundering Vulnerabilities in Prepaid Access Devices

In dealing with prepaid access, just as is the case in approaching any financial sector, one of our biggest challenges as a regulator of financial institutions is striking the right balance between the costs and benefits of regulation. Recognizing the emergence of sophisticated payment methods and the potential for abuse by criminal actors, several years ago FinCEN began working with our law enforcement and regulatory counterparts and the industries we regulate to study the stored value/prepaid card industry in the context of expanding AML obligations to emerging payment systems. When FinCEN issued its first rule regarding money services businesses (MSBs) over a decade ago, it limited certain requirements for the prepaid or stored value arena based on varied and emerging business models, the desire to avoid inhibiting development, and other unintended consequences with respect to an industry, which at the time was in its infancy. Over time, however, it was clear that more comprehensive regulations were needed. Recognizing the importance and value of bringing a cross-section of experts together to study this issue, in May 2008, FinCEN formally established a subcommittee to focus on stored value issues within the Bank Secrecy Act Advisory Group (BSAAG). The BSAAG is a Congressionally-chartered forum[i] that brings together representatives from the financial services industry, law enforcement, and the regulatory community to advise FinCEN in its regulatory functions. The now renamed prepaid access subcommittee provides a comprehensive panel of experts available to consult on these issues and from whom a body of empirical information is gathered and exchanged.

Prepaid access is attractive to customers who do not have similar easy-to-obtain options for non-cash payments or the ability to conduct transactions remotely. But the ease with which prepaid access can be obtained and used, combined with the potential for the relatively high velocity of money moving through accounts involving prepaid access, and the potential, in some cases, for anonymity could make it particularly attractive to illicit actors. Criminals value the ability to receive and distribute a significant amount of funds without being subject to many of the reporting or recordkeeping requirements that would apply to similar transactions using cash or involving an ordinary demand deposit account at a bank.

FinCEN began to take formal steps to address this industry sector – including seeking public comment on how stored value should be defined and related issues in the proposed rule, Amendment to the Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses.[ii] After we had begun efforts to revise our regulations, on May 22, 2009, President Obama signed the Credit Card Accountability, Responsibility, and Disclosure (CARD) Act of 2009.[iii] Section 503 of the CARD Act directed FinCEN, as administrator of the BSA, to issue regulations regarding the sale, issuance, redemption, or international transport of stored value, including prepaid devices such as plastic cards, mobile phones, electronic serial numbers, key fobs and/or other mechanisms that provide access to funds that have been paid for in advance and are retrievable and transferable. Although FinCEN had taken steps toward more comprehensive regulations for the prepaid/stored value sector before the CARD Act became law, the statute accelerated our timeframe.

After extensive study, consultation with the Department of Homeland Security and various other law enforcement and regulatory agencies, and a solicitation of public comments through a formal

notice of proposed rulemaking, on July 29, 2011, FinCEN published a final regulation amending Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Prepaid Access,[iv] amending the money services businesses (MSB) rules and establishing more comprehensive regulations for prepaid access.

The final regulation's most important provisions are as follows:

- It renames "stored value" as "prepaid access," without narrowing or broadening the meaning of the term, but to more aptly describe the underlying activity.
- It adopts a targeted approach to regulating sellers of prepaid access products, focusing on the sale of prepaid access products whose inherent features or high dollar amounts pose heightened money laundering risks.
- It excludes from the rule prepaid access products of $1,000 or less and payroll products, if they cannot be used internationally, do not permit transfers among users, and cannot be reloaded from a non-depository source.
- It excludes closed loop prepaid access products that provide access to less than $2,000 on any day.
- It excludes government funded and pre-tax flexible spending for health and dependent care funded prepaid access programs.

The final rule addresses regulatory gaps that have resulted from the proliferation of prepaid access innovations over the last 12 years and their increasing use as an accepted payment method. FinCEN's prepaid access regulation also provides a balance to empower law enforcement with the information needed to attack money laundering, terrorist financing, and

other illicit transactions through the financial system while preserving innovation in this rapidly growing area of consumer payments and the many legitimate uses and societal benefits offered by prepaid access. Moreover, while prepaid access is most often associated with a card, the new regulation was designed to be technology neutral to allow it to be adaptable to a range of products, such as a plastic card, an internet system, a mobile phone network, and other forms of developing technology that enable the ability to introduce and realize monetary value.

Under FinCEN's regulation, non-bank providers of prepaid access are now subject to comprehensive requirements similar to depository institutions. The final regulation reflects FinCEN's attempts to achieve the right balance. FinCEN believes that certain prepaid programs operate in such a way as to reduce potential money laundering threats and are therefore generally not subject to the provisions of the regulation. Such products include payroll cards, government benefits cards, health care access cards, closed loop cards, and low dollar products with strong safeguards in place.

Other risk variables – such as whether a product is reloadable, can be transferred to other consumers, or can be used to transfer funds outside the country – were all things that we identified through our extensive regulatory, law enforcement, and industry consultations. When developing the regulation, we asked the general public to help validate whether we found the right balance so that higher-risk persons and products are appropriately regulated while lower-risk products are not subject to undue regulatory obligations or constraints. For the sake of clarity, let me emphasize that a payment system allowing the transfer of funds from one mobile phone to another, such as by reference to a phone number, is subject to FinCEN's regulations for prepaid access

Separately, FinCEN is nearing finalization of a rule that would include the reporting of tangible prepaid access devices as part of the current requirement to report more than $10,000 in currency or monetary instruments when crossing the border.[4]

Subsequent Outreach to the Prepaid Access Industry

Shortly after the publication of the final prepaid access regulation and as part of FinCEN's ongoing commitment to engage in dialogue with the financial industry and continually learn more about the industries that we regulate, FinCEN announced in October 2011 its interest in holding town hall meetings in its Vienna, Virginia offices with representatives from the prepaid access industry. The town halls were designed to elicit feedback on the implications of recent regulatory responsibilities imposed on this industry, and to receive industry's input on where additional guidance would be helpful to facilitate compliance. This outreach was intended as a part of FinCEN's overall efforts to increase knowledge and understanding of the regulated industry and how its members are affected by regulations, and thereby help FinCEN most efficiently and effectively work with regulated entities to further the common goals of the detection and deterrence of financial crime.

In response to the open invitation, FinCEN was contacted by 49 entities expressing an interest in attending the town hall meetings. Based on the information provided by the entities, FinCEN selected a representative cross-section of 16 entities that described themselves as engaging in activities that would likely fall under FinCEN's new regulatory definition of provider of prepaid access, or that acted as service providers to banks or potential providers of prepaid access. Town halls were held on November 17 and 29, 2011. FinCEN has released a number of pieces of

[4] Bank Secrecy Act Regulations: Definition of Monetary Instrument, 76 FR 64049 (Oct. 17, 2011).

guidance with respect to the prepaid access regulations and anticipates that additional guidance will be forthcoming related to some of the issues raised by the industry attendees during those town halls and through other ongoing requests for clarification and guidance on the new regulations.

FinCEN's Efforts with Respect to Mobile Payments

In the mobile payments universe, as noted in the World Bank study, a mobile phone can typically be used as an access device or method of communication and instruction to access accounts, initiate payment instructions, and/or notify the recipient by way of text messaging of the receipt of funds into their account. In a similar manner, so-called "mobile wallets" can be established, typically in conjunction with subscriptions to telecommunications companies, which can serve as mobile payment initiation or receipt points for customers. For some of the larger MSBs that have recently entered into the mobile payments space – such as Western Union, MoneyGram, and PayPal – the operational aspects of the actual money transfer and payment transaction segment remains similar to traditional methods of funds transfer processes facilitated by the companies, where the basic transaction flows and related recordkeeping obligations remains relatively consistent but with the mobile aspect (recipient's mobile phone number) added to it.

As part of our ongoing support to law enforcement, FinCEN provides reference manuals to help better understand the workings of various payment mechanisms and to provide steps to utilize this understanding in specific criminal investigations, including ways to subpoena records and interpret them. One recent such manual focused on mobile payments, and we have lent FinCEN's expertise in emerging payment technologies, including mobile payments, in a range of

law enforcement sensitive notices to our customers in addition to individual case support. In preparing the manual and in subsequent law enforcement outreach we have seen an interesting trend in the mobile payments industry where different telecommunication systems and/or financial mechanisms may merge and become interwoven in the same overall mobile payments transaction. For example, a customer may choose to initiate a remittance through a traditional, brick-and-mortar MSB agent location with the transaction then being processed through that MSB's centralized internal system, and the payment of funds then going to a recipient's mobile wallet account. Upon completion of the transaction, the recipient typically receives a text message notification on their mobile phone that indicates the funds have been credited to their mobile wallet account. The recipient also then may be able to withdraw the funds at an ATM via a debit card. This transactional overlap often provides multiple informational choke points that potentially lead to each other, which may, in turn, actually pose a benefit to law enforcement in their efforts to follow the money trails and identify other accounts and transactions associated with a given subject(s). Borrowing from procedures provided to FinCEN by one of the nation's largest providers of mobile payment services, consider the following scenario as an illustration of how a typical transaction from the United States to the Philippines might work:

- A customer goes to a domestic MSB agent facility and completes a standard money remittance form, including the recipient's mobile number;
- The funds are transferred through the MSB's internal processing system to a recipient's "SMART Money" account that is affiliated with a participating communications company and the account is maintained at a financial institution in the Philippines.
- The recipient receives a text message notifying them that the funds are now available, at which point the recipient can then either use their mobile phone to transfer funds to

another SMART Money account, reload airtime, pay bills with participating merchants, or retrieve the funds directly from an ATM through the use of a SMART Money card (similar to a debit card).

As discussed previously, FinCEN's prepaid access regulation was specifically designed to be flexible and to accommodate new technologies as they emerge, but also to capture innovative payment methods currently used by U.S. institutions, including aspects of the scenario described above. In addition, FinCEN's money transmitter regulations also may serve as a basis for regulating aspects of such activity. Consistent with past practice, FinCEN will interpret its regulations as they apply to various business models and provide guidance as necessary to industry with respect to the application of FinCEN's requirements.

Conclusion

In the area of new payment methods, the Administration has made appropriate oversight of prepaid access products a priority, and as a result the Treasury Department's efforts in this regard have increased significantly over recent years through targeted regulatory measures, outreach to regulatory and law enforcement counterparts and our partners in the private sector. In addition, FinCEN's regulations in the MSB space, whether in the context of prepaid access or money transmission, can apply to select actors in the mobile payments space depending on the variety of business models that develop. We are very encouraged by the progress we have made thus far, and we are dedicated to continuing to build on these accomplishments as we chart a course for the future that encourages legitimate consumer and commercial activity to flourish, but also helps financial services providers to focus on serving their customers, not criminals. Thank you

for inviting me to testify before you today. I would be happy to answer any questions you may have.

[i] http://www.ffiec.gov/bsa_aml_infobase/documents/regulations/Annunzio_Wylie.pdf
[ii] 74 FR 22129 (May 12, 2009)
[iii] http://www.gpo.gov/fdsys/pkg/PLAW-111publ24/pdf/PLAW-111publ24.pdf
[iv] http://www.gpo.gov/fdsys/pkg/FR-2011-07-29/pdf/2011-19116.pdf