Statement for the Record
House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit
"The Future of Money,…#157"

The Clearing House Association L.L.C. ("The Clearing House")[1] appreciates the opportunity to submit this statement for the record in connection with the June 29, 2012, hearing before the House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit.

Mobile phones and other devices are increasingly being used to initiate payment transactions in the United States and are expected to begin to displace magnetic-stripe payment cards for consumer payments. The adoption of mobile payments technology holds the potential to vastly expand financial inclusion and facilitate growth in commerce. At the same time, the rapid expansion of mobile payments has introduced new payment service providers and mechanisms into the payment system, which bring with them the potential to create new risks. Payment integrity, security, and other consumer protections, once the domain of highly regulated, supervised, and examined depository institutions, are now influenced by mobile phone manufacturers, mobile phone network operators, application developers, and providers of Internet services, including social media. Although some of these service providers and mechanisms are subject to existing consumer protections under federal laws and regulations, others are not. Even in cases where existing federal payments rules may apply, these new entrants raise new issues and present new challenges for regulators and consumers.

We believe that:

- the varying regulatory structures applicable to mobile payment providers yield uncertain consumer protections and uneven oversight of the safety and soundness of various payment systems;
- the complex and fragmented mobile payments ecosystem has the potential to create a confusing consumer experience, increase the risk of fraud, and create new risks to the protection and management of customer bank data; and
- the evolving mobile payments environment presents significant issues that will need to be addressed to ensure that law enforcement has the tools it needs to successfully monitor, track, and prevent money laundering and terrorist financing.

[1] Established in 1853, The Clearing House is the nation's oldest banking association and payments company. It is owned by the world's largest commercial banks, which collectively employ 1.4 million people in the United States and hold more than half of all U.S. deposits. The Association is a nonpartisan advocacy organization representing—through regulatory comment letters, amicus briefs, and white papers—the interests of its owner banks on a variety of systemically important banking issues. Its affiliate, The Clearing House Payments Company L.L.C., provides payment, clearing, and settlement services to its member banks and other financial institutions, clearing almost $2 trillion daily and representing nearly half of the funds transfer, automated clearinghouse, and check image payments made in the United States. For additional information, see The Clearing House's Web page at www.theclearinghouse.org.

I. The varying regulatory structures applicable to mobile payment providers yield uncertain consumer protections and uneven oversight of the safety and soundness of various payment systems.

Mobile payments commonly refer to payments initiated through a mobile phone or a mobile Internet communication device such as a smartphone or a tablet. The pervasive access to mobile phones throughout the population and the growing ubiquity of smartphones holds significant promise for the rapid growth of mobile commerce in the United States and the provision of payment methods to previously underbanked populations.[2] At the same time, divergent mobile technology models and the diversity of entrants into the mobile space also present significant regulatory challenges.

Mobile payments can generally be divided into two categories: proximity payments, where technology embedded in or displayed on the payor's mobile device interfaces with the payee's point-of-sale equipment to initiate payment (e.g., near field communication, barcode or QR code), and remote payments, where the payor uses the mobile device to initiate payment to the payee without regard to proximity to the payee or point-of-sale equipment. Mobile phones greatly facilitate the communication aspects of payments and open the door to many new payment methods and channels.

This vast potential for communication can be readily coupled with an agreement with the consumer using the mobile phone that binds the consumer and obligates the consumer on the payment. This agreement can be with the mobile network or with a third party providing a service that can be accessed through the mobile phone.

The broad communication ability of mobile phones and a ready means of binding the consumer to the payment obligation make the means of settling the payment the primary constraint on mobile payments. Viewed from a settlement perspective, mobile payments diverge widely, falling into three general models—bank payments, money transmitter payments, and mobile network payments.[3]

Mobile phones can serve as devices for accessing traditional bank payments including credit card, debit card, and automated clearinghouse payments. In these cases the phone merely substitutes for other access devices, such as the familiar plastic credit or debit card, and payments are processed through interbank arrangements subject to existing legal requirements, including well-established federal consumer protection laws.[4] Mobile payment services offered by banks must also comply with the significant regulatory guidance applicable to banks and are conducted under the extensive standards

[2] Mobile phone use is high among groups that are prone to be unbanked or underbanked according to a recent study released by the Board of Governors of the Federal Reserve System (Consumers and Mobile Financial Services, March 2012).

[3] It should be noted that these three categories are somewhat simplified. The mobile ecosystem is emerging in complex ways and there can be many variations on the basic models discussed here. It should also be noted that the word "bank" is being used in a broad sense to include banks, credit unions, and other depository financial institutions.

[4] Applicable law includes the Truth in Lending Act ("TILA") for credit card payments and the Electronic Fund Transfer Act ("EFTA") for payments initiated out of bank deposit accounts held in the name of a consumer making the payment. These laws provide important consumer rights including the right to receive monthly statements describing transactions, the right to have billing errors addressed, and, subject to certain conditions, the right to have unauthorized transactions reversed. In the case of credit card transactions, these rights also include the ability to assert claims and defenses that the holder has against the merchant, subject to specified conditions.

and examination procedures adopted by bank supervisors and, more recently, the Consumer Financial Protection Bureau ("CFPB").[5]

Mobile phones can also access the services of nonbank money transmitters. In doing so, mobile phones, as well as other electronic communications, have the potential to greatly increase the use of these services by providing more convenient access and facilitating the delivery of payments to payees, who may be notified of the payment through their own electronic or mobile devices. Money transmitter payments are not subject to the full panoply of bank regulation and supervision. While certain aspects of their business have been subject to federal oversight, such as federal anti-money laundering requirements and, depending upon their business model, some aspects of their business may be subject to federal consumer protection laws such as the Electronic Fund Transfer Act, the transmitters themselves, to date, have only been subject to supervision and oversight under state laws.[6] These state laws vary and may not cover all mobile applications or service providers that provide access to money transmitter payments, because their activities are limited to the communication aspects of the payment and do not include a settlement function.

Finally, payments initiated through mobile phones can be settled through the mobile phone network itself either by billing the transaction to the mobile phone holder's account with the network or by charging the payments to a prepaid card or phone account. Mobile phone networks are under the general oversight of the Federal Communications Commission and operate under a regulatory and supervisory regime that vastly differs from the regulatory and supervisory regime that applies to banking organizations or even the more limited state law regime that applies to money transmitters.[7] Although in some cases federal consumer protection laws that also apply to bank payment services may apply, the bank supervisory regime does not, making enforcement of these laws, as well as the security and integrity of the payment process, less certain.[8]

Because the multitude of nonbank players entering the mobile payments ecosystem are generally not subject to the same functional regulation that applies to depository institutions, they are considered "shadow payments providers." The patchwork of regulatory and supervisory regimes applicable to shadow payment providers leaves consumers with varied and often uncertain protections and a supervisory and examination structure that unevenly regulates the soundness and integrity of providers in the mobile payments space. For example, shadow payment providers are in some

[5] By federal law, with some exceptions, banks receive at least one full-scope, on site examination at least once during each year (every 18 months under certain circumstances). The examination process is supported by supervisory guidance that addresses both compliance with laws applicable to mobile payments services and the management, technology, and operations infrastructure necessary to support mobile payments.

[6] EFTA and its implementing regulatory protections may apply if the money transmitter offers the customer an account in which to hold funds.

[7] For example, while billing error rights are a focus of the consumer protections provided under TILA for credit cards and EFTA for electronic payments out of bank deposit or other consumer accounts, a consumer's recourse for a billing dispute with a mobile phone carrier is to complain to the Federal Communications Commission, which will endeavor to resolve the issue.

[8] As in the case of money transmitter payments, the supervisory guidance developed through decades of experience that strengthens the platform for payments though the banking system is absent, as is the experienced and skilled examination conducted by federal bank examiners.

circumstances subject to more limited regulatory requirements than banks in key areas such as "know your customer" and anti-money laundering.

In general, the entrance of less-supervised providers is likely to result in a reduction in the reliability and integrity of payments. The extent to which this reduction results in significant harm to consumers will depend, in part, on the extent to which mobile payments are covered by existing regulatory regimes such as the Truth in Lending Act and the Electronic Fund Transfer Act. However, coverage by these laws alone will not be sufficient to ensure comparable consumer protections. Such coverage would need to be supplemented by a robust and rigorous regime of supervision and enforcement.

II. The complex and fragmented mobile payments ecosystem has the potential to create a confusing consumer experience, increase the risk of fraud, and create new risks to the protection and management of customer bank data.

Historically, the customer bank data (personal account information) necessary to authorize payment transactions has been issued by banks to consumers in finite, recognizable forms that consumers readily understood required protection. Checkbooks were guarded in safe places, checks were manufactured with features to prevent counterfeiting, and authorized signatures were required for negotiation. Credit and debit cards were issued in plastic format, were kept in wallets or purses, and, as time went by, were imbued with additional security features, such as picture IDs or specially encoded information. The issuer of the customer bank data was listed on the check or card and was readily understood by the consumer to be the party the consumer needed to contact should the payment vehicle containing the customer's bank data be lost, stolen, or otherwise compromised. When notified, banks easily cancelled and reissued cards or checks and changed account numbers.

Over time, banks also developed sophisticated fraud detection systems with artificial intelligence capable of using customer profiles and historical transactional information to evaluate in real time the likelihood that a given transaction was fraudulent, thereby limiting the risk of unauthorized charges to the consumer's account. The law developed within this historical context to limit, within certain constraints, a consumer's liability for fraudulent transactions.

However, as the mobile payments ecosystem is evolving, consumers are being confronted with an ever-dizzying array of business and technology models including some that rely on customer transactional and geolocation data to engage in targeted advertising. The result is a plethora of parties and payment devices that may store customer bank data. As a result, without careful product structuring by a regulated bank, consumers may be left without a clear understanding of what to do when an unauthorized charge occurs or a payment device is lost or stolen. For example, a consumer may be issued a credit card by a bank which the consumer then "stores" in the consumer's mobile phone through the use of an application provided by an application developer. Does the consumer now realize that his or her phone has now become the equivalent of a physical wallet and needs to be protected with the same degree of security and vigilance? If the consumer's phone is stolen, or an unauthorized transaction occurs, does the consumer call the mobile phone provider, the app developer, or the consumer's bank? Banks are well positioned, based on their extensive experience in payments, to develop mobile payments products that provide customers the level of security and customer service they expect based on their experience with traditional payments products such as checks and credit cards.

The emerging number of mobile wallets (including "cloud-based wallets" where the payment information is not stored on the device or provisioned securely by a bank issuer) and other devices within which customer bank data can be stored makes it difficult for consumers and issuers to seamlessly and reliably track and update customer bank data when needed. The growing complexity of this system is not only likely to increase security risks, but may result in customer confusion and frustration, lost transactions for merchants, and support system nightmares for issuers.

In addition, shadow payments providers often disintermediate the messaging of traditionally regulated systems, inserting themselves into the transaction as the merchant of record. Thus, the merchant of record that may appear on a consumer's bank statement may be the shadow payments provider rather than the actual entity from whom the consumer actually purchased goods or services. This is likely to cause consumer confusion as to the true nature of the charge, whether the charge is fraudulent or erroneous, and the proper means through which a potential dispute should be resolved. Further, because the merchant of record is not the merchant in fact, the sophisticated fraud detection systems banks have built to monitor transactions in real time may be impaired in their ability to receive data (the identity of the merchant or the real nature of the goods or services purchased) useful in fraud prevention.

Finally, under the current regulatory scheme, banks are usually required to absorb fraud liability and always absorb the cost of recredentialing regardless of whether they had any connection with the underlying breach that compromised the data. Because the liability and costs of fraud are not always properly aligned with the responsibility, other players in the mobile ecosystem may have less of an incentive to develop stringent security safeguards and standards to reduce incidents of fraud, particularly in the absence of an effective regulatory regime. Ultimately, this would result in higher costs to consumers and merchants as the costs of fraud liability protection increase.

III. The evolving mobile payments environment presents significant issues that will need to be addressed to ensure that law enforcement has the tools it needs to successfully monitor, track, and prevent money laundering and terrorist financing.

The Bank Secrecy Act ("BSA") and FinCEN's anti-money laundering ("AML") regulations serve the important public-policy goal of discouraging money laundering and terrorist financing by enlisting financial institutions in this effort. The financial institutions covered under these requirements include depository institutions, money services businesses, credit-card system operators, and insurance companies along with businesses such as casinos and dealers in precious jewels.

The regulations impose four basic types of requirements on these financial institutions: filing reports of certain transactions, record-retention requirements, customer due diligence responsibilities, and active monitoring for suspicious activities. The reports (including Currency Transaction Reports and Suspicious Activity Reports) provide FinCEN and other law-enforcement agencies with information on transactions, currency flows, and suspicious activity so they can study trends and deploy their resources effectively. The record-retention requirements provide law enforcement the opportunity to get a complete picture of a suspect's financial transactions and relationships including any payees, sources of funds, and other transactions.

As the mobile payments environment evolves, significant issues will need to be addressed to ensure that law enforcement has the tools it needs to monitor, track, and prevent money laundering and

terrorist financing. The disintermediation effect that shadow payment providers can have in the mobile space can add a significant layer of complexity to an effective AML regime.

If the shadow payment provider appears as the merchant of record, either as the payee or the source of funds for a consumer's bank transactions with another consumer or merchant, bank records will not disclose to law enforcement the true payee or source of funds for the real transaction. By disintermediating banks from the actual beneficial parties of the end-to-end payment transaction, banks have a less-than-comprehensive picture of the customer's financial activities and the bank's ability to monitor for suspicious activity will be compromised.

While investigators could go to the shadow payment provider to discover the identities of the actual beneficial parties to the transaction, it remains uncertain whether all shadow payments providers are subject to FinCEN's record-retention requirements, potentially denying investigators the ability to compile a complete picture of a suspect's transactions. At the very least, investigators will be deprived of a clear and efficient record of the transactions through utilization of the bank's records.

* * * * *

Although mobile payments technology holds great promise for the advancement of commerce and financial inclusion, the rapid growth and fragmented ecosystem of mobile also presents serious regulatory and oversight challenges. Providers engaged in functionally similar activities will need to be regulated and supervised in functionally equivalent ways so that important consumer protections are applied evenly across provider categories and models and that safety, soundness, and security concerns are being evenly addressed and compliance examined. Industry standards will need to be developed to ensure that customer bank data is securely and appropriately protected in all transactions and that data will be capable of being appropriately tracked and easily updated. Finally, significant issues will need to be addressed to ensure that law enforcement continues to have the tools it needs to efficiently and effectively monitor, track, and prevent money laundering and terrorist financing regardless of the nature of the provider or the business model or technology employed.

If you have any questions about this statement or would like to discuss these issues further, please contact Robert C. Hunter at (336) 769-5314 or Rob.Hunter@theclearinghouse.org.

Respectfully submitted,

The Clearing House Association L.L.C.

/s/

Robert C. Hunter
Deputy General Counsel