Testimony of David Fortney
The Clearing House Payments Company
House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
March 5, 2014

Good morning Chairman Capito, Ranking Member Meeks, and members of the subcommittee. My name is David Fortney, Senior Vice President of Product Development and Management for The Clearing House Payments Company. Thank you for the opportunity to talk about issues critical to all Americans – the security of our payments system and the protection of sensitive consumer financial information.

The Clearing House is the nation's oldest banking association and payments company, founded in 1853. Our mission is to ensure the safety, soundness and efficiency of the payments system in particular, and to enhance financial stability more generally. As such, we provide payment, clearing, and settlement services to our twenty-three owner banks and other financial institutions, clearing and settling nearly $2 trillion daily. The Clearing House also engages in cutting-edge thought leadership on payments technology and payments system security. The organization's owner banks collectively represent over 55% of the nation's deposits; over 40% of debit cards; and over 70% of Visa and MasterCard-branded credit cards.

The recent escalation of merchant data breaches demonstrates the increasing sophistication of cybercriminals and underscores the urgent need for financial institutions, merchants, and all who touch the payments system to work together to protect against current and future threats. While banks, along with federal and state laws and regulations, protect consumers against monetary loss, data breaches can result in identity theft and the ensuing consumer impacts of card replacement, account monitoring and fraud reporting, as well as a real loss of confidence in the payments system.

From the other witnesses we have heard about the nature and sophistication of cyber threats, how the recent breaches occurred, and what measures are in place to help prevent future breaches. Like other witnesses, we encourage the adoption of technologies such as point-to-point encryption to ensure that swiped card information is immediately encrypted at the point-of-sale and remains so until it is unlocked behind the firewalls of merchant acquirers.

I will focus the remainder of my testimony on payment system technologies on the horizon that will reduce the risk of future breaches. In particular, two technologies—EMV and tokenization--will play significant roles in protecting against future threats.

EMV, which stands for Europay, MasterCard, and Visa, is a standard for chip-based payments cards and terminals. EMV cards contain embedded integrated circuits and are designed to provide greatly enhanced protection against counterfeiting, as compared to magnetic strip-based cards. As we've heard today, it is relatively easy to produce fake cards with today's magnetic stripe technology.

However, EMV alone would not have prevented the theft of card information in the recent data breaches because it relies on merchants receiving and processing the same static account numbers in use today. Those customer account numbers would still be significantly valuable to cybercriminals for committing fraud online is where most fraud occurs. Additionally, as EMV was designed prior to the Internet, mobile smartphones and tablets, it does not address transactions initiated via those means.

Tokenization addresses online and mobile phone payments by substituting a limited-use random number—a digital token—for the customer's account number during the transaction. Working behind the scenes, the secure digital token acts just like a regular account number as it goes through the system and requires very little change in how customers and merchants operate. The digital token is refreshed regularly, as often as after each purchase. A customer's true account number is never present in the smartphone or in the merchant's system, preventing malware residing on these systems from capturing that information in the first place. Even if the system is compromised, the digital token is of limited or no use to criminals. The customer's real account number remains securely stored in bank data vaults residing behind firewalls at highly-regulated and closely-examined financial institutions or payments networks.

The implementation of these two technologies—EMV and tokenization—will require cooperation amongst banks and merchants as the tangible benefits can only be achieved by moving in tandem. The timeline for the move to EMV in the U.S. has been established by the card networks, and we are pleased to see the recent statements by merchants and financial institutions announcing the acceleration of their individual EMV adoption timelines. As mobile smartphones and other smart devices such as smart watches become increasingly prevalent and enabled for commerce, there is little doubt that payments will increasingly be initiated by these devices in the future. While tokenization is a much newer technology, we are working to see it rapidly standardized and adopted to provide needed protection against future cyberattacks.

Today, customers provide personal financial data to merchants, online wallets, alternative payments providers, merchant aggregators, and others. This proliferation of "live" sensitive customer account data increases the risk of breach-related fraud and presents a confusing and complicated process for consumers to maintain. When my bank sent me a new card last year after a data breach, I needed to update the card information on 47 different merchant and payment provider websites. In a tokenized environment, customer account data is held securely behind bank firewalls, and consumers won't need to update account information when cards are reissued.

Tokenization mitigates the risk of sensitive data being compromised, greatly benefiting both consumers and merchants. Tokenization can be implemented in back-end processing systems with banks and payment processors being the ones responsible for deployment. Merchants will no longer

need to keep and safeguard vast quantities of sensitive data. They will still be able to track customer purchases for performing analyses and driving targeted offers, and customers will enjoy a much more secure payments system.

With hundreds of millions of consumers, millions of merchants, thousands of banks and credit unions and hundreds of networks and processors, the only way to gain broad adoption of tokenization and ensure a consistent customer experience is to develop an open tokenization standard. Open standards promote innovation and allow customers and merchants to choose the point-of-sale technology that works best for them. But it will require banks, merchants, networks and processors to work together to accomplish these goals.

Two years ago, The Clearing House and its owner banks began working together to create an open tokenization standard called Secure Token Exchange. We are working with mobile wallets, networks, merchants and payments processors to pilot and trial the standard. The initial pilot began late last year, and we will soon expand the trial phase to encompass additional banks, merchants and cities. Secure Token Exchange is technology agnostic and focuses on the communications necessary to safely and securely correlate a digital token to a customer's account for transaction processing. By keeping a narrow focus, Secure Token Exchange creates minimal disruption to the current payments ecosystem and promotes innovation throughout. This is especially important at the point-of-sale where customers and merchants should be the ones that choose how they communicate with each other. This initiative has acted as a catalyst, with an increasing number of payments system participants now working on tokenization. We remain very much at the center of this activity.

For example, The Clearing House is now working with the card networks, standards bodies, merchants and processors on digital tokenization efforts with a goal of upholding core openness, and safety and soundness principles. We have also joined a coalition of merchant and financial industry trade associations to form a cybersecurity partnership. We are committed as an organization and a company to protect consumers, merchants, and the entire payments system from cyberattacks.

Thank you again for the opportunity to testify on this critical issue. Everyone involved in the payments ecosystem has a responsibility to work toward the implementation of solutions like point-to-point encryption, EMV and tokenization. Doing so will help ensure that the nation's payments system remains safe, sound, and secure in the decades to come. I am happy to address any questions.