Statement for the Record
Senate Committee on Banking, Housing and Urban Affairs
Subcommittee on National Security and International Trade and Finance
February 3, 2014

Cyber criminals are becoming more sophisticated, and recent breaches of consumers' data underscore the urgency of updating the payments system to protect against current and future threats. At the same time, the way consumers pay for transactions is undergoing unprecedented change. In addition to ever increasing amounts of online shopping, all evidence indicates that more and more consumers will use smartphones for mobile payments at physical point-of-sale, bringing with it new risks to consumers and merchants alike.

While banks along with federal laws and regulations protect consumers, data breaches result in lost consumer confidence, as well as the inconvenience of card replacement, account monitoring, and fraud reporting. It is critical that the entire payments ecosystem- retailers, processors, banks and networks—embrace and deploy secure tokenization to protect consumers and merchants. "Tokenization" substitutes a limited-use random number (token) for customers' account numbers so that the sensitive information remains safe.

The planned U.S. migration to the EMV (Europay, MasterCard and Visa) standard is an important step in enhancing the overall protection of point-of-sale payments systems. Since EMV cards are designed to prevent counterfeiting, they lessen the resulting fraud consequences of a breach. However, because EMV-enabled transactions still transmit cardholder data at the point-of-sale, EMV would *not* have prevented the theft of customer account numbers that occurred in the Target and other recent retailer breaches. Moreover, as EMV was designed prior to the Internet, it does not protect consumers against online fraud, which is where the majority of these crimes are committed. As a result, the implementation of EMV in Europe has led to a shift in fraud from point-of-sale to online. [1] EMV, while an important step forward, is only a partial solution.

Research shows that the overwhelming majority of consumer account information breaches occur as the result of security vulnerabilities on the retailer side of the transaction.[2] Tokenization of sensitive data is the best possible solution because no actual customer account information will be stored in retailer environments. Rather, it will only exist behind the security of highly-regulated and closely-examined financial institutions and their service providers.

---

[1] While EMV & chip implementation in Europe has helped reduce losses at the point-of-sale by 24%, that is offset by card not present losses which remain high and now account for 56% of all card fraud. *Second Report on Card Fraud,* European Central Bank, July 2013, available at: http://www.finextra.com/News/FullStory.aspx?newsitemid=25023

[2] The business sector, because of the Target breach, accounted for almost 82 percent of 2013's breached records. The Banking, Credit and Financial sector accounted for only 4 percent of all breaches and less than 2 percent of all breached records. *2013 Data Breach Category Summary*, Identity Theft Resource Center, January 1, 2014, available at: http://www.idtheftcenter.org/images/breach/2013/BreachStatsReportSummary2013.pdf .

Tokenization substitutes a limited-use random number ("token") for customers' account numbers, with the real account numbers securely stored in bank data vaults. Tokenization protects *both* consumers and merchants from the risks of future data breaches. Even if compromised, the token is of limited or no use to criminals.[3] In addition to providing a significant increase in security for consumers, it alleviates a burden placed on retailers because they do not have to keep and safeguard vast quantities of sensitive data. Also, tokenization can be implemented with minimal disruption to retailer point-of-sale environments, while still supporting merchants' customer service and data analytics capabilities.

A number of tokenization efforts, including one undertaken by The Clearing House and its owner banks, are in progress. We believe it is important for Members of Congress to understand the promise that this technology holds to solve the security issues that seem to be plaguing our nations' top retailers. This endeavor is being pursued proactively by the industry and is designed to proceed quickly to implementation.[4]

All parties in the payments ecosystem have a responsibility to ensure that consumers remain protected and that the nations' payment systems remain safe, sound, and secure. The Clearing House and its banks will continue to work proactively and cooperatively with all participants in the payments ecosystem, including merchants, processors, and networks, to ensure that the best possible solutions are implemented to combat the increasing threats posed by cyber criminals.

About The Clearing House

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.

---

[3] In a dynamic tokenization system, a token is valid either for a single transaction or for a limited number of transactions occurring in the typically very short time interval during which a new token is generated and provisioned to the mobile wallet. If a dynamic token were to be intercepted by malware residing in a retailer point-of-sale system, the ability to use that token for a subsequent fraudulent purchase is nearly impossible, would require the fraudster to be in the same immediate vicinity, and would be rapidly detected.

[4] Two years ago, The Clearing House banks recognized the emerging security risks related to mobile payments, as well as the growing risks due to the proliferation of sensitive customer account information online. They organized an initiative, TCH Secure Cloud, to mitigate these risks. Secure Cloud uses tokenization technology so that customers' real account numbers are never provided to the merchant and are never present on a mobile device. Secure Cloud is currently in a live pilot. The solution is being developed as an open standard, meaning it will be accessible to everyone, demonstrating the banking industry's commitment to work cooperatively with all participants in the payments ecosystem, including merchants, processors and networks.