WRITTEN TESTIMONY OF RACHEL MCGREEVY
VICE PRESIDENT, STATE GOVERNMENT AFFAIRS AND COMMUNITY RELATIONS
MASTERCARD

FRAUD PREVENTION
IN THE ELECTRONIC PAYMENT SYSTEM

Chairman Dickinson, Vice-Chairman Morrell, Chairman Wieckowski, Vice-Chairman Wagner and Members of the Banking and Finance and Judiciary Committees:

My name is Rachel McGreevy and I am Vice President of State Government Affairs and Community Relations for MasterCard. Thank you for the opportunity to present testimony regarding fraud prevention in the electronic payment system. In preparation for today's hearing, the Committee Staff asked me to address the following questions:

1. Magnetic stripe technology that is commonly used on payment cards,
2. MasterCard fraud prevention measures,
3. EMV technology, otherwise known as "chip and PIN" technology
4. Cardholder personal information that is used by MasterCard to process payment card transactions,
5. Liability allocation for fraudulent payment card transactions resulting from a data breach.

First, very briefly, about MasterCard:

MasterCard does not issue payment cards of any type (credit, debit or prepaid), nor does it contract with merchants to accept those cards. Those functions are performed in the United States by numerous banks. MasterCard operates a payment network through which banks that issue cards, known as "issuers" and "acquirers," or merchant banks, can interact to complete payment transactions and drive commerce. It is a technology infrastructure connecting over 30 million merchants, 40,000 financial institutions and two billion cardholders worldwide.

We are very deeply committed to the safety, security and integrity of this system and operate fraud prevention systems to protect data and prevent fraudulent transactions on a 24/7/365 basis. While these efforts, and the efforts of others, have caused fraud levels to decline to all-time low levels, our job is protecting consumers and businesses against these threats. While no financial transaction can be completely free from the risk of fraud, a comprehensive security approach including the implementation of EMV technology is the best way to reduce fraud and ensure the safety of cardholder data in a constantly changing environment.

1. The Anatomy of a Magnetic Stripe Payment Card Transaction

The magnetic stripe on the back of a payment card stores basic cardholder data which typically includes the payment card account number and the card expiration date. The merchant also enters the dollar amount and date/time of the transaction and a code that identifies the merchant. A message containing this information is transmitted electronically from the terminal to the acquiring bank. This is known as the "authorization message" which MasterCard receives from the merchant bank, transmits to the cardholder's bank for verification, and sends back to the acquirer who authorizes the merchant to process the transaction.

In-person magnetic-stripe payment card transactions are generally authenticated through one of two methods: signature authentication or personal identification number ("PIN") authentication. Currently, credit card transactions are authenticated using signatures, while debit card transactions may be authenticated either using a signature or a PIN.

For "card-not-present" transactions, such as those conducted online or over-the-phone, an additional layer of security is provided by using a card security code, which is a series of numbers printed on the card that is not part of the account number, and is not stored on the magnetic stripe or transmitted during an in-person transaction. The MasterCard security code is known as CVC2, for Card Validation Code which is printed on the back side of the card. MasterCard introduced the card security code in 1997, and was the first of the major payment brands to introduce the technology to help further reduce fraud in card-not-present transactions.

2. MasterCard Fraud Prevention Tools and Zero Liability Guarantee

We are constantly working to improve security on our network and make a number of fraud prevention tools available to issuers and acquirers to add additional layers of security to payment card transactions. For example, we offer state-of-the-art fraud monitoring services to our customers that identify fraud patterns both domestically and internationally, and we alert issuers and acquirers to unusual activity patterns. We also are developing new tools like SecureCode technology, which relies on a code known only to the consumer and their bank (similar to a PIN) to ensure that cards are used only for authorized transactions online.

Consumer peace of mind is always at the forefront of our anti-fraud activities. MasterCard-branded consumer cards are backed by our Zero Liability Guarantee. Issuers fund this guarantee, further demonstrating their commitment to protecting consumers.

3. The EMV Technology Roll-Out

The EMV technology standard was developed in 1996 by Europay, MasterCard and Visa. EMV technology relies on a microprocessor chip embedded in the payment card, allowing for dynamic authentication. The presence of chip technology on an EMV card makes creating counterfeit cards significantly more difficult, reducing the risk of fraudulent transactions even if account data is compromised.

We introduced our future of payments **"roadmap"** for EMV implementation in the United States in January 2012. In this roadmap, we took insights and perspectives from the other payment system participants to enable the next generation of payments. As the world's largest payment card market, with thousands of issuers and acquirers and millions of point-of-sale terminals that must be upgraded to accept EMV transactions in the US, this was an important step and reflects our commitment to secure all payment channels.

The roadmap was designed not to mandate specific actions by merchants and issuers, but provide a path to help them make their own business decisions. A central element is a liability shift for fraudulent transactions, which is an incentive to help merchants and issuers move toward the EMV standard. In this liability shift, the party that employs the less secure technology will be liable for the potential fraud. MasterCard is committed to implementing our planned EMV rollout without delay.

On January 8, 2014, Chris McWilton, MasterCard's president for North America, sent a letter to our domestic customers and partners reiterating our commitment to the EMV roadmap and emphasizing the importance of implementing state-of-the-art security technology in light of recent merchant data breaches.

4. The Use of Cardholder Personal Information in the Payment Network

Again, in a typical payment card transaction, MasterCard receives from the acquirer an authorization message that contains only the payment card account number, the card expiration date, the dollar amount, date/time of the transaction and a code that identifies the merchant. The primary use of the information captured in the authorization message is to process and complete the requested cardholder transaction. The information is also used for processes related to the transaction, such as resolving cardholder disputes, and detecting and preventing fraud and account data compromise events (including merchant data breaches).

MasterCard's use of cardholder information is subject to the financial privacy and information security requirements of the Gramm-Leach-Bliley Act ("GLBA") and our protocols are subject to examination by federal banking agencies for compliance with the GLBA.

5. Data Breach Liability Allocation

In the case of a data breach suffered by a merchant in which payment card account data is compromised (an Account Data Compromise or ADC event), MasterCard will investigate the circumstances surrounding the event to allocate financial responsibility between the acquiring bank and the issuing bank. MasterCard Rules are designed to place responsibility for ADC events on the payment system participant that is in the best position to guard against and respond to such risk. That is generally the entity whose network, system, or environment was compromised. The process that we use in assessing ADC events is described in the MasterCard Rules, which we make publicly available on our website.

In Conclusion

Thank you for allowing us to appear before you today regarding the vitally important issue of payment card data security. We appreciate the opportunity to discuss our technology

and our commitment to delivering the most secure payment solutions in the world. We hope you and your staff will continue to look to MasterCard as a resource.