ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

Embargoed until 10am on May 14

Written Testimony of

Jason Oxman, CEO
The Electronic Transactions Association

House Financial Services Committee
Hearing on
"Protecting Consumers: Financial Data Security in the Age of Computer Hackers"

May 14, 2015

Introduction:

Chairman Hensarling, Ranking Member Waters, and members of the Committee, I am Jason Oxman, CEO of the Electronic Transactions Association (ETA), and I submit this written statement for the record for the hearing on Protecting Consumers: Financial Data Security in the Age of Computer Hackers. By way of background, ETA is a global trade association whose mission is to advance the payments technology industry. As the trade association of the payments industry, the ETA represents more than 500 of the world's most innovative payments and technology companies, from Fortune 500 financial institutions, to small, local sales organizations, to the world's largest technology companies. ETA's members are dedicated to providing merchants and consumers in our country the safest, most reliable, most secure payments system to facilitate commerce and power our economy. At the outset, I want to affirm ETA's strong support for legislation that creates uniform, national data breach and data protection standards that are industry neutral, preemptive of state law, such as H.R. 2205 does, and we applaud Chairman Neugebauer and Rep. Carney, as well as the entire Committee leadership, in this regard.

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

The Electronic Payments Ecosystem – Driver of Economic Growth:

To help put the electronic payments industry into context, when a consumer buys something from a merchant, they often will use a form of electronic payment, such as a credit card, debit card, gift card, prepaid card. Purchases can be made in person with the card or with a mobile device, or remotely, over the phone or the Internet. While the transaction is simply and securely completed within seconds of a swipe or tap, it involves an enormous and complex electronic payments ecosystem, which includes:

- consumer card issuing banks;
- the card brand networks that connect merchants and consumers;
- payment processors that connect merchants with networks of banks (issuing and acquiring) to ensure the transaction is authorized and processed;
- program managers that work with consumers and issuing banks to help consumers obtain credit and prepaid cards;
- point of sale equipment hardware and software companies;
- program managers that work with consumers and issuing banks to help consumers obtain credit and prepaid cards;
- enablers of payment technology and e-commerce;
- merchant acquirers, which provide payment acceptance services;
- independent sales organizations that work directly with merchants to provide access to the payments system;
- sponsor banks, which establish policies for merchant acquirers, sponsor their registration with the card brands, and hold the risk of payment;

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

- anti-fraud companies that work with providers in the ecosystem to help ensure fraudulent transactions do not occur; and
- security companies that work with all other providers in the ecosystem to protect and secure transactions against intrusion.

This ecosystem is largely invisible to consumers and merchants because it works seamlessly to process billions of transactions each year – that's literally thousands of transactions every second. Electronic payments are key drivers of commerce and economic growth in our country. To put this into greater context: 70% of U.S. GDP is attributed to consumer spending, and 70% of consumer spending is done electronically. Last year, electronic payments surpassed $5 trillion and electronic consumer spending will only continue to grow. Indeed, by 2017, we project that ETA member companies will process $7.3 trillion in consumer spending in the U.S.

Lessons Learned from 2014: The Year of the Breach

You have asked me to address why and how data breaches occur. Some have dubbed 2014 as "The Year of the Breach," and this past year businesses of all sizes, across various industries, those who store, transmit or process payment card data and those that contain other valuable information, experienced a breach. By and large, the types of high-profile breaches we saw last year were caused by cyberattacks perpetrated by highly-sophisticated, international criminals, and we should not forget that those businesses who were attacked are, like consumers, also the victims of a crime. Moreover, according to Trustwave, an ETA member company, there are a number of important lessons learned based on information collected from hundreds of post-breach forensic investigations:

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

1. Misconfiguration issues persist, including the use of weak passwords such as "Password1" and using the same password for multiple logins.

2. Lack of resources limits the time or manpower necessary to make sure that adequate security technology is installed, updated, monitored and continuously working properly.

3. There are security weaknesses across third party providers. The industry has taken steps to require third party providers to use a unique password for each client and two factor authentication.

4. Lack of segmentation, whereby businesses mix all of their networks together so that all of their data – sensitive and non-sensitive – flows through the same networks.

The Electronic Payments Industry's Commitment to Securing Customer's Information:

ETA member companies take seriously their affirmative and continuing obligation to protect the confidentiality and security of their customers' information. Our payments systems are built to detect and prevent fraud -- and to insulate consumers from any liability. In fact, consumers in the United States choose electronic payments over cash and checks in large part because they have zero liability for fraud, making electronic payments the safest and most reliable way to pay. The liability is borne by companies in the payments industry due to Federal law and even more stringent payment network rules. In light of this financial responsibility and a desire to preserve consumer confidence in the security of electronic transactions, ETA members have a strong interest in making sure fraud does not occur, including through the misuse by criminals of consumer data that happens to be compromised through a data breach. Towards that end, payments technology businesses are bolstered by robust compliance practices – whether their own in-house policies, or ETA's own carefully crafted industry *Guidelines*, which establish underwriting practices to help payments companies detect and eliminate fraud.

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

Importantly, for those companies that follow them, self-regulatory guidelines help ensure that consumer data is secure. The Payment Card Industry Data Security Standard (PCI-DSS) created by the PCI Security Standards Council, is an example of one such successful industry-led, multi-stakeholder program, safeguarding personal information that should serve as a model. As a point of reference, fraud accounts for less than six cents of every one hundred dollars spent on the payments systems – a fraction of a tenth of a percent – and the payments industry is on the cutting edge of technology to help further limit fraud. But inasmuch as we just emerged from 2014, which the media dubbed "the year of the data breach" following several high profile breaches, I would like to highlight five concrete steps the payments industry is currently taking to further combat data breaches and protect consumer information against increasingly sophisticated cyber criminals:

(1) ETA Members: Embracing the EMV migration

ETA has long championed adoption of EMV enabled chip cards as one protection for consumers. EMV enabled chip cards, which can be identified by a conspicuous chip on the card's face, currently only make up about 1%-5% of total card circulation in the US, but this number is expected to increase to 90-95% within the next two years.

To incentivize more rapid migration to EMV adoption, the payments industry faces an October 2015 liability shift for their card transactions, at which point any participant in the transaction chain who is not EMV compliant will be responsible for any resulting fraud. This industry-led initiative is an example of how payments companies are proactively working to strengthen protection for consumers and the payments system.

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

To explain further, EMV, which stands for EuroPay, Mastercard, Visa, is the global standard for integrated circuit, or "chip" cards. Today, EMVCo (the body that sets that EMV standard) is owned jointly by American Express, Discover, JCB, MasterCard, UnionPay, and Visa, and includes other organizations from the payments industry. EMV cards feature embedded microprocessor chips that store and protect cardholder data – similar to magstripe, but safer. An EMV card is superior to a traditional magstripe card because it supports dynamic authentication. EMV technology does this by encrypting account information and generating a unique, or "dynamic," one-time security code for each transaction, which makes the card nearly impossible to replicate. Counterfeiting such cards is currently far more difficult than producing cards with data that is "skimmed" from the magnetic stripes of genuine cards or stolen from stored payments data, such as the high-profile merchant breaches of recent months. Because EMV cards generate a dynamic security code with each transaction, unlike a magnetic stripe card which uses the same static code with every purchase, a counterfeit card could not successfully produce the correct security code and would not work in a card-present or face-to-face transaction. Accordingly, EMV is an effective tool to combat the manufacture and use of counterfeit cards and card-present fraud. But although chip cards reduce the value of compromised data by inhibiting the creation of counterfeit cards, they do not stop data breaches. Other initiatives within the industry further augment the protections provided by EMV and will help erect additional barriers to bad actors, while simultaneously reducing the value of the data they may attempt to obtain.

(2) ETA: Chip and Cardholder Verification Methods

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

A separate question, independent of the EMV migration, has arisen regarding whether consumers should be required to use a personal identification number (PIN) for each credit card transaction at the point of sale. The EMV chip functions as a fraud prevention tool by generating a dynamic security code, thus preventing the production of counterfeit cards, the single largest (by far) cause of fraud. Put another way, this ensures that the card itself is valid. It is important to note that a PIN is a method of verifying the cardholder's identity (not that the card itself is valid, but rather that, in theory, the person presenting the card is the actual cardholder). This is referred to as a cardholder verification method, or CVM. A CVM prevents a type of card fraud called "lost and stolen" fraud – where a criminal has stolen a physical card from a wallet, for example, and then attempts to use the card before it has been reported stolen. Other methods of CVM include signature and, in some cases, no CVM is required, for example, because the transaction is a low dollar amount or low risk of fraud, and a CVM would not be beneficial to require.

ETA strongly supports the migration to EMV, and we believe that card issuers should be permitted to make the choice that is best for their customers as to cardholder verification method to accompany the chip cards, whether it be signature, PIN, or neither, when authorizing a transaction. Consumers and merchants have benefitted from flexibility in cardholder verification methods – including speedier checkout times for low dollar, low risk transactions. For example, drive throughs, quick service restaurants and convenience stores, in collaboration with payments companies and card networks, allow consumers to move quickly through checkout lines through "swipe and go" transactions that benefit all parties to the transaction and help maintain overall consumer satisfaction. Similarly, new mobile payments technology replaces traditional CVMs with even more secure biometrics that promise both fraud protection and consumer convenience at a higher level. An important part of the decision of card issuers whether to require their customers to use a

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

PIN is whether merchants have the capability to accept PIN as a CVM. It should be noted that, at present, roughly 2/3 of the nation's merchants do not have a PIN pad and thus cannot accept a PIN transaction from their customers. For such merchants, consumers who are required to use a PIN for a transaction could represent lost customers.

Similarly, mobile payments cannot use a static PIN with the transaction. As merchants and consumers move from plastic cards to mobile devices, including mobile phones and wearables, this next generation of payments technology must not be inhibited by plastic card-era systems. Also, many consumers prefer not to have to remember PINs. Indeed, in 1967, the inventor of the ATM, John Shepherd-Barron, first envisioned a six-digit numeric code for customer authentication, but his spouse could only remember four digits, which became the commonly used length. Furthermore, the PIN is static and can be stored on a card, making it vulnerable to interception or even being guessed (there are only 10,000 possible 4 digit PIN combinations). As our industry moves to dynamic security, biometrics, and other systems that are even more secure, we must consider these important factors in making the right choice to secure transactions.

The fact remains that criminals are adaptive and constantly probe for vulnerabilities. Focusing on one specific technology gives hackers an open invitation to focus their energies on that technology and to detect and exploit loopholes in the payments system. Strong security involves a multi-layer approach which has the ability to evolve in response to the changing threat environment, allowing the industry to be as nimble as the bad actors it is attempting to thwart. At the end of the day, we all need to work continuously and collaboratively across banks, payments companies, merchants and consumers to find the most effective and efficient security mechanisms.

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

(3) ETA Members: Fostering other new technology

As previously mentioned, EMV is one part of the overall, multi-layered solution to protecting data, consumers, and the payments system. ETA members are simultaneously deploying new innovations to further enhance security. For example, another technology, tokenization, removes sensitive information from a transaction by replacing customer data with a unique identifier that cannot be mathematically reversed. In its simplest form, it works like a secret code substituting symbols for important information like a credit card number. This way, only banks and payment processors know real account information. Tokenization is designed to work when a consumer pays with plastic in person, online or with a mobile phone.

In a non-tokenized transaction, a consumer's actual account number is transmitted and, in some cases, stored by retailers, e.g., for purposes of facilitating returns. This trove of information is what hackers typically seek in the case of retailer data breaches. But in a tokenized environment, actual account numbers are replaced by one time-use tokens that represent account numbers but cannot be tied back to the actual number. If a breach occurs, the criminal only sees the tokenized code, which is useless to them because it cannot be used to generate a subsequent fraudulent transaction.

Another layer of protection deployed by ETA member companies is the use of point-to-point encryption. Point-to-point encryption is an advanced risk management tool that helps further protect data throughout the transaction lifecycle. With point-to-point encryption, card data is encrypted from the moment the card is swiped or tapped, while the data is in transit, all the way to authorization. This technology minimizes opportunities for hackers and criminals to access data during a purchase.

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

Additionally, many payment companies continue to innovate advanced computer systems that monitor transactions and data patters detect unusual activity that may indicate an account has been hacked or a card lost or stolen. This monitoring occurs in both traditional, card-present as well as in card-not-present transactions, such as those taking place over the Internet or phone. Lastly, using a mobile device to initiate a transaction will soon be as common as swiping a card. Mobile payments and digital wallet cloud technology are actively employing new security technology that improves on legacy systems. Mobile devices provide enhanced security, including passcode protection for the phone, biometrics security features like a fingerprint, secure chip technology, geo-locational information to assist with verification, as well as both device and cloud based encryption and tokenization capabilities.

The payments industry is creating innovative solutions today to solve tomorrow's security threats. This protection ensures the flow of information vital to helping consumers access and use electronic payments, promotes competition and ensures the free flow of commerce, and maintains public confidence. It is imperative to find ways to encourage new technologies and enterprises, ensuring that the payments revolution will realize its maximum potential.

(4) ETA Members: Supporting Legislation to Promote Information Sharing

In addition to self-regulation and new security technology, ETA is working to remove barriers that prevent government and industry from sharing information about cyber threats. One lesson learned from recent high profile data breaches is that they are being perpetrated against U.S. companies by highly sophisticated and global cybercriminals. Along these lines, ETA is strongly supporting legislation, such as

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

H.R. 1731, the "National Cybersecurity Protection Advancement Act of 2015"[1] and H.R. 1560, the "Protecting Cyber Networks Act," both of which would promote sharing of Internet traffic information between the U.S. government and technology and manufacturing companies in order to help the government investigate cyber threats and ensure the security of networks against cyberattacks. Such legislation would provide a simple and effective means of sharing important cyber threat information with the government.[i]

(5) ETA Members: Supporting Legislation to Stream-line Consumer Notification of Breaches and Data Protection

Perhaps most pertinent to this hearing today, this Committee and the U.S. Congress have an important role to play in protecting consumers in the United States from the criminals who prey upon the financial system. One area ripe for reform is the unworkable and harmful state of regulations regarding consumer notification of breach events.

Currently, there is a patchwork of 47 separate state data breach notification laws with which retailers and the payments industry must comply, making uniform notifications virtually impossible while simultaneously making the process of notifying customers more costly, more cumbersome, and less timely. ETA is strongly supporting legislation to create, as H.R. 2205 does, a uniform national standard, preemptive of state law, for reporting financial data security breaches. One standard will provide certainty and predictability to consumers and the industry.

On setting a uniform data protection standard, ETA strongly supports the provisions in H.R. 2205, the *Data Security Act of 2015*, making data security a federal requirement for non-banks. The provision in the bill is both technology- and industry-neutral and flexible, reflecting the rapidly changing pace of technology

[1] HR 1731 has been merged into HR 1560.

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

and the wide array of companies that serve a major role in the current payments ecosystem. Protection of consumer data is crucial for all participants in the payments space to help prevent cyber theft of consumers' information. H.R. 2205 recognizes this, and ETA supports the bill.

Conclusion:

Headline-grabbing events inevitably lead to calls for additional government regulations. The members of the ETA are the first line of defense for consumers to avoid the fraud perpetuated by criminals in the financial systems. As described, the payments industry takes seriously this charge and works hard every day to detect and deter crime. ETA members are deploying multiple layers of protection, including EMV, tokenization, encryption, biometrics, and other payments technologies that secure systems against criminal intrusions and protect consumers and merchants. While we support legislation to provide a uniform, federal breach notification law, and flexible data protection standards for the payments industry, we believe that new burdensome regulations that dictate payment technology would ultimately harm consumers and retailers and would stifle nascent marketplace innovations that hold great promise for reducing future criminal activities and enhancing the payments system. Indeed, such regulation could be counterproductive, making the industry less capable of responding to the adaptive methodologies of cyber criminals and constraining the industry within a narrow band of allowable technologies on which criminals could concentrate their attacks.

As the trade association of the payments industry, ETA stands ready to assist the Committee in its efforts to ensure that consumers, merchants, and the economy continue to benefit from the safety and security of our nation's payments systems.

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

[2] Currently, the U.S. Secret Service, the US Computer Emergency Readiness Team, and the US Department of Homeland Security participate in information sharing through VERIS (Vocabulary for Event Recording and Incident Sharing), but more is needed.