Testimony of Scott Talbott,
Sr. V.P. for Government Relations,
Electronic Transactions Association (ETA)

House Small Business Committee
Hearing on the
EMV Deadline and What It Means for Small Business

Oct. 7, 2015

Introduction:

Chairman Chabot, Ranking Member Velazquez, and members of the Committee, I am Scott Talbott, Senior Vice President for Government Relations of the Electronic Transactions Association (ETA). Thank you for inviting ETA to testify on the EMV transition and what it means for small business.

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 – and the EMV migration is another major step forward in this regard.

The Electronic Payments Ecosystem – Driver of Economic Growth:

To help put the electronic payments industry into context, when consumers buy 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, dip, 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;
- 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;
- 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.

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.

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," the payments industry continues to innovate in order to further combat data breaches and protect consumers against increasingly sophisticated cyber criminals. It's our highest priority, since our business depends on customers entrusting us with their personal and financial data.

An important step in this security upgrade is the transition to more secure chip, or "EMV," cards, which use smart technology providing enhanced security.

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 25% 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, just last week, on Oct. 1, the payments industry implement a long-planned liability shift for their card transactions, at which point any participant in the transaction chain who is not EMV compliant became 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.

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 specifications) 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 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. Because counterfeit card represents the single largest type of card fraud in stores in the U.S. today, the EMV migration is the most important step we can take. But although chip cards reduce the value of compromised data by inhibiting the creation of counterfeit cards, they do not stop data breaches. Later in my testimony, I will describe other initiatives within the industry that 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.

Small Business Merchant Perspective

Of course, EMV-enabled cards are only half the EMV-migration equation, the other half is whether merchants have converted their point of sale terminals to accept them. Merchant acceptance of EMV cards is voluntary, and there are any number of factors facing individual small business merchants at this juncture which may affect their relative focus on, and timing for, their respective conversions. For instance, the cost of the conversion of terminals for the average small business merchant is in the $50 - $500 range, and the cost and complexity vary depending on whether a small business merchant only needs to convert a single terminal, versus those with multiple terminals or terminals with integrated systems that combine payments functions with other functions, like inventory or payroll. For some, conversion to new EMV terminals may provide them an opportunity to upgrade to near field communication-enabled terminals in order to also be able to accept mobile payments, adding additional benefit for the merchant to convert sooner rather than later. In addition, there is a certification process all merchants must undertake in order to ensure compliance with card network rules and safeguards. On a much more practical level, we expect merchants right now are focusing on the upcoming holiday shopping season, but that migration efforts will really resume in 2016 after the holidays when many small business merchants renew their contracts with the card networks.

However, given that it was only last week that the official EMV liability shift happened, it appears as if the migration for some small business merchants will lag behind other businesses, especially if a small business merchant is the type where the likelihood of fraudster using a fraudulent card is low due to the low dollars involved in an average transaction -- like at a dry cleaner or a car wash – and the resulting financial exposure to the merchant from the fraudulent transaction is, therefore, low. Put another way, a small business merchant may view the need to convert to EMV terminals – in order to avoid liability for a $16 dry cleaning bill or a $10 car wash paid for by a fraudulent card – as a relatively low priority. By contrast a small jeweler's risk of liability for a fraudulently purchased $6,000 diamond ring likely provides a greater incentive to convert to EMV terminals as soon as possible. Small businesses will make this risk/reward calculation, and this will cause variation amongst small business merchants in their respective EMV migration rates. At the end of the day, in the near term, the migration may require small business merchants to teach consumers how to check out with their newly-issued EMV cards in the new point of sale terminals in order to keep customer transactions flowing smoothly, and this will take some effort on the merchant's part.

All of that said, there are any number of payments industry financial assistance and incentive programs to assist those merchants who many need it, and ETA has an educational website, www.sellsafeinfo.org, to assist small business merchants with the EMV migration. Additionally, ETA's own Risk and Fraud Council recently published materials for small merchants to determine what they need to do when a breach occurs.

Finally, ETA is a participant in the PCI Security Standards Council Small Merchant Task Force. The goals and objectives of the task force are focused on ensuring that small merchants understand their responsibility for protecting payment card data and to identify and mitigate areas of risk in their environment. The payments industry has, and will continue, to educate and assist small business merchants in this regard.

EMV Chip and Cardholder Verification Methods

While this hearing specifically focuses on EMV, it is important to note that 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 in stores. Put another way, this ensures that the card itself is valid. The protection provided by EMV cards does not require a PIN. 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 specific 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 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. It could also result in a shift of additional liability for fraudulent card transactions to those merchants that do not have a PIN pad.

Similarly, not all mobile payments can 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.

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 the bank that issued the card knows the 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.

Additionally, many payment companies continue to innovate advanced computer systems that monitor transactions and data patterns 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 may well 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 – like voice and facial recognition- 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.

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