Testimony of

Paul Weston
Of
TCM Bank, NA
Tampa, FL

On behalf of the

Independent Community Bankers of America

Before the

United States House of Representatives
Committee on Small Business

Hearing on

"The EMV Deadline and What It Means for Small Businesses"

October 7, 2015
Washington, D.C.

Chairman Chabot, Ranking Member Velazquez, and members of the committee, my name is Paul Weston, and I am President and CEO of TCM Bank, N.A. in Tampa, Florida. I testify today on behalf of the more than 6,000 community banks represented by the Independent Community Bankers of America (ICBA). Thank you for convening this hearing on the migration to EMV chip credit and debit card technology and what it means for small businesses. We're grateful to you for raising the profile of this important topic.

TCM Bank, N.A. is a $178 million asset bank that serves as the credit card issuer and "back office" for over 650 community banks that have chosen to outsource the specialized function of credit card issuance. TCM Bank community bank clients brand and market their credit cards, expand their product offerings and customer relationships, and gain access to a new revenue stream, without committing financial, technical, or personnel resources to the day-to-day administration of a credit card program. This arrangement allows our community bank clients to focus on their core lending competencies: small business, consumer, and farm lending. TCM operates by the values and standards of service of our community bank clients.

The community bank business model is directly linked to the success of their small business customers. Community banks hold a disproportionate market share of small business loans – nearly 50 percent – though they hold less than 20 percent of all banking assets. ICBA and its community banks members take a keen interest in the migration to EMV chip cards, both as card issuers and as partners with the small businesses that are so important to the national economy. Locally-managed community banks are uniquely positioned to help small businesses make a smooth transition to EMV chip cards and are committed to doing so. TCM talks with community banks and their small business customers every day.

Before discussing in greater detail the ongoing migration to EMV chip and the respective roles of card issuers and merchants, I would like to stress that consumers – your constituents – are not on the hook for fraud losses as all credit cards have zero liability provisions for consumers and the Electronic Funds Transfer Act limits consumer liability for any fraud on debit cards. This is true whether or not the card issuer or the merchant is EMV chip compliant.

Small businesses that are involved with retail are already being presented with payment cards with an EMV chip on the front of the card in addition to the familiar magnetic stripe on the back of the card. In order to process those cards using EMV chip technology at the point of sale, most small business merchants will need to upgrade their terminals and train their front line staff to assist customers.

EMV chip cards contain a microprocessor that generates a unique, one-time code to authenticate card transactions. If the card information is stolen, it is useless to a criminal because it cannot be used to conduct another transaction. EMV chip cards are much more secure than magnetic stripe cards because they are exponentially more difficult to counterfeit. Counterfeit cards made with stolen information represent the largest portion of fraud in the United States. And while consumers are protected against loss, having to replace a credit or debit card is inconvenient at best. EMV chip cards, together with merchant-provided chip readers at the point of sale, will play a critical role in reducing counterfeit fraud for both debit and credit cards.

Community banks are joining other financial institutions in the orderly migration to deploy EMV chip technology for debit and credit cards. This migration is already underway. A story in *USA Today* last week reported that roughly four in ten consumers already have an EMV chip card.

There is no legal mandate that card issuers adopt EMV chip or that retailers invest in EMV chip card readers. However, new rules in the card industry took effect on October 1, 2015 that will incentivize a shift to EMV chip technology that is in the best interest of all parties. The new rule provides that liability for fraudulent transactions sits with the party (i.e. retailer or bank) that didn't invest in chip technology. In a case where the bank doesn't offer chip cards and the merchant doesn't have a card reader, the bank will continue to be held responsible for covering the cost of the fraud. Similarly, in a case where both the bank and the merchant are chip compliant, the bank will continue to be responsible for losses incurred from fraudulent use. The October 1 liability shift represents a change in economic incentives rather than a legal mandate.

October 1 is not a *deadline* in any meaningful sense of the word. Instead the liability shift serves as a catalyst for change. Already, many card issuers and merchants have adopted EMV chip. Others will limit their liability exposure by adopting EMV chip before year-end. Some will choose to defer adoption into 2016 or even 2017 for automated fuel dispensers. Each issuing bank and each merchant will decide when to adopt EMV chip based on its own business model, vulnerability to fraud, and management of risk. The timing to complete each bank's reissuance of all cards in chip form will vary. Community banks will weigh the implementation and issuance costs with potential risk and demand from consumers. The migration to full EMV chip card usage will likely take several years to accomplish.

Based on many conversations with community banks and their small business customers, I believe that most small businesses are taking a very prudent approach to the migration. They are not buying from the first terminal salesperson who calls, and they are planning to closely follow as larger national retailers begin to enable EMV chip at the point of sale.

To give you a sense of what's involved for community banks, the initial costs of issuing EMV chip cards fall broadly into three categories:

1. *Card production and deployment*- Includes artwork and card redesign, acquiring new inventory of card stock, card personalization, and postage.
2. *Implementation* - Includes programming, software upgrades, processor costs, and new authorization techniques. ATMs and branch card issuance systems also need to be upgraded.
3. *Training*- All parties have to be trained. Community banks will focus on educating the cardholders as they adapt to a new way of presenting a card for payment at the point of sale in addition to training bank personnel and merchants to ensure that all parties can assist the consumer, even at the point of sale.

For merchants, the costs involve the purchase, deployment, and activation of EMV chip card readers. They must also train retail personnel to assist cardholders in the use of an EMV chip card. Community banks will serve as an important ally and resource to smaller retail businesses making the transition. They will help their merchant customers by providing equipment, expertise, and education to guide them through this change. Since community banks are local, they serve as "feet on the street," especially for the small businesses in their communities.

For consumers, the transition will involve relearning a process which has become second nature. Instead of swiping a card through the magnetic stripe slot, a process that has become very well ingrained over many years, using an EMV chip card involves inserting the card into an open slot and leaving it there for a short time as the transaction is completed. Community banks are actively working to educate and reassure their customers about these changes coming to the point of sale.

While EMV chip cards are an effective means of reducing fraud related to counterfeit cards, they are not a panacea for all types of payment card fraud. Multiple layers of security technologies are needed in addition to EMV chip to mitigate other types of fraud. Card numbers and cardholder information must still be protected. The PCI Data Security Standards provide requirements for all merchants and processors to mitigate data breaches and compromise events that fuel payment card fraud. End-to-end encryption should be deployed to protect cardholder information while in transit, and newer technologies, such as tokenization, should and will be developed and deployed to protect online transactions.

Until this layered approach can be fully implemented, consumers should know that banks comply with significant legal and regulatory requirements and are subject to rigorous examination and supervision of their data security practices and procedures.

Some are touting PIN in combination with EMV chip as the only way to eliminate payments fraud. We believe any form of a PIN mandate would be misguided for a number of reasons. First, PINs only protect against fraud in cases of lost or stolen cards, which is a relatively small portion of total fraud. Second, as a static data element, PIN is more vulnerable than active technologies like EMV chip or tokenization. As PIN use becomes more prevalent, it attracts more criminal activity. A 2012 report by the Federal Reserve Bank of Atlanta found that debit PIN fraud rates have increased more than threefold since 2004.

Additionally, in order to better protect consumers, all participants of the payment system – including merchants – should be subject to the same federal data security standards and oversight as financial institutions. ICBA supports legislation introduced by Reps. Randy Neugebauer (R-TX) and John Carney (D-DE), the Data Security Act (H.R. 2205), that would apply Gramm-Leach-Bliley Act-like data security standards for all industries that handle sensitive financial information.

Closing

Thank you again for the opportunity to testify today. We hope that this hearing will help to educate all stakeholders, especially small businesses and consumers. The engagement and cooperation of all parties is critical for a smooth transition to EMV chip which will ultimately reduce fraud and bolster confidence in the payments system.