THE VOICE OF FOOD RETAIL
Feeding Families Enriching Lives

October 21, 2015

Chairman Steve Chabot
House Committee on Small Business
2371 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Nydia Velázquez
House Committee on Small Business
2302 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Chabot and Ranking Member Velázquez,

The Food Marketing Institute[1] commends you for holding the hearing entitled, "*The EMV Deadline and What it Means for Small Businesses: Part II.*" It is essential that the merchant's voice is heard on this most important issue. FMI was particularly pleased that you invited one of our board members, Art Potash of Potash Markets, a family-owned, three store company in Chicago, Illinois to testify about his company's experience migrating to EMV. Art is an active member of the FMI Independent Operator Committee and will be a great addition to your panel. In addition to the perspective that Art Potash offers, FMI would like to offer this letter highlighting what we have learned from our members in the supermarket industry regarding EMV migration here in the United States for the Committee record.

For the past four years, since Visa and then MasterCard and the other card brands announced their roadmaps for migrating to EMV in the United States, EMV migration has been a top priority for our members. Through the FMI Electronic Payment Systems Committee, we have held numerous interactive EMV migration sessions, starting four years ago and continuing through the first half of 2015. We engaged with experts involved in EMV migration in Europe on the food retail side to get their perspective and lessons learned. Unfortunately, the card brands have not rolled out EMV in the U.S. in the same or a similar fashion to the implementation globally.

Need For PIN-Enabled Cards

[1] Food Marketing Institute proudly advocates on behalf of the food retail industry. FMI's U.S. members operate nearly 40,000 retail food stores and 25,000 pharmacies, representing a combined annual sales volume of almost $770 billion. Through programs in public affairs, food safety, research, education and industry relations, FMI offers resources and provides valuable benefits to more than 1,225 food retail and wholesale member companies in the United States and around the world. FMI membership covers the spectrum of diverse venues where food is sold, including single owner grocery stores, large multi-store supermarket chains and mixed retail stores. For more information, visit www.fmi.org and for information regarding the FMI foundation, visit www.fmifoundation.org.

One of the most notable differences between EMV in the U.S. and globally is the lack of the requirement that credit cards be PIN-enabled. As you know, a PIN, a personal identification number, is unique to the user of the card and is a simple way of verifying the individual presenting the card is indeed authorized to use it. PIN is universally considered to be far safer than a signature verification method that does nothing to ensure the person using the card is actually authorized to do so. The migration to EMV chip and PIN was successful in other parts of the world because the card networks and issuing banks recognized the effectiveness of PIN in reducing lost and stolen credit card fraud and made it a practice to issue cards with a PIN and then give merchants an incentive to make the investment in reducing fraud via lower card acceptance costs.

Unfortunately, in the U.S. the card brands have taken the unprecedented path of allowing for "chip and choice," where issuing banks can make the business decision whether to issue PIN-enabled cards or stick with the fraud-prone signature cards. Unfortunately, the vast majority of banks so far have chosen the easier route of issuing signature cards instead of the safer PIN-enabled cards – the path suggested by the White House and chosen for federal government payment and benefit cards.

This is particularly frustrating for the grocery industry, which is already fully enabled to accept PIN authentication. Every day, customers enter their PIN to get cashback at our registers or to use government issued benefit cards for programs like SNAP and WIC. Grocers are ready and willing to utilize the more robust PIN authentication, but unfortunately the card brands have held firm against requiring banks to issue these safer cards, leaving us with the untested "chip and choice" option as the one most widely seen in the current marketplace.

We are also challenged to find logic in the issuers' new line of arguing that a PIN is not safe because it is a static number that does not change, and if it were to become compromised is useless. They argue that because the PIN is set, and not dynamic it is not secure and instead say they want to look forward to using biometrics such as fingerprints. This is an interesting argument, as anyone who has been issued a debit card with a PIN knows; you can go to your bank and change it if you think it may have been compromised or if you forgot the number. However, as many former and current government employees recently learned from the Office of Personnel Management breach, once your thumb print is compromised in a data breach, you cannot "reset" it like a PIN. We agree, technology is advancing, and new solutions are coming to the market, but arguing PINs are not secure because they are "static" is inherently flawed. Additionally, we know PIN works today to reduce fraud. It is tried and proven on debit cards, government benefit cards and credit cards in Europe and around the world. The card brands should move as they have in other countries to require banks to PIN-enable all cards and allow a merchant to require a PIN for transactions.

FMI would also like to respond to a point that was raised during the first hearing when a member asked about whether a merchant could require a customer to enter a PIN. We felt that the question went unanswered, and would like to point out that under the existing operating rules, a merchant may not require a PIN for a transaction that does not include cashback under the current Visa, MasterCard and other brands' operating rules. The operating rules allow a merchant to prompt for PIN, but a customer may bypass the prompt and choose only a signature. The card brands require all merchants, small, medium and large, to comply with all of their operating rules or face extraordinary fines for non-compliance. It is worth noting that the card brands and banks continue to see the value in PINs as they still require a customer to enter a PIN in order to withdraw money from their ATMs. All we ask is that merchants be given the opportunity to utilize the same level of authentication.

As an interesting point, some of our members have reported that because the card brands decided to change course and go with "chip and choice" unlike the traditional and proven "chip and PIN" solution it complicated the migration here in the U.S. and slowed the process down. Instead of taking what was used in the United Kingdom and throughout Europe, Canada and elsewhere as a starting point, they had to provide additional specification for "chip and choice."

In short, PINs are proven and available in the market today. While issuers may have decided to make the business decision against issuing PIN cards, it was not in the name of security. For your reference, we have included a very informative article from the September 2015 issue of *Digital Transactions*, "EMV's Signature Moment." In this article, the author outlines three business drivers that led banks to decide not to issue PINs, first their concern of consumer experience and if a bank put a PIN on a card, the consumer would pick the one without it instead. The article also explained that there lacked a return on investment for banks, and finally the actual bank's processor capabilities and need for upgrading to process larger PIN volumes. Nowhere did the article suggest that banks chose not to issue PIN due to security concerns.

The Continued Cost of Accepting Credit and Debit Cards

Another important point that was raised during the last hearing was the anticipated savings from fraud reduction post-EMV migration, and if Visa expected to share any of those savings with the merchants. Unfortunately, Visa reaffirmed merchants' fears that they currently have no plans to share savings seen from reduction in fraud due to EMV migration with merchants. American merchants paid the card brands over $71 billion in interchange fees in 2013. The card brands have long defended these extraordinary fees saying they needed them to help cover their fraud costs. So now, when they are pushing merchants to invest billions to upgrade to EMV in the name of fraud reduction, they are not planning to share savings resulting from the investment in

EMV equipment and cards, leaving U.S. merchants to still pay an overwhelming bulk of global interchange fees.

When you couple this with the pure lack of financial incentive beyond facing additional fraud liability for EMV migration, American merchants are clearly going to be paying more, not less. Visa, MasterCard and the card brands have continually said EMV is not mandated on merchants; it is their choice. First, supermarket retailers have been investing for years in payments security. We want our customers' transactions and data to be secure. This is true, however, merchants are left with the choice of not investing significant funds and being saddled with new additional fraud costs on top of what they are already paying in interchange and chargebacks, or invest heavily to upgrade to EMV. This is different from the choice banks were given. Banks could choose to maintain their current fraud liabilities and not issue chip cards, or chose to issue chip cards and be rewarded with lower fraud costs. The banks were given a clear financial incentive, where merchants were given threat of higher costs if they did not.

FMI's members have invested significant funds in EMV-compliant terminals, software interfaces and certification to migrate to EMV and hopefully a more secure system here in the United States. Many of our members are now EMV certified and are currently accepting EMV cards today. Many more are still in the process, having purchased EMV-compliant terminals months ago, yet still waiting for certification of the links to their merchant acquirer and other vendors. In the meantime, until the other links are ready, they will continue to accept cards and potentially face higher fraud liability heading into the busy holiday season.

What to Expect Next

Last week, merchants in the United Kingdom were notified by their merchant acquirers that the Near Field Communications (NFC) "option" they have had since migrating to EMV will no longer be an option; it will now be required. Visa and MasterCard are now mandating that all merchants turn on and become NFC certified in the United Kingdom. This is a very different message from what the committee heard from Visa during the last hearing. The witness from Visa testified that NFC was a feature and was optional for merchants as they migrated to EMV. American merchants were essentially put on notice last week that mandatory NFC is what we should expect next.

The card brands have chosen NFC as their mobile solution, but there are others already in the market, and more that can still come. Some mobile solutions utilize reading QR codes; others use blue tooth technology or the existing magnetic stripe reading solution that is already in the point of sale devise. By mandating NFC, the brands are ensuring that all point of sales take their solution even if a merchant would prefer to use a QR or blue tooth solution instead.

This mandate is particularly troubling as merchants look toward mobile payments solutions and the opportunity for real competition entering into the payments space. With Visa and MasterCard mandating merchants turn on and accept all NFC transactions, they are essentially ensuring their hold on the market requiring that merchants accept their mobile solution universally. This is something American merchants had feared. It is also important to note, beyond the policy concerns that the mandate brings, there is always a cost associated with it as well. It is not as easy as flipping a switch for a merchant to start taking NFC transactions. They will have to again invest funds into both programming and certification. These are costs that will certainly come out of the merchant's pocket, yet again without any promise of a rate reduction.

The Payments Realm Needs Real Competition

Currently, Visa and MasterCard hold over 85% of that credit and debit card market. In dollar terms, Visa and MasterCard debit, credit and prepaid cards that were issued in the United States generated over $3.6 trillion in purchase volume in 2014. That kind of market power has worked to block others from entry and threaten to do the same when our economy migrates to mobile payments.

Conversely, the grocery industry is incredibly competitive with large and small merchants competing every day to earn and keep customers. They do this by keeping costs low, in fact, the grocery industry averages around 1% profit margin every year. Merchant customers have benefited from lower costs, greater benefits and numerous options on where to spend their grocery dollars.

It is time the credit card industry became an open and competitive market, where efficiencies and competition drive down the cost for merchants to accept these payments. Mobile offers the possibility of new players and greater competition, but it is essential that the card brands not be allowed to put up road blocks preventing others from entering into the market.

The Need for Federal Data Security Legislation

Finally, FMI would like to respond to the bank and credit union witness's call during the last hearing for support for H.R. 2205, the Data Security Act of 2015. FMI has members operating in every state, many operating in multiple states. Currently, merchants must comply with a myriad of state data security and breach notification laws. Grocers and many other merchant groups have long advocated for a federal data security and breach notification standard to replace the various and sometime conflicting state laws. However, we strongly believe that any federal law must be written carefully to ensure it is not overly burdensome on any of the industries covered by the law. Unlike the Gramm-Leach Bliley law that was written specifically for one industry, the banks and financial institutions, this federal law would cover anyone who accepts a

credit or debit card --including a dentist, political campaign, grocer and charitable cause. All of those entities have unique needs and what works for a grocer with regard to breach notification would be different than what a dentist or charitable cause should do. FMI and our members advocate for a federal law that allows for the flexibility to tailor standards to meet the needs of a particular business in a particular industry. Unfortunately, as written, H.R. 2205 attempts to place standards that were written specifically for banks and those in the financial services industry on anyone who accepts a credit or debit card, including the smallest merchant. FMI has engaged with the bill drafters and is actively working to reach a compromise that will take into consideration the Federal Trade Commission's existing authority reflect the various needs of all industries covered under the legislation. Additionally, a basic premise for breach notification should be that the breached party notifies. There may be places for an exception, but merchants believe that the underlying standard should be that the breached party notifies. In its current form, H.R. 2205 does not meet that standard and could leave small businesses liable for notifying customers about a breach when they were not even the one breached. FMI is committed to working with the bill drafters to address these challenges and ensure that any legislation is written to properly cover all industries without unnecessary subjecting anyone, particularly small businesses, to unnecessarily liability or punitive overly burdensome actions.

Conclusion

Clearly it is a pivotal time for merchants in the payments sphere. We commend the committee for taking an active interest in EMV migration and how America's small businesses are faring under the card brands' initiatives. Thank you for your interest in this matter, and we look forward to working with you on EMV and other issues moving forward.

Sincerely,

Jennifer Hatcher
Senior Vice President
Government and Public Affairs

VOLUME TWELVE, NUMBER NINE • DIGITAL TRANSACTIONS.NET • SEPTEMBER 2015

DIGITAL TRANSACTIONS

Trends in the Ele xchange of Value

PayPal Unchained

Free of eBay, what will it do now that it calls all the shots?

ALSO IN THIS ISSUE:

- Mobile Payments' Second Act
- EMV's Certification Headache
- Nothing Inapt About In-App Payments
- PINs Vs. Signatures

EMV's Signature Moment

By John Stewart

While PINs are more secure, signatures are by far card issuers' preferred authentication method for U.S. EMV credit cards. Why?

By the time you read this, the big EMV deadline will be anywhere from 15 to 30 days away. Yet, with so little time remaining, the effort to implement the chip card standard in the United States faces any number of hurdles, from certification headaches (page 16) to lagging merchant terminal adoption.

And you can add one more item to the list: the PIN vs. signature controversy. It's one of the oldest disputes in the brief history of American EMV, but merchants are still wrangling with banks over the question of whether chip cards should be universally issued with PINs—credit cards as well as debit.

Merchant groups have aggressively pushed PINs for EMV ever since the card networks got serious four years ago about the conversion from magnetic-stripe cards to the chip card standard. But most U.S. financial institutions that have issued EMV credit cards so far have overwhelmingly done so with the signature authentication so familiar from decades of card swiping.

In fact, issuers are so entrenched in signature-card issuance that some experts see signature-based EMV credit cards as a *fait accompli*. "This train has left the station whether it'll be PIN or signature," says Nick Holland, a senior analyst at Javelin Strategy & Research, Pleasanton, Calif., who follows EMV.

But the issue simply won't die, even with a crucial deadline only weeks away.

By card-network rules, merchants that aren't prepared to accept EMV chip cards by Oct. 1 will assume liability for any counterfeit fraud (some networks add lost-and-stolen fraud) losses—losses that are currently borne by the issuer. The issuer will continue to bear those losses if the card involved isn't EMV-compliant.

'Worthless' Signatures

Despite the deadline's proximity, merchant groups aren't giving up. They're adamant that PINs are surer barriers to fraud than signatures, which a number of retail executives over the years have dismissed as "worthless."

Their latest salvo came out in July in the form of a survey of 84 IT decision makers conducted in May and June by business-technology company Randstad Technologies. The study not only concluded PINs were superior to signatures, it all but called for an industry mandate that issuers adopt PINs. Nearly two-thirds of the respondents preferred PIN security for EMV.

"The majority (66 percent) believe chip and signature does not offer ample security and that PIN technologies should be required," reads a Randstad summary of the survey results.

"If there's anything surprising in these numbers, it's that nearly six percent of respondents believe that mag-stripe technology offers sufficient security," summary continues. "That's a perspective that's been undercut on many occasions by costly security breaches to a number of prominent businesses."

Merchants are also questioning why they're spending so much time and money on EMV training and installations when their chip readers will end up accepting only signature-based credit cards.

"Retailers are investing billions to implement new chip-enabled card readers in stores nationwide. They're asking banks and credit unions to meet that commitment by issuing new chip cards with PINs," says the Arlington, Va.-based Retail Industry Leaders Association in a recent press release.

The retailer faction received further support this summer from no less a figure than a governor of the Federal Reserve Board.

"New approaches to authentication increasingly offer greater assurance and protection. Given the current technologies that we have at our disposal, we should assess the continued use of signatures as a means of authenticating card transactions," said Fed governor Jerome H. Powell in a speech given late in June at a payments conference at the Kansas City Fed.

To be sure, some financial institutions have gone with something they refer to as "chip and choice," an approach by which they support online PIN authentication as well as signature.

A prominent example is Raleigh, N.C.-based State Employees Credit Union, the second largest credit union in the country. SECU issues all of its EMV credit cards with PINs and allows its cardholders to authenticate with either the PIN or a signature, says Leanne Phelps, senior vice president for card services.

So far, though, less than one-half of 1% of all of SECU's credit card transactions have been PIN-authenticated. And of the 120 million or so EMV cards U.S. financial institutions had issued by the start of the year, the great majority were credit cards requiring only a signature from the cardholder.

That number is expected to balloon to 600 million by the end of 2015, according to the EMV Migration Forum, an industry trade group. Most will still be credit cards, and no one's betting that any appreciable number of them will require a PIN.

'Pretty Stupid'

So, with merchants insisting on PINs for EMV, and with few doubting that PINs are more secure, why are banks and credit unions mostly issuing signature-based credit cards? The reasons are manifold, but fall into three broad categories: consumer experience, return on investment, and processor capability.

Experts cite consumer familiarity with signature-based credit cards—along with a dearth of consumer education about EMV—as a prime reason issuers are sticking with signature authentication.

They don't want to see their cards disfavored by consumers who aren't accustomed to memorizing and entering a PIN. Typically, if you forget your PIN, it's hard to start all over and use a signature. "If your card is suddenly harder to use, you lose top of wallet," notes Rick Oglesby, senior analyst at Double Diamond Research, Centennial, Colo.

So, "issuers are defaulting to the method they know always works," says Louis Buccheri, an analyst at Auriemma Consulting Group, New York City.

Besides that, the type of fraud issuers are most concerned with is counterfeit fraud, which chip cards are pretty effective at preventing. Lost-and-stolen fraud, which PINs would prevent, comes to a much smaller total.

Indeed, of all card-fraud losses, 37% are attributable to counterfeit cards, compared to 14% for lost-and-stolen cards, according to a study of 18 of the 40 largest issuers conducted in 2014 by Aite Group, a Boston-based research firm.

That makes it harder for issuers to justify investments in credit card operations to handle PIN resets, among other back-office changes. "Lost-and-stolen is the only thing PIN buys you [as an issuer]. It was a pretty easy business case for chip-and-signature," says Julie Conroy, a senior analyst at Aite.

Finally, issuers that are supporting online PINs with EMV credit cards, like SECU, are doing so with in-house systems. Or they've signed up with a processor that can handle credit card PINs.

But it turns out some processors that handle card transactions on behalf of issuers haven't geared up for PINs on credit card transactions, say Conroy and other experts. "A lot of the [third-party] issuer systems on the credit card side are really pretty stupid," says Steve Mott, principal at Stamford, Conn.-based payments consultancy BetterBuyDesign.

How Long?

Most markets around the world that have adopted EMV, such as Canada and United Kingdom, are using offline PIN authentication (chart). In this configuration, the card relies on its embedded chip to match the PIN entered at the terminal with the encrypted PIN in the chip. But this method relies on a more powerful, and hence more expensive, chip.

That's another thing that makes EMV credit cards a more costly proposition for issuers. After all, they're also racing to get cards out the door, and not just because of the liability shift. They know that the last mag-stripe issuer will be the one on which the fraudsters will focus all their considerable resources.

Still, no one is ruling out EMV credit card PINs forever. The superiority of PINs over signatures can't be denied, after all, when cardholders catch on and start asking about the matter. It would just be nice to know how long that's going to take. DT

How the World Verifies EMV

(Preferred methods)

Country or Region	Signature	Online PIN	Offline PIN
Asia[1]	✓		
Australia		✓	
Bahrain			✓
Belgium			✓
Brazil			✓
Canada			✓
Estonia			✓
Finland			✓
France			✓
Germany	✓		
Ireland			✓
Italy	✓		
Kuwait			✓
Mexico	✓		
Netherlands			✓
New Zealand		✓	
Norway			✓
Poland			✓
Portugal	✓		
Qatar			✓
Russia	✓		
Saudi Arabia			✓
Slovakia			✓
Spain	✓		
Sweden			✓
Turkey	✓		
U.K.			✓
U.A.E.			✓

1 Except Japan Source Aite Group