STEVE CHABOT, OHIO
CHAIRMAN

NYDIA M. VELAZQUEZ, NEW YORK
RANKING MEMBER

# Congress of the United States
## U.S. House of Representatives
## Committee on Small Business
2361 Rayburn House Office Building
Washington, DC 20515–6315

**Memorandum**

| | |
|---|---|
| To: | Members, Committee on Small Business |
| From: | Committee Staff |
| Date: | October 7, 2015 |
| Re: | Hearing: "The EMV Deadline and What it Means for Small Businesses" |

---

On Wednesday, October 7, 2015 at 11:00 a.m. in Room 2360 of the Rayburn House Office Building, the Committee on Small Business will hold a hearing to examine the implications of the Europay, MasterCard, Visa (EMV) chip deadline for small businesses and the efforts that are being made to ensure America's small businesses are in compliance with the requirement of these credit card processors. Financial service providers mandated an October 1, 2015 deadline for customers to shift point-of-sale (POS) terminals to an EMV chip system. The upgraded technology is designed to enhance protection against cybercrime and fraud. However, many small businesses are unprepared for this new technology. These businesses will not only be more vulnerable to cyber threats, but they also will be held liable for certain incidents of fraud. A July 2015 study observed that less than 49 percent of small businesses are aware of the October 1 date and liability shift.[1]

## I. Background

In the early 1990s, financial institutions believed chip-based payment systems and international standards for electronic payments were essential to ensure global interoperability of credit card-based transactions. In 1994, Europay, MasterCard, and Visa joined together to create EMV. EMV is the trademark owned by all of the equity owners of EMVCo: American Express, Japan Credit Bureau (JCB), Discover, MasterCard, UnionPay, and Visa.[2] However, EMV also refers to the various forms of electronic payments that are administered by EMVCo.[3] EMVCo states that "as the industry has evolved, additional EMV Specifications have been written to advance new payments initiatives" and EMV now includes several other transaction types as well.[4]

EMV cards contain a microchip inside which is designed to protect cardholders from cyber theft during transactions. All United States credit cards currently store the card number on a magnetic stripe on the

---

[1] WELLS FARGO/GALLUP, SMALL BUSINESS SURVEY TOPLINE 3RD QUARTER, JULY 10, 2015, [hereinafter "WF Survey"], *available at* https://wellsfargoworks.com/File/Index/btDsu4gv9UqK07hpFKVbgw.
[2] https://www.emvco.com/about_emv.aspx.
[3] *Id.*
[4] EMV has evolved from a single, chip-based contact specification to include EMV Contactless, EMV Common Payment Applications (CPA), EMV Card Personalization, and EMV Tokenization. Chip-based contact specifications are different methods of EMV payments.

back side of the card. When a cardholder swipes the card at a checkout terminal, the computer verifies the card information from the magnetic stripe and authorizes the transaction with the retailer. However, the information transmitted via the stripe is a static number,[5] meaning cybercriminals only have to acquire the credit card number from the terminal or database once to carry out transactions at other retailers.

The EMV standard for credit cards requires the use of a microprocessor chip so that the card generates a unique code for every transaction which renders the card useless if a criminal has stolen the card number from a retailer because the chip number is only good once.[6] EMV chip technology has been standardized throughout much of the world. In the fourth quarter of 2014, nearly 1.8 billion chip cards had been deployed outside of the United States and less than 10 percent deployed in the United States.[7] In the same year, more than 96 percent of transactions in the European Union (EU) were made with EMV chip cards.[8] Additionally, the EMV system in the EU uses chip-and-pin rather than chip-and-signature[9] – opponents of the new EMV technology shift state, "while chip cards are difficult to counterfeit … a PIN provides another layer of security that shouldn't be tossed aside."[10]

## II. Migration to EMV

There have been several issues prompting the adoption of EMV chip cards in the United States. Data breaches are increasingly disconcerting for both financial service providers and merchants. Current data suggests that there has been a noticeable increase in the number of security breaches between 2012 and 2013.[11]

The cyber breaches associated with credit cards increased to $5.3 billion in 2012 – up nearly 15 percent from the previous year – created an incentive to find a more secure technology.[12] This represented a growing trend in which the Federal Reserve Bank of Atlanta found that incidents of fraud involving United States credit cards rose 70 percent between 2004 and 2010[13] and all parties involved in the transaction were affected negatively.[14] A number of high profile data breaches have been widely covered in the media which has contributed to consumer weariness and caused retailers to take significant financial losses. For example, the New York Times reported that "Target's data breach shook customer confidence in the retailer at a critical time, and executives have said it had a noticeable effect on the bottom line."[15]

---

[5] A static credit card number is one in which the numbers and pattern is the same for every transaction.
[6] http://consumerist.com/2015/08/06/most-small-business-owners-arent-ready-for-chip-and-pin-credit-cards/.
[7] https://www.emvco.com/documents/EMVCo_Card_present_EMV.pdf.
[8] *Id.*
[9] Chip-and-pin transactions require a personal identification number to authorize payments while chip-and-signature requires the cardholder's signature.
[10] https://nrf.com/news/eyes-only-visa-document-says-pin-is-safer-signature.
[11] VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 9, *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.
[12] http://www.economist.com/news/finance-and-economics/21596547-why-america-has-such-high-rate-payment-card-fraud-skimming-top/.
[13] FEDERAL RESERVE BANK OF ATLANTA, CHIP-AND-PIN: SUCCESS AND CHALLENGES REDUCING FRAUD at 20 (2012), *available at* https://www.frbatlanta.org/rprf/publications.aspx.
[14] *Id.*
[15] Hiroko Tabuchi, *$10 Million Settlement in Target Data Breach Gets Preliminary Approval*, THE N.Y. TIMES, Mar. 19, 2015, *available at* http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0.

## III. Adoption of EMV – Barriers in the United States

EMV technology and its use around the world has shown to be effective in reducing credit card fraud. As a result, credit card issuers in the United States established an October 1, 2015 deadline for retailers and others to have EMV technology for credit card transactions. For those businesses that have not adopted the technology, the liability for fraud will shift from banks to merchants. Despite the deadline, adoption of EMV chip technology has been slow to catch on in the United States. A July 2015 survey of small businesses observed that 34 percent of small businesses intend to upgrade their credit card processing system to begin accepting EMV credit cards at some point in the future, but not until after October 1, 2015.[16] Additionally, another report claims that 7 percent of small businesses are not even aware of the October EMV liability shift.[17] However, financial service providers claim to be making sincere efforts to prepare merchants for the liability shift. For example, the electronic transaction startup, Square Inc., has been offering merchants a chip-card reader at no charge.[18]

Industry experts note that the United States market poses challenges that make the shift to EMV more cumbersome than it has been for other countries. For example, former Governor Tim Pawlenty said in a recent Committee on Financial Services hearing that "most other EMV markets do not have 14,000 financial institutions and tens of millions of merchants that need to move in relative unison to implement EMV . . . the magnitude of the change is different in the United States and that change requires a significant overhaul of current systems."[19]

Additionally, opponents of the financial services firms' EMV deadline argue that the high cost of implementation of EMV is a deterrent to embracing the new system. Many industry observers agree that the new technology will cost merchants $4.5 billion.[20] Experts estimate that the cost for an individual retailer could be as high as $600 per payment terminal;[21] however, companies like Square could offer card readers that reduce the cost per terminal to less than $100.[22]

Another hurdle to the implementation of EMV technology has been the retail community's reluctance to switch. A major point of contention between the retail community and financial service providers is the card issuing firms' decision not to issue chip-and-pin cards.[23] Notably, in June 2015, Governor Jerome Powell of the Federal Reserve suggested that PINs offer a strong level of protection and that "the deployment of EMV chip cards in the United States represents an important step forward. But we should

---

[16] WF Survey, *supra* note 1, at 33.
[17] http://www.softwareadvice.com/retail/will-smbs-meet-emv-deadline/.
[18] Ruth Simon, *Small Businesses Are Slow to Embrace New Chip-Card System*, WALL ST. J., Sept. 2, 2015 [hereinafter "Simon"], *available at* http://www.wsj.com/articles/small-businesses-are-slow-to-embrace-new-chip-card-system-1441239109.
[19] *Protecting Consumers: Financial Data Security in the Age of Computer Hackers: Hearing Before the House Comm. on Financial Services,* 114th Cong. (2015) (statement of the Hon. Tim Pawlenty, The Financial Services Roundtable), *available at* http://financialservices.house.gov/uploadedfiles/hhrg-114-ba00-wstate-tpawlenty-20150514.pdf.
[20] http://tsys.com/ngenuity-journal/will-losses-in-consumer-confidence-in-payments-accelerate-emv.cfm.
[21] http://www.forbes.com/sites/centurylink/2014/05/29/retail-it-gets-ready-for-chip-and-pin-tech-2/.
[22] *Id.*
[23] *Protecting Consumers: Financial Data Security in the Age of Computer Hackers: Hearing Before the House Comm. on Financial Services,* 114th Cong. (2015) (statement of Brian A. Dodge, Executive Vice President, Communications and Strategic Initiatives, Retail Industry Leaders Association), *available at* http://financialservices.house.gov/uploadedfiles/hhrg-114-ba00-wstate-bdodge-20150514.pdf.

not stop there."[24] There is agreement among some industry analysts that EMV technology may not strengthen a merchant's security and general reluctance by retailers to switch indicates widespread adoption of EMV in the United States may not occur until 2020.[25] Data security analysts also observe that chip-and-pin enabled terminals, alone, would not have prevented cyber criminals from obtaining customers' card information during the December 2013 Target breach and that end-to-end encryption of card data is necessary to prevent online transactions with the stolen data.[26]

Furthermore, there is anxiety over the potential impact that EMV technology will have on business to consumer interactions.[27] Industry experts in favor of EMV concede that the transaction time may increase by several seconds[28] which can be problematic for small businesses that conduct a high volume of transactions. On the other hand, not all small businesses will be liable for counterfeit credit card transactions because card issuers do not always pass on liability for "high-volume, low risk transactions where merchants aim to keep lines moving, such as fast food and cups of coffee."[29]

## IV. Small Business and EMV

Surveys suggest that small businesses are the least prepared for the EMV migration. In July 2015, Wells Fargo found that of the 35 percent of small businesses that accept point-of-sale (POS) credit card payments, only about one-third of them had a system capable of accepting chip enabled cards.[30] In the same survey, nearly half of the businesses stated that they do not want to pay for the EMV terminal.[31]

Opponents of the EMV migration note that small businesses also will face heavier burdens in implementing the new technology. For example, merchants may have missed the deadline because their technology vendors offer services that are no longer in compliance with the new system.[32] There also is a concern that small businesses that have the new hardware installed may be slow to receive certification[33] due to certification providers being inundated with last-minute requests – a process that could take several months.[34]

---

[24] *The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System,* Federal Reserve Bank of Kansas City Conference, Kansas City, MO (2015) (statement of Governor Jerome H. Powell, Federal Reserve), *available at* http://www.federalreserve.gov/newsevents/speech/powell20150625a.htm.

[25] http://www.afponline.org/mbr/reg/res/reg_news/Fatal_Flaw__Why_Retailers_Aren_t_Rushing_to_Adopt_EMV.html.

[26] http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

[27] https://nrf.com/news/emv-ahead.

[28] http://gizmodo.com/the-gizmodo-guide-to-the-new-emv-chip-credit-card-payme-1734011799.

[29] Simon, *supra* note 18.

[30] WF Survey, *supra* note 1, at 32.

[31] *Id.*

[32] https://nrf.com/news/emv-ahead.

[33] The card accepting terminals will need to have the appropriate software on it in order to interface with the EMV cards. As with the hardware, this interface from the card to the terminal requires a certification and the interface from the card accepting terminal to the POS also will need to be updated to handle the new data elements presented in an EMV transaction. Further, the POS to gateway, switch or acquirer also will need to be updated to handle these data elements as they have simply not been required in the past. http://blog.verifone.com/a-four-step-guide-to-emv-for-merchants-part-ii/.

[34] https://nrf.com/news/emv-ahead.

Small businesses continue to be at risk of cyber attacks and data theft. Small businesses generally have fewer resources available to combat security threats, which make them an easy target for cyber criminals. In a recent survey, 77 percent of small businesses believe their company is safe from a cyber attack; however, 87 percent, the vast majority, do not have a formal written security policy in place, and 60 percent surveyed do not have a privacy policy in place to protect company information.[35]

## V. Policy Issues Concerning Implementation of EMV

The issues that pose the most serious hurdles to EMV migration have been addressed primarily through industry negotiation, although some challenges remain. Fraud reduction is the paramount issue regarding implementation of EMV technology. Policymakers face obstacles in assessing how effective the shift to EMV will be because there are insufficient recorded metrics for EMV signature verification in the United States market – as mentioned previously, the existing use of EMV technology, in markets like the EU, employs chip-and-pin verification, not chip-and-signature verification.

## VI. Conclusion

The implementation of EMV chip technology offers small businesses some level of protection from fraudulent activity and data theft. Small businesses that fail to adopt the new payment system may put themselves at even greater risk "as fraud will migrate to the weakest technology (magnetic stripe)."[36] However, many small businesses are generally unaware of the October 1, 2015 EMV deadline or the implications of the resulting liability shift and small businesses often do not have the resources that large merchants employ to convert to the new system. Strong outreach and awareness raising efforts are the first steps to ensuring small businesses are able to adopt EMV technology. However, industry analysts have reported that the technology shift is not a silver bullet; fraudulent charges with counterfeit cards at the POS fell by 56 percent after chip-enabled cards were introduced in the United Kingdom, while online fraud increased by 64 percent.[37]

---

[35] NATIONAL CYBER SECURITY ALLIANCE/SYMANTEC, SMALL BUSINESS STUDY 4 (2012), *available at* http://www.staysafeonline.org/stay-safe-online/resources/.

[36] https://www.chasepaymentech.com/faq_emv_chip_card_technology.html.

[37] JULIE CONROY, AITE GROUP, EMV: LESSONS LEARNED AND THE U.S. OUTLOOK (2014), *available at* http://www.mapacific.com/files/4282012/uploaded/Aite%20Report%20-%20EMV%20Lessons%20Learned%20and%20the%20U.S.%20Outlook.pdf.