What EMV Chip Card Adoption Means for US Nonprofits
# Table of Contents

01  *Introduction*

01  *The Upside of Chips*

02  *EMV Adoption Trends*

03  *Need-To-Know Fine Print*

04  *Best Practices for Nonprofits*

05  *Conclusion*
The United States is joining more than 130 other countries in the widespread adoption of EMV chip cards. Named for its original developers, Europay, MasterCard and Visa, EMV credit, debit and prepaid cards have a small computer chip that makes them exponentially harder to counterfeit. While these cards are but one piece of the fraud-prevention puzzle, the sophisticated technology is aimed at making data theft less appealing, reducing fraud significantly for card-present transactions. Ultimately, EMV is moving the country closer to dynamic data authentication and paving the way for more secure mobile transactions.

Introduction
The United States is joining more than 130 other countries in the widespread adoption of EMV chip cards. Named for its original developers, Europay, MasterCard and Visa, EMV credit, debit and prepaid cards have a small computer chip that makes them exponentially harder to counterfeit. While these cards are but one piece of the fraud-prevention puzzle, the sophisticated technology is aimed at making data theft less appealing, reducing fraud significantly for card-present transactions. Ultimately, EMV is moving the country closer to dynamic data authentication and paving the way for more secure mobile transactions.

The roadmap for EMV adoption has been years in the making, but this October 2015 marks a crucial milestone: Liability for fraudulent charges will shift to the card issuer when the customer uses a point-of-sale terminal for purchases in which a customer pays with an EMV chip card. Here’s what this shift means for nonprofits who are using physical POS terminals and how they can deploy best practices to guide them through the adoption phase and beyond.

The Upside of Chips
The U.S. currently leads the world in credit card fraud, and it’s the only country in which counterfeit-card fraud is growing. Counterfeit card fraud now represents 37% of card fraud losses in the U.S., according to research by the Aite Group. Total global payment-card fraud losses topped $11.3 billion in 2012, up nearly 15% from the prior year, the Nilson Report found. The U.S. accounted for 47% of that total, with card-issuers losing $3.4 billion and merchants losing another $1.9 billion. Those losses are staggering—but not entirely unavoidable.

1 http://usa.visa.com/personal/security/chip-technology/emv-chip.jsp
EMV cards hold the promise of drastically reducing card-present counterfeit fraud. Each card contains a computer microchip that securely stores the card data that’s historically resided on the card’s magnetic stripe. While data on the magnetic stripe is static—making it easy to copy, or “skim,” and duplicate into counterfeit cards—the data from the EMV card’s microchip is dynamic. The microchip produces a one-time use code for each transaction, called a cryptogram. Even if that data is stolen, it cannot be used to create counterfeit cards because the stolen cryptogram will have expired. This makes the data less valuable, leading data theft to become less enticing to criminals.

EMV Adoption Trends

There are approximately 2.4 billion EMV chip cards in circulation today, and nearly 37 million terminals active worldwide. Yet, the U.S. — a leader in so many technologies—trails the pack.

In many ways, it’s the U.S.’s relatively advanced digital infrastructure that’s now made it a laggard of EMV adoption. Other countries originally embraced the technology because they didn’t have the telecommunications infrastructure in place to support real-time network authorizations for each transaction. Instead, these markets developed a technology that could allow communication between the card and terminal to complete the necessary security checks. The microchip fit the bill, and so the EMV chip card was developed.

In fact, the U.S. is one of the last developed countries to adopt EMV. In Western Europe, 99.9% of point-of-sale terminals are EMV-enabled. In Asia Pacific, that figure is 71.7%, and in Canada, Latin America and the Caribbean, it’s 84.7%. Yet only 4.5% of payment card transactions occur via EMV chip in the U.S.

In the early 2000s, momentum began building among credit card issuers to move toward EMV chip cards. They were motivated in part by the consistent uptick in counterfeit card loss and by fears that the U.S. could gain increasing attention from more fraudsters as other markets migrate to the chip. Widespread adoption of EMV would also allow the U.S. to build the infrastructure necessary for ubiquitous mobile payments.

However, the 2013 Durbin Amendment put the brakes on much of EMV’s forward movement. The federal law had several provisions regulating the debit card industry, including a mandate that merchants be given a choice of at least two unaffiliated networks for routing debit card transactions. In July 2013, Judge Richard Leon of the District Court threw up another hurdle for the industry, writing in an opinion that the dual routing provision applied to signature-debit and PIN-debit transactions.

EMV’s future seemed to face massive uncertainty. Yet the high-profile Target data breach, which was made public in December 2013, helped propel the technology forward. While EMV cards wouldn’t have stopped the data from...
being stolen, they would have prevented the criminals from being able to make counterfeit cards or monetize the data theft. EMV became the focus of congressional hearings, and in January 2014, the U.S. Federal Court of Appeals struck down Judge Leon’s opinion, putting the EMV migration in the fast lane once again.

Many card issuers are now moving aggressively to get EMV chip-enabled cards on the market, and merchants are investing in POS hardware upgrades in advance of the deadline. It’s estimated that merchants will spend a total $6.75 billion to upgrade to EMV chip-enabled POS terminals.

Specifically, Visa’s new policy will be that the party at fault for an EMV transaction not occurring will be liable. As of Oct. 1, 2015, MasterCard’s new policy will be that merchants with at least 95% EMV transactions will be free from liability for fraud. American Express’s new policy will be that the party with the most secure form of EMV technology will hold the least liability. And Discover’s new policy will dictate that fraud liability will shift to benefit the party with the highest-security payment technology.

The average cost of an EMV-compliant POS terminal is $500. It’s important to note, however, that there are no industry requirements forcing merchants or nonprofits to purchase new terminals, mobile devices or POS systems that are EMV-enabled. And no fines will be leveraged for failure to purchase or operate one of these terminal types. Card issuers will continue to distribute cards with magnetic stripes on the back, and those stripes will continue to provide global interoperability with existing terminals.

It’s estimated that merchants will spend a total $6.75 billion to upgrade to EMV chip-enabled POS terminals.
The October 2015 shift is a major inflection point only around liability for card-present fraud, and some organizations may deem the risk of chargeback to be smaller than the cost of hardware upgrades.

**Best Practices for Nonprofits**

Nonprofits experience incredibly low rates of card-present fraud, the type of fraud that EMV targets most heavily. Typically, just 0.05% of charges for nonprofits are disputed as chargebacks, and less than 20% of those are due to fraud. For a nonprofit that handles 4,000 transactions per year, that means on average just two of those would be chargebacks.

"Most of our nonprofit customers do not have much in the way of chargebacks, so the liability shift will have a very small impact in our sector," stated Tom Epplett, COO and founder of iATS Payments, a leading payment processor for nonprofits.

Nonprofits that do upgrade to EMV chip terminals should configure them to support online options only and ultimately simplify ongoing EMV compliance. Likewise, nonprofits that choose to support PIN verification in addition to cardholder verification methods like signatures should make sure that the PIN entry devices are Payment Card Industry PIN Transaction Security compliant.

Whether or not a nonprofit chooses to embrace EMV, its leaders should be well aware that *fraudsters are expected to shift more of their criminal activity online in the face of EMV’s more rigorous security for card-present transactions. Online fraud-prevention tools are a must to curb this anticipated rise in Web-based fraud.*

When the United Kingdom rolled out EMV chip cards, it saw this exact shift in fraudster activity. Between 2008 and 2013, loss from counterfeit cards fell from £97 million to £43 million. But during that same period, card-not-present fraud rose from £183 million to £301 million. It’s a trend that’s happened in many markets following the widespread adoption of EMV for card-present transactions, and many card issuers have invested or plan to

---

5 [https://www.blackbaud.com/BBMS/FAQ#question27](https://www.blackbaud.com/BBMS/FAQ#question27)

invest in Card Not Present fraud – any instance of fraud using credit or debit card numbers in a non-face-to-face setting – mitigation technologies like transactional alerts, tokenization and risk-based authentication to help blunt the impact.

**Conclusion**

Moving the world’s largest card market to a new technology has already taken years, and it will likely be decades before the familiar magnetic stripe is phased out entirely. 2015 marks an important moment for EMV chip cards, as the shifted liability encourages more widespread adoption of these cards and the infrastructure to support them. Nonprofits looking to stay ahead of this curve would be wise to focus less on the implementation of EMV-enabled terminals and more on the security measures surrounding their Card Not Present transactions. More pertinent information can be found in iATS Payments’ “Credit Card Fraud Prevention in Nonprofits.”