Conduent Public Sector
Payment Services

CONDUENT

EMV Migration

What You Need to Know about the Technology, the Security Protection it Provides, and When to Implement

According to a 2016 TSYS study identifying consumer payment preferences, 40 percent of Americans prefer using credit cards, 35 percent prefer debit cards and 11 percent prefer cash[1]. With U.S. consumers eight times more likely to reach for plastic over cash, the ongoing migration to EMV chip technology impacts millions – card issuers, merchants and consumers alike. Since more and more government agencies and government benefit programs are implementing debit card programs, the EMV conversion is beginning to impact the public sector as well.

While EMV chip technology has long been the global standard for credit card and debit card payments, the US has only recently begun the process of embracing it. Still, enormous progress has been made nationwide migrating cards to EMV. The Strawhecker Group reports that 52 percent of merchants today are enabled to accept chip payments. But that number doesn't tell the whole story. While 63 percent of all cards in the market are chip cards, the type of cards converted is not at parity: 81 percent of credit cards are converted to chip, but only 46 percent of debit cards converted to chip, per Glenbrook Partners[2].

In this paper, we'll discuss the technology behind EMV and review some misconceptions about EMV security in terms of what is protected by EMV and what is not. We'll also share some insights into how to determine the best time for your program to implement EMV, depending on your unique circumstances.

What is EMV and why the migration now?

EMV stands for Europay, MasterCard and Visa, named after the three companies that created the standard. It is an open-standard set of specifications for smart card payments that includes requirements to ensure interoperability between payment cards and point of sale (POS) terminals.

The chip in an EMV chip card contains a microprocessor that supports functionality well beyond that of a traditional magnetic stripe card, including strong transaction security. When using an EMV-enabled card at an EMV-enabled terminal, the cardholder doesn't swipe the card as is done today for a magnetic stripe transaction. Instead, the card is inserted into a reader in the payment device. Some EMV cards are also available with contactless functionality, which enables the chip to be read over a short distance using radio-frequency identification (RFID) technology.

So why has the U.S. only recently begun a conversion that the rest of the world undertook years ago? One of the main reasons for the delay in the U.S. is the sheer volume of those impacted by the changeover. The U.S. has more banks, card issuers, merchants and consumers using payment cards than any other country, which equates to a massive and complicated coordination between numerous parties.

Additionally, adopting the new technology means card issuers must create and issue new cards to consumers and merchants must update payment terminals with both new hardware and software, all of which is expensive. EMV cards can cost upwards of one dollar more per card than traditional magnetic stripe-only cards. While the estimated cost of replacing the 15 million point-of-sale terminals with chip card compliant machines is $6.75 billion with an average cost of $500 - $1000 per terminal[3].

In 2011, after some very public data breaches impacting millions of cardholders nationwide, the payment networks (MasterCard, Visa, American Express and Discover) began to announce their roadmaps for EMV implementation in the United States. The announcements contained important fraud liability shift milestones to ensure incentives for both issuers and merchants to convert to EMV. The most impactful shift occurred in October 2015 when a fraudulent transaction at a point of sale location became the responsibility of the party that was least EMV-compliant. In October 2016, fraud shifted to the least-EMV compliant party for ATM transactions routing over the Mastercard Cirrus ATM network. For other networks, such as the Visa Plus ATM network, the fraud liability shift will take effect in October 2017.

The final fraud liability shift will take place in October 2020 for gas station owners running Automated Fuel Dispensers (AFDs). Originally given a deadline of October 2017, AFD owners have been granted a 3-year extension to implement EMV technology due to the cost and complexity of the changes required.To explain a little further, the October 2015 POS liability shift date meant that the least secure party – or the one not capable of performing an EMV transaction – would now be responsible for any counterfeit fraud occurring during the transaction. Prior to the shift, the POS counterfeit fraud was largely absorbed by the card issuer. This type of liability shift is adding incentives and motivation for merchants to update payment terminals to be EMV-compatible.

One thing to keep in mind as we consider the current state of transition in the market: magnetic stripe cards have been the standard for card payments for decades and, even with the introduction of EMV, the magnetic stripe is not fully going away. Cards issued with EMV technology also have magnetic stripe capabilities, so consumers still have the ability to pay via magnetic stripe if they encounter a payment terminal without EMV capability.

EMV security

A key difference between the use of the EMV chip and the magnetic stripe on the security front is EMV's use of dynamic data during a transaction. Each transaction carries a unique 'stamp' which prevents the transaction data itself from being fraudulently reused, even if the cardholder data in compromised.

Overall, EMV secures the payment transaction with enhanced functionality in three areas (see new comment):

1. Card authentication: The card itself is validated typically by the issuer during a payment transaction. Also, during the transaction, the chip creates unique transaction data, which means that any captured data during the transaction cannot be used to create counterfeit cards and execute new transactions.

2. Cardholder verification: This is the process by which the issuer verifies the person attempting the transaction is actually the person to whom the card was issued. In the US, cards typically support online PIN, signature, and no cardholder verification (which is typically used for low risk and low dollar transactions).

3. Transaction authorization: Similar to the authorization process used for magnetic-stripe only cards, issuers use issuer-defined rules to decision transactions. However, with EMV transactions, additional transaction data, including the transaction-specific cryptogram, is available. This enables the issuer to make more robust authorization and decline decisions on each transaction.

Through the use of advanced encryption, embedded card risk analysis capabilities, and online authentication, most of the traditional methods used to steal card data or to clone cards using magnetic stripe technology are ineffective, or at the very least, very difficult to accomplish.

Beyond EMV

It's important to note that EMV can't protect against all types of fraud. For example, a lost or stolen card where the PIN has been compromised can still be used by a criminal or fraudster to make a POS transaction. Additionally, card-not-present (CNP) transactions like those done online or by phone are not protected by EMV because the chip is not read in the transaction.

Fraud follows the path of least resistance. Much like a burglar bypasses the house with the locked gate and security system in favor of the one with the open window, criminals will always look for the easy money. EMV isn't a silver bullet to prevent fraud but rather one of an array of effective tools used in the fight. Protecting against fraud requires a multi-pronged approach with a combination of fraud prevention tools, data analytics, and expertise.

In our card programs, we apply analytics to uncover suspicious activity. The quick use of data produced by payment cards offers a powerful fraud-fighting weapon. There are new tools using advanced algorithms to monitor behaviors and patterns in real time that send alerts of suspicious behavior, based on preset parameters, directly to the fraud prevention team's desktops for follow up. Lengthy, overloaded reports have been replaced with streamlined on-screen dashboards that provide a cohesive view of activity for rapid response.

By analyzing data over time, or comparing active case information, the following fraud markers can be identified:

- Outlier Detection: finding merchants and recipients that stand out from their peers
- Network Analysis: finding merchants and cardholders that are connected to each other and highlighting networks with similar suspicious behavior
- Geospatial Analysis: finding cardholders that are traveling unusual distances or that are near centers of suspicious activity
- Temporal Analysis: finding merchants whose sales, adjustment or return volume has suddenly spiked when nothing else appears to have changed

Even with the right mix of technology, most agencies can't effectively tackle ongoing fraud mitigation on their own. The best defense is finding a technology partner who offers a full portfolio of tools, a highly developed analytics practice and a deep understanding of the intricacies of government benefits programs – like Conduent

Is it time to switch to EMV?

While millions of personal credit and debit cards have already been converted to EMV, government benefits prepaid cards are just beginning the conversion process. As with any technology, the path to full rollout takes time. State agencies – in partnership with their program managers - must do their due diligence to determine the best time for conversion. While a 2014 Executive Order signed by President Obama sped the adoption of EMV for federal benefits cards, no such mandate has yet been put in place for state programs.

One of the ways we at Conduent help our customers determine a timeframe for EMV migration is by tracking fraud losses on a monthly basis and evaluating the cost of EMV implementation in comparison to the potential counterfeit fraud savings. Due to the high cost of the EMV plastics (resulting from the embedded chip), conversion costs often times outweigh potential counterfeit fraud savings.

However, due to differing counterfeit fraud levels on each program, some programs are ready for conversion. In fact, we have issued more than 5.5 million EMV cards to Direct Express federal benefit program cardholders and are similarly leading the way at the state level. For the rest of our programs, we continue to monitor past fraud behavior and model future potential fraud to determine the optimal time for EMV conversion.

The future with EMV

EMV migration in the U.S. is occurring in stages, with merchants, banks, processors and others working toward a singular goal, but at their own speed. Card programs should not feel pressure to rush into migration, but should instead work closely with experts to build a conversion road map on a timeframe that makes sense based on their specific needs.

We're at the forefront of EMV migration. We've already converted several of our customer programs to EMV, and we're working with several others to determine optimal timelines. The decision on when to migrate is yours; when you determine the time is right, we can help make that transition quickly and with minimal risk.

EMV's security benefits are undeniably effective in the fight against counterfeit fraud. But no single tool can stop fraud completely. The true key to protecting against fraudsters is remaining vigilant and investing in the right combination of fraud prevention tools, data analytics and expertise to deflect the ever-evolving threats.

We monitor industry fraud trends and employ sophisticated real-time fraud tools to protect both EMV and magnetic stripe cardholders alike. Our philosophy is to leverage the best practices from a variety of sources with our fraud team bringing proven experience from the world's leading banks, card associations, law enforcement, and government programs to benefit our clients. Whatever technology and partner you choose, protecting the integrity of card transactions is absolutely essential.

For more information, visit Conduent.com
or reach out to us via e-mail at PublicServices@Conduent.com.

1TSYS 2016 Consumer Payments Study
2 http://www.uspaymentsforum.org/us-payments-forum-spring-2017-market-snapshot-merchant-emv-chip-adoption-clarifying-cnp-fraud-status-and-increasing-focus-on-transit-payments/
3 http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php

CONDUENT