THE U.S. GOVERNMENT SHIFT TO EMV PAYMENTS

VERIFONE’S GUIDE TO THE NEW WHITE HOUSE EMV MANDATE

The U.S. Government has embarked on a migration to the chip and PIN EMV payment standard. This guide explores why the White House mandated adoption of EMV chip cards and payment terminals and how to fulfill the new requirements.
EXECUTIVE SUMMARY

By January 2015, U.S. government agencies -- mandated by presidential executive order -- must begin the shift to the chip and PIN EMV payment card standard that offers more secure authentication options to prevent card fraud.

The data encoded on payment card mag-stripes is an increasingly easy target for criminals who seek to clone the information to perpetuate payment fraud. The U.S. is the last G20 country to migrate away from this vulnerable technology. It’s estimated that in 2013, the U.S. accounted for 51% of the total worldwide card fraud.

Government executive departments and agencies must as soon as possible “transition payment processing terminals and credit, debit, and other payment cards to employ enhanced security features, including chip and PIN technology.” The effort parallels - and seeks to encourage - a commercial industry shift toward card payment technology based on EMV (an acronym for the three original participants -- Europay, MasterCard and Visa -- behind the effort).

Government issued EMV cards embedded with integrated circuits (“chips”) will interact with EMV payment terminals to ensure more secure verification and authentication in the payment process. EMV chip-based cards store encrypted data for authentication and can dynamically interact with a payment terminal. An EMV terminal reads data stored on the chip card for transactions and authenticates that it is legitimate, thus preventing use of stolen or cloned cards.

As agencies and other governmental entities move to comply with the mandate, they will need to evaluate, select and begin implementation of newer, more secure payment technology. EMV migration in the U.S. does not have to be costly and difficult -- EMV card-acceptance devices are readily available -- and government agencies may be intrigued by the additional benefits of implementing consumer-facing EMV devices that can deliver information, digital media, and create a deeper relationship with consumers.

EMV makes it exceedingly difficult to counterfeit payment cards but will not eliminate card fraud. Rather, it should be viewed as part of an overall security portfolio for protecting all aspect of card transactions and the payment infrastructure.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>2</td>
</tr>
<tr>
<td>WHY THE U.S. GOVERNMENT IS EMBRACING EMV</td>
<td>4</td>
</tr>
<tr>
<td>WHAT IS DRIVING THE EMV MIGRATION</td>
<td>8</td>
</tr>
<tr>
<td>BENEFITS OF EMV</td>
<td>13</td>
</tr>
<tr>
<td>GOVERNMENT REQUIREMENTS AND DEADLINES</td>
<td>16</td>
</tr>
<tr>
<td>DEVELOPING EMV SOLUTIONS FOR</td>
<td></td>
</tr>
<tr>
<td>GOVERNMENT AGENCIES</td>
<td>17</td>
</tr>
<tr>
<td>ENCRYPTION AND EMV</td>
<td>20</td>
</tr>
<tr>
<td>NEXT STEPS</td>
<td>21</td>
</tr>
<tr>
<td>RESOURCES</td>
<td>22</td>
</tr>
<tr>
<td>GLOSSARY</td>
<td>23</td>
</tr>
</tbody>
</table>
WHY THE U.S. GOVERNMENT IS EMBRACING EMV

The magnetic stripe was mandated for bank cards in the U.S. in 1980 and has been the essential element in electronic payment transactions ever since. But the data encoded on those mag-stripes is an increasingly easy target for criminals who seek to clone the information to perpetuate payment fraud. The U.S. is the last G20 country to migrate from mag-stripe payment cards to EMV (an acronym for the three original participants -- Europay, MasterCard and Visa -- that founded the organization behind the development of that standard). In October 2014, President Barack Obama issues an executive order directing U.S. government agencies to join that migration process by January 1, 2015.

The president’s order requires executive departments and agencies as soon as possible to “transition payment processing terminals and credit, debit, and other payment cards to employ enhanced security features, including chip and PIN technology.”¹

This will result in a shift to government issued cards embedded with integrated circuits (“chips”) that can interact with payment terminals to ensure more secure verification and authentication in the payment process. In addition, all newly acquired payment terminals will have to support chip and PIN transactions.

Older mag-stripe card technology is susceptible to crime in ways as simple as running a card through a hand-held “skimming” device, to sophisticated cybercrime network penetration schemes. Skimmers can be affixed to ATMs, gas pump card readers and older point-of-sale terminals to record magnetic card data, sometimes even employing a video camera to capture the PIN (personal information number) - but these devices typically collect information on tens or even hundreds of card accounts before they are detected. Network breaches, however, can result in theft of information pertaining to multiple millions of accounts, as has been the case in recent years with major retailers and a payment processor.²

In 2013, payment card fraud in the U.S. increased by 29% to $7.1 billion, according to the Business Intelligence research service, which found that the U.S. accounts for 51% of the total worldwide card fraud.

In 2013, payment card fraud in the U.S. increased by 29% to $7.1 billion, according to the Business Intelligence research service, which found that the U.S. accounts for 51% of the total worldwide card fraud.³

Chip and PIN has been widely implemented in other countries through adoption of the EMV payment standard that utilizes chip card technology. After Canada implemented chip and PIN nationwide in 2008, losses due to card skimming fell from CAD$142 million in 2009 to CAD$38.5 million in 2012.⁴ The European Central Bank (ECB) reported that countries in Europe’s Single Euro Payments Area (SEPA) experienced a drop of 24% in the amount of fraud at the point-of-sale between 2007 and 2011⁵, largely as a result of EMV adoption.

President Obama’s directive -- part of a broader, BuySecure Initiative -- requires action by January 1, 2015, aimed at beginning the U.S. government’s shift to EMV card technology. By that date, chip and PIN cards will become the standard for Federal Government programs like SmartPay and Direct Express with the goal of issuing 1 million cards within the calendar year. Also by that date, agencies will be required to purchase only chip and PIN-capable payment terminals.

The White House action parallels - and seeks to encourage - a commercial industry shift toward EMV card technology. “The goal is not just to ensure the

security of doing retail business with the government, but also, through this increased demand, to help drive the market towards swifter adoption of stronger security standards,” according to a White House fact sheet.

As part of the BuySecure Initiative, the White House announced that Home Depot, Target, Walgreens, and Wal-Mart will be rolling out secure chip and PIN-compatible card terminals in all their stores — most by January 2015. American Express will initiate a program to support small businesses upgrading point-of-sale terminals and Visa will launch a new program to educate consumers and merchants.

The major U.S. payment networks -- Visa, MasterCard, American Express and Discover -- have each implemented guidelines and roadmaps intended to steer card payment issuers, processors and merchants to adoption of EMV card transactions.

In August 2011, Visa announced a major U.S. payment infrastructure initiative that included a liability shift regarding who bears the cost of fraud. “With this type of liability shift,” Visa noted, “the party that is the cause of a chip-on-chip transaction not occurring (i.e., either the issuer or the merchant’s acquirer) will be financially liable for any resulting card-present counterfeit fraud losses.”

Subsequently, MasterCard announced its roadmap and incentives for EMV adoption, followed by Discover -- which disclosed in 2013 that it had already accepted EMV in the U.S. at certain Wal-Mart locations -- and American Express.

“When the liability shift happens, what will change is that if there is an incidence of card fraud, whichever party has the lesser technology will bear the liability,” Carolyn Balfany, group head, U.S. Product Delivery for MasterCard Worldwide, told the Wall Street Journal. “So if a merchant is still using the old system, they can still run a transaction with a swipe and a signature. But they will be liable for any fraudulent transactions if the customer has [used] a chip card. And the same goes the other way -- if the merchant has a new terminal, but the bank hasn’t issued a chip and PIN card to the customer, the bank would be liable.”

Each card brand has adopted a “carrot and stick” approach to steer acquirers and merchants toward EMV compliance. After October 2015, the liability will fall on essentially the weakest link in the payments chain, creating incentive to adopt EMV, rather than absorb new fraud costs.

State and local governments, while not impacted by the BuySecure Initiative deadlines, need to be cognizant of the liability shift impact. A Federal Reserve report several years ago pointed out that, “The U.S. General Services Administration’s SmartPay program is the world’s largest commercial card portfolio. Nearly every state uses payment cards to electronically distribute unemployment insurance, child support, Temporary Assistance to Need Families, or other funds. Federal, state, and local governments, as well as universities and other public-sector organizations, accept payments made with debit, credit, and prepaid cards.”

---

WHAT IS DRIVING THE EMV MIGRATION

EMV was initiated to provide a worldwide standard for interaction between integrated microprocessor “smart cards” -- also known as chip cards -- and approved payment devices and ATMs. This standard encompasses credit, debit and contactless payment transactions.

Adoption 2013

By the end of 2013, EMV payment cards in circulation totaled 2.37 billion and 36.9 million EMV terminals were active worldwide, according to EMVCo, an organization overseen by American Express, Discover, JCB, MasterCard, UnionPay, and Visa to manage and evolve the EMV specification. Excluding the U.S., EMV acceptance device adoption is estimated at more than 70%.

General-purpose credit cards date back to 1966 when Bank of America franchised the BankAmericard brand (now known as Visa) to other banks and the InterBank Card Association (now known as MasterCard) was formed by another group of credit-issuing banks. As cards became widespread in the 1970’s, merchants utilized so-called “knucklebuster” devices to imprint the embossed card information onto charge slips, and merchants could either telephone a verification service or check numbers against a printed booklet of invalid account numbers. In an effort to reduce transaction processing costs and losses due to fraud, MasterCard and Visa in 1981 began an effort to shift merchants toward electronic card readers that could verify sufficient credit and authorize payment by transmitting information via telephone networks.

---

With mag-stripe cards, static cardholder data is encoded on the magnetic stripe on the back of the card using technology first developed by IBM in the 1960s and the only way to change that data is to issue a new card. When the card is swiped, all of the cardholder data, such as the account number, name, and expiration date, is sent in one direction from the payment terminal to the authorization network, which checks the information, authorizes the charge and provides a payment guarantee to the merchant. The data from a mag-stripe card can be easily copied using a skimmer, or from networks and servers, and applied to blank mag-stripe cards that can be used for fraudulent purchases.

The U.S. card industry’s development of a real-time verification and authentication system relied on ubiquitous and relatively low-cost access to a nationwide telephone network. In Europe, where telephone usage was less reliable and more costly, European banks were going in a different direction. Leading banks opted for a microprocessor-based card that not only could store information, but which also allowed for information to be modified or removed.

The smart-card approach enabled POS devices to verify card information whether the POS card acceptance device was connected to a telephone network (“online”) or operating standalone (“offline”). With EMV cards, “authentication can take place online with the issuer authenticating the transaction using a dynamic cryptogram, offline with the card and terminal performing static or dynamic data authentication, or both,” according to a Smart Card Alliance explanation.

Payment authentication, the Smart Card Alliance explains, can also be handled in online or offline manner: “For an online authorization, transaction information is sent to the issuer, along with a transaction-specific cryptogram, and the issuer either authorizes or declines the transaction in real time. In an offline EMV transaction, the card and terminal communicate and use issuer-defined risk parameters that are set in the card to determine whether the transaction can be authorized.”

EMV chip-based cards store encrypted data for authentication and can dynamically interact with a payment terminal. During the transaction authorization process, authorization request and response cryptograms can be exchanged between the card and either the POS acceptance device or a network host to verify authenticity.

In an offline verification and authorization process, MasterCard explains, “If your chip card supports offline acceptance, the terminal can determine if the card is genuine, the cardholder can be verified as the authorized user, and the

---

12 EMV FAQ, Smart Card Alliance.
transaction can be completed without having to connect to the issuer host system.\footnote{13}{“Offline Acceptance Support.” MasterCard website.}

For general payment applications, an EMV terminal reads data stored on the chip card for transactions and authenticates that it is legitimate, thus preventing use of stolen or cloned cards. In general, most EMV implementations have utilized chip and PIN, which relies on cardholders entering their personal identification numbers at the point-of-sale to authenticate them as the legitimate holders of the cards.

Unlike mag-stripe cards that are swiped though a reader, EMV cards are inserted (or “dipped”) into a slot so that an EMV card acceptance reader can make contact and interact with the chip on the card. “Card authentication can take place online with the issuer authenticating the transaction using a dynamic cryptogram, offline with the card and terminal performing static or dynamic data authentication, or both,” according to the Smart Card Alliance.

There have been previous efforts to move the U.S. toward EMV adoption voluntarily in the past decade, but with little success. In other countries, strong, centralized authorities or dominant card issuers have taken the initiative and enforced adoption of EMV. In the U.S., however, the industry operates under relatively loose regulation and must accommodate the often-contradictory interests of multiple influencers and consumers:

- Card networks, such as Visa and MasterCard.
- Card issuers ranging from national giants such as Bank America and Wells Fargo to regional and local banks.
- Acquiring banks and financial institutions (“acquirers”) that process (or “acquire”) card payments on behalf of merchants.
- The merchants themselves.

Card issuers were reluctant to replace relatively cheap mag-stripe cards with more expensive chip cards, particularly as there were few devices in stores where they could be used in that manner. Merchants, often operating on thin profit margins, were equally reluctant to invest more aggressively in new payment devices and disrupt ongoing operations without any incentive or perceived benefit to doing so.

There was very little agreement among industry stakeholders that there was a business case for EMV adoption, noted a Federal Reserve working paper.
published in 2012.  

But the tide was already turning as a result of growing consumer unease with card fraud and identity theft combined with highly publicized network breaches that compromised hundreds of millions of cards. Retailer TJ Maxx disclosed in 2007 a breach that compromised potentially 100 million card accounts, followed by disclosure of a 2008 network breach at card processor Heartland Payment Systems, Inc., that impacted an even greater number.

With network breach incidents mounting and legislators questioning the integrity of the payment system, the card networks acted to force the initiative, beginning with Visa’s 2011 announcement that it would enforce a liability shift. Since that point, millions of EMV-capable terminals have been shipped into the field.

Verifone CEO Paul Gallant noted in mid 2014 that more than 80% of the Verifone products shipped in the company’s Fiscal Year 2014 second quarter were EMV-capable.

Today’s EMV acceptance devices are more likely than not able to accommodate more than just chip and PIN transactions. The card networks are offering incentive to retailers that deploy “dual interface” devices that in addition to chip and PIN will accept wireless EMV transactions utilizing Near Field Communications (NFC), which can be implemented on contactless EMV cards, fobs and other devices, and increasingly is being integrated within mobile phones and other mobile devices.

Chip and PIN is not the only verification method that falls within the EMV specification. Some countries have opted for a “Chip and Signature” approach, which Visa has indicated will be one of several Card Verification Methods (CVM), which include “signature, online PIN and no card holder verification for low-value, low-risk transactions.” Chip and Signature is a controversial issue with some larger retailers: The Merchant Advisory Group, which includes Wal-Mart, Target, Sears, CVS Caremark and many others, has strongly endorsed chip and PIN as a requirement, rather than an option, for U.S. EMV adoption.

---

No one should be under the illusion that EMV adoption will eliminate card fraud. New EMV cards issued by banks will almost certainly all incorporate a mag stripe to ensure their cardholders can make purchases at non-EMV devices. It will likely be several years before U.S. issuers no longer provide mag-stripes on their cards.

EMV does nothing to stop network compromises or the placement of malware. What EMV does do is authenticate that the card being presented at the point-of-sale is not counterfeit and with a PIN, it can verify that the person presenting the card for payment is the legitimate account holder.

While EMV encrypts the PIN during the transaction process between the terminal and card, there is no requirement for encrypting the transmission of the transaction data itself. Unless a merchant and processor adopt end-to-end, or point-to-point, encryption, cybercriminals may still be able to intercept large volumes of EMV cardholder data. Nonetheless, as EMV terminals and cards become prevalent, it will become increasingly difficult to counterfeit cards.
BENEFITS OF EMV

Security is essential to management of government systems. Maintaining availability and ensuring integrity of government information are vital to the ongoing operations of government and its interactions with citizens, businesses and foreign entities. The migration to EMV provides the government additional capabilities to better protect citizens doing business with the government, executive departments and agencies.

The government functions both as a card issuer (providing, through contracted third parties, payment cards for government employees and beneficiaries) and as a merchant (accepting payment card transactions).

In 2010, total card receipts for all U.S. government entities, excluding the Internal Revenue Service, were $9 billion\(^\text{18}\) and since then the government has rolled out additional programs enabling payment of obligations by credit and debit card. In addition, the General Services Administration SmartPay program encompasses $26.4 billion annually through 87.4 million transactions by U.S. agencies and organizations utilizing over three million purchase and travel cards.

Over the past decade, consumers have significantly shifted away from cash payments to credit and debit. In 2012, two-thirds of noncash payments made in the United States were made by card, compared with only one-third of noncash payments by card in 2000," according to the Federal Reserve 2013 payments study.\(^\text{19}\) In that year there were more than 775 million general purpose credit, debit and prepaid cards in force, which were used for 41.4 billion card-present debit card payments, 18 billion credit card payments and 2.7 billion prepaid card payments.


All of those cards and transactions generate huge volumes of data that cybercriminals are increasingly seeking to scoop up for fraudulent purposes. In 2012, according to the Federal Reserve, general-purpose cards accounted for 92% of unauthorized transactions identified as third-party fraud and 63% of the value of those transactions.

As WIRED magazine noted, “What happens to stolen bank card data hasn’t changed in 15 years—the hackers package it and sell it in bulk to the underground’s third-party resellers…Once it’s in an underground shop, card counterfeiters buy the mag-stripes they need—sometimes ordering by bank or ZIP code—and copy it onto fake cards using their own mag-stripe encoding machines. Then they use the cards to buy goods they can resell or dispatch crews to do the shopping for them in exchange for a cut of the profits.”

EMV provides strong defenses to prevent the counterfeiting of cards. Mag-stripe cards contain static data, so counterfeit (or “cloned”) versions can be used until card networks’ and processor systems are updated with information that the stolen card information is no longer valid.

With EMV, however, payment cards have multiple layers of security to prevent misuse. Card issuers store encrypted keys to identify a card as legitimate and encrypted PINs can be used to verify the person presenting the card is the legitimate account holder. Finally, because each individual transaction utilizes dynamic data that essentially creates a unique ‘stamp’ it is impossible to steal that data and use it for fraudulent transactions.

The U.S. government’s adoption of EMV goes hand-in-hand with its efforts to enforce agency compliance with the Payment Card Industry Data Security Standard (PCI DSS). The Treasury Departments Card Acquiring Service advises federal entities that, “Failure to maintain compliance with the PCI DSS puts your organization at risk of significant fines, fees, penalties or losing the ability to process card payments, as may be prescribed by the applicable card associations.” Similarly, agencies need to be cognizant of the impact that the EMV liability shift will have on their payment acceptance operations.

President Obama’s order on chip and PIN adoption was positioned as “leading by example” in the effort to transition the U.S. to a more secure card payments
environment. With its clout as both issuer and merchant, the government’s increased demand for EMV cards and terminals is expected to “help drive the market toward swifter adoption of stronger security standards.”
GOVERNMENT REQUIREMENTS AND DEADLINES

The Federal Government’s BuySecure Initiative requires executive departments and agencies to transition as soon as possible to payment processing terminals and credit, debit, and other payment cards that employ enhanced security features, including chip and PIN technology. Specific deadlines include:

- No later than January 1, 2015, all new payment processing terminals acquired through the Department of the Treasury or through alternative means authorized by the Department of the Treasury shall include hardware necessary to support enhanced security features.

- The Department of the Treasury shall by January 1, 2015, develop a plan for agencies to install enabling software that supports enhanced security features.

- By January 1, 2015, begin replacement of credit, debit, and other payment cards provided through General Services Administration (GSA) contracts.

- By January 1, 2015, other agencies with credit, debit, and other payment card programs must provide plans to ensure their payment cards have enhanced security features.
DEVELOPING EMV SOLUTIONS FOR GOVERNMENT AGENCIES

The U.S. Government’s BuySecure Initiative represents an effort to get out ahead of a broad U.S. payments industry shift to EMV-compliant payments. The major card networks --Visa, MasterCard, American Express and Discover - have each adopted a “carrot and stick” approach to steer card acceptance entities toward EMV adoption.

Each card network is providing some incentives for achieving particular adoption milestones. But it is the potential penalties embodied in the “fraud liability shift” that are likely to be the primary motivator.

After October 2015 (October 2017 for fuel dispensers), the liability for cost incurred due to counterfeit fraud that could have been prevented through use of EMV will shift to essentially the weakest link in the payments chain. To this point, card networks have offered up only general comments regarding how the guidelines will be implemented:

**Visa** -- “To spur adoption of the new technology, starting in 2015 our guidelines will place financial responsibility for counterfeit fraud on the party (either the financial institution or the retailer) that hasn’t adopted the chip.”

**MasterCard** -- “The party that has made investment in the most secure EMV options is protected from financial liability for card-present fraud losses for both counterfeit and lost, stolen and non-receipt fraud on this date.”

**American Express** -- “Will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology.”

**Discover** -- “Fraud Liability Shift policy will be a risk-based payments hierarchy that benefits the entity that leverages the highest level of available payments security.”

---

The liability shift date is actually the culmination of a lengthy process, which began in 2011, to enable the payment industry to process EMV payments. As of April 2013, “acquirers, service providers and sub-processors” were required to have “the capability to process any EMV point-of-sale (POS) transaction,” both contact and contactless,” according to a MasterCard Advisors report.\(^{24}\)

In addition to meeting network approvals and completing testing procedures, acquirers also needed to be able to identify terminals with the appropriate EMVCo approvals and confirm that payment network-specific application logic is loaded onto the terminals, the MasterCard Advisors report noted.

EMVCo has developed specifications required of processing hosts, cards, terminals, and mobile payment. The organization defines two levels of “Terminal Type Approval” and certification aimed at providing confidence in the achievement of interoperability and consistent behavior between compliant applications:

**Level 1 Type Approval** applies to hardware aspects and “tests compliance with the electromechanical characteristics, logical interface, and transmission protocol requirements defined in the EMV Specifications.”\(^{25}\)

**Level 2 Type Approval** applies to software that runs on the terminal and tests “compliance with the debit/credit application requirements as defined in the EMV Specifications.”

With NFC increasingly being integrated into mobile phones (such as Google Wallet on Android-based devices and Apple Pay on new iPhone 6 generation devices), NFC payment acceptance capability now becomes the default option.

Mobile payment has been inextricably linked to EMV acceptance by the major card brands, all of whom have stated that they require card acceptance devices to be dual-interface (or hybrid) systems that both accept EMV card insertion as well as NFC-based mobile payments transactions. With NFC increasingly being integrated into mobile phones (such as Google Wallet on Android-based devices and Apple Pay on new iPhone 6 generation devices), NFC payment acceptance capability now becomes the default option, rather than a decision on whether or not to invest in new technology.

EMV migration in the U.S. does not have to be costly and difficult. EMV card-acceptance devices are readily available -- as a global supplier, Verifone, for

---


\(^{25}\) “Approvals & Certifications,” EMVCo website.
example, has been selling EMV-capable solutions in overseas markets for many years and is well versed in EMVCo certification processes. Additionally, EMV-capable PIN pads may in some cases enable adaptation of some older non-EMV systems to the new payment requirements.

Agencies may be intrigued by the additional benefits of implementing consumer-facing EMV devices. Payment technology today is increasingly interactive, providing new opportunities to engage with the consumer to deliver information, digital media, and to create a deeper relationship.
ENCRIPTION AND EMV

Agencies accepting payment cards can use a comprehensive, multi-layered approach to transaction security to make a less appealing target to criminals.

While EMV limits the exposure of merchant payment transactions to fraud and misuse, it does not protect cardholder information that under EMV is still transmitted in the clear during the transaction. EMV should be viewed as part of an overall security portfolio for protecting all aspect of card transactions.

Many payment processors and retailers are moving to adopt sophisticated encryption and tokenization to secure cardholder information, from insertion of the card, to the processing host, and back to the point-of-sale device. The most secure payment transaction possible today is one that combines three technologies: EMV, data encryption and tokenization.

Data-level encryption, applied as close to the point of entry or capture as possible, almost completely eliminates access points where unencrypted card data could be intercepted. This is also called end-to-end or point-to-point encryption because data are encrypted at the point of capture, and remain encrypted until reaching the party that holds the decryption key, typically the merchant’s processor. If at any point along the way, the encrypted data are stolen, the data will be useless to criminals in their encrypted form.

Tokenization provides another barrier to cyber thieves. Tokenization replaces cardholder account numbers with a valueless substitute -- a digital token. Tokenization reduces security risks in the event of data breaches because it eliminates sensitive cardholder data from the agency’s environment after transactions have been authorized. If the token numbers are stolen, they are meaningless to thieves because outside of the correlation database, they are simply collections of random numbers. But they allow the processor or agency to conduct necessary back-end processes ranging from chargebacks to analytics.

The most secure payment transaction possible today is one that combines three technologies: EMV, data encryption and tokenization.
NEXT STEPS

The complexity of migrating to EMV chip-card standards can pose significant challenges for acquirers and agencies that accept card payments. Government agencies and integrators should look for a trusted partner with expertise in both U.S. payments implementation and worldwide EMV implementations.

EMV is a global standard and Verifone has global experience in developing EMV payment system solutions and peripherals that have achieved EMV Level 1 and Level 2 Type Approval. Since the inception of EMV, Verifone has provided internationally an unmatched line of EMV-compliant hardware and software— as well as training and support—to deliver complete solutions for meeting EMV requirements.

In recent years, Verifone has incorporated EMV and NFC capabilities into standard product offerings in the U.S. The company works with more than 100 authorized business partners strategically located around the world works closely with those partners to availability of EMV-compliant hardware and software, as well as training and support, to deliver complete solutions for meeting migration plans.

Most importantly, while EMV limits the exposure of payment transactions to fraud and misuse, cardholder information is still transmitted in the clear during an EMV transaction. Verifone provides sophisticated encryption and tokenization solutions to fully secure cardholder information, from insertion to processing and back.

Verifone draws upon over 30 years of worldwide experience in payments, product development and support teams that have experience working on thousands of EMV migrations and implementations. With a broad portfolio of secure transaction enabled and payment acceptance solutions for government entities, Verifone is able to provide agencies and integrators with the technology, expertise and services needed to ensure a smooth migration to EMV.

Verifone’s worldwide workforce represents years of experience helping thousands of partners and customers in implementing EMV. A wealth of resources from webinars and training to EMV devices and software solutions provide everything needed to plan EMV migration and avoid potentially significant risks. To learn more about how to implement the White House mandated migration to EMV, utilizes the resources below, contact a Verifone representative, or visit www.verifone.com/emv-us.
## RESOURCES

- EMV Key Incentive Dates
- EMVCo.com
- EMV Solutions
- White Paper: EMV Gathers Steam as U.S. Moves Toward Liability Shift
- EMV Transformation eBook: A Brand New Checkout Experience
- White Paper: Multi-layered Security Strengthens Payment Structures
- That's EMV website
- EMV Migration Forum Knowledge Center
- Verifone’s Guide to the White House
GLOSSARY

**Acquirer** (acquiring bank) – A bank or other financial institution that signs up merchants to accept payment cards and acquire payments from card issuers. Provides or arranges for payment processing services to manage the authorization and payment flows.

**Authorization Response Cryptogram** (ARPC) – An encrypted value generated by a card issuer during an online transaction in response to an authorization requested.

**Authorization Request Cryptogram** (ARQC) – An encrypted value generated by a card to request online authorization of a transaction.

**Cardholder Verification Method** (CVM) – A means of verifying that the person using a card is the authorized account holder. Could be a signature, an online PIN or an offline PIN.

**Chip Card** - A payment card with an embedded processor on which data can be dynamically changed.

**Cloning** - The process of using copied card data to make a duplicate or counterfeit card that can be used for fraudulent purposes.

**Dynamic Data Authentication** - The process by which an encryption key stored on an EMV card creates a unique identification number for each transaction that cannot be reused.

**EMV** - An acronym derived from the three companies (Europay International, MasterCard International and Visa International) that formed EMVCo to manage and enhance the EMV payment standard. Current members of EMVCo are American Express, JCB, Discover, MasterCard, UnionPay and Visa.

**Issuer** (card issuer) - A bank or financial institution that provides general-purpose credit, debit and prepaid cards and is the source of funds for merchants accepting cards issued by that organization.

**Mag-stripe** (magnetic stripe, magstrip) - The magnetic stripe that adorns traditional credit and other payment cards and which stores information including Primary Account Number (PAN), account holder name, expiration data and other information.

**PCI** - Acronym for Payment Card Industry, which encompasses the Payment Card Industry Security Standards Council, the its specifications including the PCI Data Security Standard (PCI DSS).
PIN - Personal Identification Number.

Processor - Organization that handles routing, authorization, payment and information flows between the merchant and the card network.

Skimming - Copying a mag-stripe data by using a handheld device or embedding a device into a card reader.

Smart Card - Cards with embedded processors that can be used for financial and other applications. Not necessarily EMV cards.

Static Data Authentication - Encrypted data stored on a chip card that verifies the card was legitimately issued.

Track Data - Data embedded on mag-stripe cards to provide information necessary to authorize a payment transaction, such as PAN, expiration date, etc.

Terminal Type Approval - A process established by EMVCo for testing compliance with EMV specifications.