EMV: A Merchant’s Primer

October 1, 2015 marked a major milestone in the US payments landscape, when liability for fraudulent counterfeit credit and debit card transactions shifted from issuers to merchants, unless those merchants migrate to POS technology that accommodates the EMV (Europay/Mastercard/Visa) standard. In this primer, we take a look at what EMV is, what the liability shift is meant to accomplish, how migration will benefit merchants, and what consequences merchants should expect from failure to embrace EMV-compliant technology. We also dispel some of the myths surrounding EMV implementation, lay out the basic groundwork for EMV migration, and explore other technologies that should be implemented in conjunction with EMV as part of a comprehensive data security solution.

Who, What, Where & Why

EMV is an open-standard set of specifications for chip card payments and acceptance devices, developed to define requirements that ensure interoperability between POS terminals and chip-based payment cards. Chip-based payment cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magstripe cards. There are three types:

- **Contact**: Contact chip cards communicate with the card reader over a contact “plate” that must touch the terminal. Such contact is usually established by inserting the card into a slot in the terminal or ATM.

- **Contactless**: Contactless cards communicate via radio frequency (RF) technology. As such, they contain an antenna.

- **Dual-interface**: Dual-interface chip cards combine contact and contactless card technologies. They communicate with the card by touching its plate or in RF mode.

As for EMV specifications, these are managed, maintained and enhanced by EMVCo, which executes testing and other processes related to EMV. Such processes include, but are not limited to, card and terminal evaluation, security evaluation and the handling of interoperability issues. EMVCo’s work is overseen by six member organizations: American Express, Discover, JCB, Mastercard, UnionPay and Visa. Other payments industry stakeholders—including banks, merchants, processors and technology vendors—participate in EMVCo initiatives as technical and business associates. EMVCo is not responsible for individual card brand certifications.

EMV Benefits

**Decreases card fraud.**

An EMV-enabled card’s microprocessor chip stores information securely and carries security credentials that are encoded by the card issuer when the card is personalized for an individual cardholder using user-specific keys. The encoding of these credentials helps prevent fraudsters from creating counterfeit cards (“cloning”). Unlike magstripe cards, which are easy to duplicate because they lack the security features of microprocessor chips, EMV cards
cannot be duplicated or used to complete fraudulent transactions. In order to be successfully processed, EMV transactions require an authentic card, validated either online by the issuer using a dynamic cryptogram or offline with the terminal using static data authentication (SDA), dynamic data authentication (DDA) or combined DDA with application cryptogram generation (CDA). EMV transactions also create unique transaction data so that any captured data cannot be used to execute new transactions.

Additionally, EMV reduces fraud resulting from card theft and loss by harnessing enhanced transaction authorization, card authentication and cardholder verification.

- **Transaction authorization** uses issuer-defined rules to authorize transactions either online or offline. For an online authorization, EMV transactions proceed in the same manner as with magstripe cards: transaction information and a transaction-specific cryptogram are sent to the issuer, which authorizes or declines the transaction. Offline, the card and terminal communicate and use issuer-defined risk parameters to determine whether the transaction can be authorized. Offline transactions are typical in situations where terminals do not have internet connectivity or in countries where telecommunication costs are high.

- **Card authentication** occurs online via cryptographic processing, which validates the integrity of the card number and certain static and dynamic (live) data used in the transaction, or offline through SDA, DDA or a combination of DDA with CDA. Dynamic data is unique to each transaction, so it can’t be used more than once even if fraudsters manage to steal it. Any attempt to do so would cause that transaction to be declined.

- **Cardholder verification** ensures that the person attempting to make the transaction is the person to whom the card belongs. It is executed through one of four cardholder verification methods (CVMs) supported by EMV: offline chip and PIN, online chip and PIN, chip and signature, and no CVM (contactless). The choice of CVM depends on the merchant, acquirer, and issuer alike.

**Allows interoperability with the global payments infrastructure.**

Consumers with EMV-enabled cards can use them on any EMV-compatible payment terminal in the world. Such interoperability is likely to become increasingly important as some nations consider phasing out magstripe cards entirely.

**Additional EMV Benefits**

Meanwhile, although merchants aren’t required to follow an EMV migration path, significant benefits await those that do. By deploying EMV-compliant hardware and software, they can:

**Avoid major financial repercussions.**

This is the strongest argument for embracing EMV. Maintaining non-EMV-compliant POS technology leaves merchants responsible for potentially steep costs stemming from fraudulent transactions and chargebacks. As of
October 2012, Mastercard will exempt merchants from 100% of account data compromise penalties if at least 95% of Mastercard transactions that originate in their stores are handled on EMV-compliant POS terminals.

**PCI audit relief**

If more than 75% of merchant Visa and Mastercard transactions since October 1, 2012 originate from EMV-compliant POS terminals that support both contact and contactless transactions, the merchant may apply for relief from the audit requirement for PCI compliance (but is still required to be PCI-compliant).

**Build a future-proof payment acceptance infrastructure that supports new payment innovations and technologies**

NFC-enabled (near-field communications) mobile devices that are used to accept mobile contactless payments, as well as other mobile applications (like mobile couponing and loyalty programs), top the list of these options. EMVCo has been playing a key role in defining the architecture, specifications, requirements, and type approval processes for supporting EMV mobile contactless payments. This helped to facilitate the launch of NFC mobile contactless payments in Europe, where an EMV-based payments infrastructure is already in place. The same is likely to happen in the US.

**Take advantage of global interoperability to boost business**

Many US merchants want to attract to their establishments to visitors from countries where chip cards are the norm. Acquiring EMV-compliant hardware and software prevents merchants from losing business of foreign customers who favor the security afforded by chip cards and are reluctant or unwilling to revert to the use of the magstripe on their cards to process payments.

As of October 2015, card brands will hold “the party that is the cause of a chip card transaction not occurring” (i.e., a merchant whose terminals are not EMV-compliant) liable for any resulting card-present counterfeit fraud losses. Review card brand specifics by visiting their websites. Note: AFD and ATM dates vary.
Myth-busting

In addition to understanding the mechanics of EMV, it’s important to debunk some of the myths that surround it and may be preventing merchants from boarding the EMV train.

**Myth:** Despite the technological advances, EMV really isn’t a proven data security solution.

**Reality:** Statistics from abroad, as reported by EMVCo, demonstrate quite the opposite. In the United Kingdom, EMV was piloted from May to September 2003 in a program that involved 600 merchants and 180,000 chip cards. The pilot was successful; nationwide EMV rollout was initiated in 2004, and an EMV liability shift occurred one year later. Card fraud losses in the UK stood at $102.3M GBP in 2013—less than half of what they were ($274.1M) in 2004, according to the UK Cards Association. Since 2004, losses at UK retailers have fallen by 67%; mail non-receipt fraud has fallen by 91%; and lost and stolen card fraud fell by 58% from 2004–2009.

Canada’s move to EMV got underway in 2003, when Visa Canada said it would begin migrating its traditional magstripe-based cards to EMV chip cards by 2004. This announcement induced Interac, Canada’s largest payment body, to declare one year later that all magstripe credit and debit cards would be replaced with chip-based cards. In 2006, Mastercard Canada announced support for chip and PIN-based EMV cards. Pilots were conducted from 2007–2009, and liability shifts were introduced in 2010. While Canada’s deadline for conversion to EMV-ready POS technology was the end of 2015, Interac reported in mid-2014 that the nation had already seen marked debit card fraud reduction as a result of the ongoing transition to EMV. Losses plummeted from a high of $142M CAD in 2009 to a record low of $29.5M CAD in 2013. A mere $7.3M CAD of these resulted from fraud perpetrated against Canadian debit cardholders within Canada itself.

**Myth:** You can buy your way of out of assuming liability for fraudulent transactions once the shift has occurred.

**Reality:** Some merchants still think the liability shift is a mandate, and that they can earn exemption from that mandate by paying an annual fee. But no such option exists.

The simple truth is, unless they upgrade to EMV-compliant equipment, merchants are liable for card-present counterfeit fraud, resulting in significant financial repercussions. Losses can add up per incident, enough to severely cripple the average small- or medium-sized merchant and possibly even put it out of business, as well as make a sizeable dent in the finances of larger operations.

**Myth:** Only larger merchants need to move forward with EMV technology.

**Reality:** Fraudsters continue to remain a step ahead of merchants, processors, card networks and other entities when it comes to finding ways to perpetrate their crimes, including counterfeiting cards. They won’t stop hacking into merchants’ databases once larger players have migrated to EMV-compliant technology; rather, they will focus their attention on smaller merchants, unless those merchants, too, have made the shift.
EMV Handbook: One Year Later

**Myth:** Migrating to EMV-compliant technology is too expensive.

**Reality:** At first glance, the cost of acquiring technology that accommodates EMV transactions, as well as expenses incurred for training and other aspects of conversion, appear steep. Even with other costs factored in, however, the financial fallout from maintaining a non-EMV-compliant POS system will almost always trump the price of any necessary upgrades. And even if a merchant isn’t presently being hit with enough chargebacks from counterfeit cards to make migration seem worth the investment, a change could rapidly occur as soon as fraudsters start hitting their store. Should that occur, the initial cost of rolling out EMV-compliant hardware will seem infinitesimal compared to lost business from failure to upgrade a non-compliant system.

**Myth:** Consumers don’t really care about EMV, and they never will.

**Reality:** Consumer media is buzzing with stories about EMV and its promise of enhanced payment security. As more information is disseminated, and especially as they fast become accustomed to the slightly different procedure for paying with chip cards, consumers will perceive EMV as the most secure way to complete transactions in store. In addition, tourists from nations where EMV is already the payment norm may be reluctant to shop at US stores that do not have EMV-compliant equipment in place.
Laying the Groundwork

Consulting POS equipment vendors

Work with vendors like Verifone to determine chip acceptance needs, whether POS devices will be standalone or integrated, and how to change customer interaction and transactional procedures as the move to EMV is made.

We recommend opting for dual-interface chip readers that accommodate contact and contactless payments, as it is a requirement for merchants in order to take advantage of EMV incentives. The growing popularity of contactless payment models comprises one rationale for this recommendation, though there are others. Notably, to qualify for relief from PCI requirements and ADC relief, merchants must implement dual contact/contactless terminals.

What's more, while contact chip cards will never become obsolete, installing POS terminals that also accept contactless cards enables NFC payment acceptance, offering rapid checkout—a perk that's in increasingly high demand among busy consumers.

Making the right software selection

Find a solution that best fits your individual processing needs and is certified to work with your chosen payment terminal. In selecting software as well as hardware, it’s important to know that EMV payment technology must be certified by EMVCo. This is known as Level 1 and Level 2 certification. Each certification process is intended to ensure the security of the device but also guarantee interoperability between brands, CVMs and other aspects of EMV deployment. The certification rule also applies to apps that are designed to facilitate EMV adoption.

Be cognizant, too, of Level 3 certification. This is an end-to-end certification conducted with the solution between the merchant and the brand, with checks made by the processor, acquirer and any independent software vendor involved. Level 3 testing assesses the integrity of the payment chain by testing every type of possible transaction that the terminal can perform.

Merchants may not need to get involved with Level 3 testing. Those with EMV implementations involving single terminals and specific, pre-made software packages that are certified to handle EMV transactions without heavy customization probably fall into this category. Larger merchants that utilize customized processing setups may need to be more active on this front. Payment processors, acquirers and independent software vendors can provide advice as to whether merchants themselves must undertake any degree of Level 3 testing.

Implementing a comprehensive training program

Providing employees with proper training is critical to the success of any EMV implementation. Using a combination of hands-on instruction and printed materials (including quick-reference guides and FAQ lists) cover:

- How and when chip cards should be inserted into the card reader. Emphasize that in an EMV scenario, chip cards aren’t to be swiped and immediately removed from the card reader, as is the practice with magstripe
cards. Rather, they must be inserted into the terminal and removed when indicated by the terminal's screen—otherwise, the transaction will terminate prematurely.

- **How to assist customers at the end of their transactions.** When chip cards were first issued in Australia, merchants noted a high incidence of cards being left behind by consumers who had forgotten to remove them from the card reader. To prevent this, train employees to remind customers to take their cards once their payments have been processed, or configure the POS software not to print the receipt until the card is removed.

- **How to handle chip card and chip reader malfunctions.** In instances where one of these two components isn’t working and the card must be swiped, the terminal reads the service code and prompts it to read the card as a chip card. Personnel generally are allowed a few attempts at using the chip reader before the terminal prompts for a fallback read of the magstripe, if permitted by the issuer.

Educating consumers on how to complete EMV transactions is also a good idea, given how they differ from magstripe transactions. For best results:

- **Create signage.** Use signs to remind customers not to swipe their cards, to leave their cards in the terminal until it signals that the transaction is complete, and to take their cards with them afterward. Post these in prominent spots at the point of sale.

- **Harness websites and social media.** A website or Facebook page is the perfect vehicle for letting customers know that secure EMV payment is now available at a store or restaurant, and for providing a short explanation of how it works. Video clips are also available from gochip.com; links to these can be featured on merchants’ websites and/or embedded in social media posts.

POS vendors, acquirers and/or acquirer processors may be able to assist by providing turnkey training materials. But whether or not this is the case, EMV training shouldn’t be a one-time endeavor given the high rate of employee turnover in both retail stores and restaurants.

**Beyond EMV**

EMV brings significant benefits to the table, but it also has its limitations. Notably, the technology’s scope is limited in that it doesn’t encrypt primary account numbers (PANs) at the point of sale. Rather, PANs are stored and transmitted in the clear, making it easy for them to fall into hackers’ hands.

Moreover, EMV isn’t effective in card-not-present (CNP) transactions because there are no provisions for consumers making online purchases to enter a PIN number, or to scan the chips embedded in their credit cards. In other parts of the world, the incidence of CNP fraud has increased in conjunction with the adoption of EMV-compliant in-store technology. The UK saw a 79% increase...
in CNP fraud between the effective date of its liability shift (2005) and 2008, from $151 GBP to $328 GBP, according to Financial Fraud Action UK.

Similarly, in Canada, losses from counterfeit and lost/stolen cards declined by 54% from the beginning of the migration to EMV in 2008 to 2013 (from $245.4M CAD to $111.5M CAD). CNP fraud saw a corresponding increase of 133% over the same time period (from $128.4M CAD to $299.4M CAD), according to the Canadian Bankers Association.

With these limitations in mind, merchants should implement other secure technologies as a part of a layered payment security solution, including:

**Tokenization**

Tokenization protects card data by replacing the primary PAN with a unique, randomly generated sequence of alphanumeric characters or a combination of a partial (truncated) PAN and random alphanumeric sequence. A one-to-one relationship between each tokenized string and the account data stored at the acquirer, merchant or network level allows merchants to use the token to facilitate settlement as well as for recurring processing, chargeback processing, fraud management and the like.

The beauty of tokenization is that data cannot be decrypted without a key, making it of no value to hackers. With tokenization, card numbers are separated from and not stored on systems or in data repositories where merchants have no need for them. This removes merchants from Payment Card Industry Data Security Standard (PCI DSS) scope and protects sensitive data in the physical and remote channels.

Tokenization has been gaining traction among merchants not only for the above reasons, but also because the formatting of tokens occurs in a manner that is similar to the formatting of card information. This eliminates the need to make major changes in payment acceptance systems. There’s also an appealing tie-in for retailers that are exploring or already pursuing mobile wallet acceptance. Proponents of tokenization note that single-use tokens might be issued to customers to store in their virtual wallets. These tokens would serve as substitutes for actual credit and debit card numbers, with consumers using them as they would plastic payment cards to pay for goods and services. In these cases, merchants would be able to complete transactions without the need to touch or store true PAN data.

**Point-to-point encryption (P2PE)**

While tokenization addresses security vulnerabilities after a transaction has been authorized, P2PE mitigates security weaknesses that exist at the moment card data is captured. Here, the card reader encrypts data at the point of capture before that data passes through the secure payment gateway to the bank or processor. As a result, clear-text data from merchants' network and POS system remains out of hackers' reach.
Opting for P2PE is an especially good idea because it secures and encrypts data from the merchant network and POS system on a hardware “end” to hardware “end” basis, rather than on a software “end” to software “end” basis. Software-to-software encryption can be effective, but it leaves room for hackers to install malware on merchants’ systems. In a nutshell, the EMV standard is mostly about securing transactions, while standards for PCI compliance are about securing the network environment.

As part of its P2PE program, the PCI Security Standards Council (PCI SSC) now offers P2PE vendors the option to validate their solutions and applications. Merchants that deploy a PCI SSC-validated P2PE solution as a complement to EMV-compliant technology not only reap the benefits of hardware-to-hardware encryption; they also reduce the scope of their PCI DSS assessments. To qualify for validation, a P2PE solution must comply with the PCI SSC P2PE Standard. As such, the solution encrypts cardholder data from when it’s swiped or dipped into a chip reader, until the point where a third-party payment processor or acquirer decrypts the data.

### 3-D Secure

3-D Secure is a protocol that adds an extra layer of security to CNP transactions. Leveraged by Visa, Mastercard and American Express as Verified by Visa, Mastercard SecureCode, and American Express SafeKey, respectively, 3-D Secure provides a mechanism through which cardholders can authenticate themselves when making purchases in a CNP environment. The protocol benefits merchants by shifting liability for fraudulent transactions to the issuer, regardless of whether or not the issuer has the access control infrastructure needed to support the 3-D Secure authentication request through risk assessment and stepped-up authentication prompts.

Merchants can enjoy the flexibility of deciding when they want to use it, and for which transactions. The authentication mechanism, which once involved easily forgotten, easily compromised static passwords, has evolved to a more user-friendly, difficult-to-defeat dynamic data format.

### The Last Word

While merchants may be tempted to delay migration to an EMV platform for as long as possible, this is a shortsighted approach. Becoming familiar with the ins and outs of EMV now rather than later, and beginning to chart a migration path, is the smarter course of action for SMB and large merchants alike.
Appendix

The Verifone Advantage

Whether your goal is to engage customers with multimedia, to go mobile or to protect data with the latest security features, Verifone’s payment solutions meet your needs. Our Verifone Engage, Verifone Carbon, VX Evolution, MX and Petroleum families prepare and enable you to meet tomorrow’s POS software and hardware needs.

Our decades of experience show that payment security technology must constantly evolve to keep ahead of the next hacker strategy or attack. Verifone’s understanding and vigilance have led to the development of the industry’s premier family of security solutions, VeriShield.

Multimedia Consumer-facing Devices

Engage your customers at the point of sale

Move beyond basic transactions to customer interaction and engagement. Fully customizable hardware and sturdy customer-facing POS payment terminal functionality let you provide multimedia content, loyalty programs, in-store promotions and digital coupons to your customers.

Verifone Carbon features dual merchant- and consumer-facing tablets that turn every interaction into a two-way conversation.
Countertop Devices

**Designed with the merchant in mind**

Our compact countertop payment terminals are NFC-capable and meet or exceed the latest security mandates. Enjoy flexible capabilities and payment options, from PIN pads to EMV and contactless payments. Our POS terminals are easy to install and use, regardless of what side of the transaction you’re on.

PIN Pads

**Performance and value**

No matter the size of your enterprise, we offer a PIN pad to meet your needs. Verifone PIN pads support PCI 3.X or 4.X, end-to-end encryption and remote key management.

Unattended Devices

**Reliability and flexibility**

Indoors or outdoors, our rugged self-service payment systems provide reliability, security, and convenience for customers and can help generate incremental revenue.
Portables

**Payment solutions that go anywhere, anytime**

Our portable payment solutions deliver the extended coverage and flexibility needed to accept payments anytime, anywhere. Portables are designed for environments such as restaurants and hospitality where drops and spills are common, as well as transit and outdoor retail where multiple wireless connectivity options are needed.

Mobile Solutions

**Empowering the mobile payment revolution**

Mobility enables merchants to accelerate sales, elevate service and boost revenues. Mobile payment technology provides a new level of consumer interaction that provides convenience and better shopping experiences. Verifone’s portfolio of devices suit a variety of needs based on merchant feedback and technology advancements. We offer solutions for all segments of the mPOS environment, compatible with a wide range of smartphones and tablets.

Networking devices

**Powerful networking and transaction routing**

Our networking solutions include hardware and communications infrastructure designed specifically for card payment transactions. Networking systems provide flexibility, reliability, security, improved speed and low total cost of ownership while allowing you to achieve superior connectivity within your POS environment.

Petroleum POS Systems

**Today’s best technology, flexible for the future**

Whether you’re a single island gas station or a multi-island gas and convenience store, Verifone offers cost-effective, end-to-end payment solutions designed to fit your business’ needs.

VeriShield Security Solutions

**Advanced and proven protection**

Certified by an independent Qualified Security Assessor to help reduce PCI scope when properly deployed, our end-to-end encryption couples with server-based tokenization to protect data from the point of capture to the processor. By eliminating usable data from the entire data lifecycle, customers’ information is fully protected.