EMV: A MERCHANT'S PRIMER

October 1, 2015 marks a major milestone in the U.S. payments landscape. As of that date, liability for fraudulent, counterfeit credit and debit card transactions shifts from issuers to merchants, unless those merchants have migrated to POS technology that accommodates credit and debit cards manufactured in compliance with 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 (and shouldn't) expect from failure to embrace EMV-compliant technology. We also dispel some of the myths surrounding EMV implementation, layout 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. The EMV specifications were developed to define a set of 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 mag-stripe cards. The cards, which continue to feature mag-stripes as well, come in three "flavors":

- **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. The card must remain in the slot for the duration of the transaction.
- **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 can communicate with the card by touching its plate, or in RF mode.

As for EMV specifications, these are managed, maintained and enhanced by EMVCo, an organization that also 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, among them banks, merchants, processors and technology vendors, participate in EMVCo initiatives as technical and business associates. **However, EMVCo is not responsible for individual card brand certifications.**

When it comes to EMV adoption, the U.S. is the last "holdout," with an installed terminal base that remains in the low single digits percentage-wise, according to a report by First Data. By contrast, most estimates hold that 40 percent of the world's cards and 70 percent of its terminals presently conform to the EMV standard. According to Visa, 62 percent of transactions conducted across international borders are currently completed with chip-enabled cards used at chip-enabled terminals.

What's more, according to EMVCo, payments made with chip-based EMV cards accounted for a respective 96 percent and 50 percent of card-present transactions in "Europe Zone 1" (38 nations, including France and the UK) and "Europe Zone 2" (17 nations, including Russia and Ukraine) from July 2013 through June 2014. During the same time period, 83 percent of card-present transactions originating in Canada, Latin America and the Caribbean were EMV-based. So, too, were 76 percent of transactions originating in Africa and the Middle East.

Wherever it's occurring, the case for EMV adoption is very strong because it:

Decreases card fraud.

As mentioned above, EMV-enabled cards contain a microprocessor chip that stores information securely and carry security credentials that are encoded by the card issuer at the time each card is personalized for an individual cardholder using user-specific keys. The encoding of these credentials helps to prevent fraudsters from creating counterfeit cards ("cloning"). Unlike mag-stripe cards, which are easy to duplicate because they lack the security features of microprocessor chips, EMV cards cannot be duplicated and utilized 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. (For more on the dynamic cryptogram, see the "Card Authorization" bullet point below.

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

- **Transaction authorization** enlists issuer-defined rules to authorize transactions either online or offline. For an online authorization, EMV transactions proceed in the same manner as with mag-stripe cards. Transaction information and a transaction-specific cryptogram are sent to the issuer, which authorizes or declines the transaction. In an offline transaction, the card and terminal communicate and use issuer-defined risk parameters within the card to determine whether the transaction can be authorized. Offline transactions are typically used in situations where terminals do not have online connectivity (e.g., at a ticket kiosk) or in countries where telecommunications 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 in an effort to complete a fraudulent transaction 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. At present, most U.S. issuers are opting for chip and signature over chip and PIN as the cardholder verification method. Moreover, no CVM is used almost exclusively on unattended devices where transaction amounts are typically quite low and the speed of the transaction is most important.

Allows interoperability with the global payments infrastructure.

Consumers with EMV-enabled cards can use their card on any EMV-compatible payment terminal throughout the world. Such interoperability is likely to become increasingly important as some nations consider phasing out mag-stripe cards entirely.

Meanwhile, although merchants aren't required to follow an EMV migration path, significant benefits also 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. As of the liability shift date, MasterCard will exempt merchants from 100 percent of account data compromise penalties only if at least 95 percent of MasterCard transactions that originate in their stores are handled on EMV-compliant POS terminals. As of the same date, Visa will hold "the party that is the cause of a chip card transaction not occurring" (e.g., 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.

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

Near-field communications (NFC)-enabled 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 U.S.

Take advantage of global interoperability to boost business.

Many U.S. 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 mag-stripe on their cards to process payments.

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: EMV will never be widely accepted in the U.S.

Reality: Some merchants believe this is true because other much-hyped technologies, like near-field communications (NFC), have yet to make it into the "major leagues," also because banks and issuers aren't serious about making a transition to chip cards. But while not all merchants will be "EMV-ready" by the October 2015 deadline, statistics show that many are heading in that direction. According to the Payments Security Task Force (PST), a poll of an unspecified number of acquirers reinforces an earlier forecast in which it projected that at least 47 percent of U.S. card terminals will be EMV-capable by year-end 2015.

Statistics also show that banks and issuers are quite serious about moving ahead on the chip card front. Based on the poll, the PST estimates that by the end of 2015, EMV chips will be found in 63 percent of cards issued by eight financial institutions representing 50 percent of U.S. payment card volume. Applying this EMV share to the entire U.S. card base (approximately 1.2 billion general-purpose credit and debit cards), it's reasonable to conclude that 800 million chip cards may have been distributed in the U.S. when 2015 draws to a close.

Statistics from research firm Aite Group also dispel this myth. Eighty-six percent of financial institutions plan to issue EMV debit cards in the next two years, Aite says, with 40 percent of debit cards and 70 percent of credit cards issued in the U.S. expected to be EMV-enabled by the end of 2015.

And as if that weren't enough, Discover earlier this year announced that a majority of its transaction volumes would be generated by EMV-enabled cards by the end of 2015. Discover has also introduced merchant incentives for migrating to an EMV platform.

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

Reality: A look at statistics from abroad, as reported by EMVCo, demonstrates that quite the opposite is true. Consider the United Kingdom, where the concept of EMV was pilot-tested between May and September 2003 in a program that involved 600 merchants and 180,000 chip cards. The test was successful, with a nationwide EMV rollout initiated in 2004 and an EMV liability shift occurring one year later. Card fraud losses in the United Kingdom stood at $102.3 million GBP in 2013, less than half of what they were ($274.1 million) in 2004, according to the UK Cards Association. Losses at U.K. retailers have fallen by 67 percent since 2004; lost and stolen card fraud fell by 58 percent between 2004 and 2009; and mail non-receipt fraud has fallen by 91 percent since 2004.

Then, there's Canada. Its move to EMV got underway in 2003, when Visa Canada said it would begin migrating traditional mag-stripe-based Visa Canada cards to EMV chip cards by 2004. This announcement induced Interac, Canada's largest payment body, to declare one year later that all mag-stripe credit and debit cards would be replaced with chip-based cards.

In 2006, MasterCard Canada announced support for chip and PIN-based EMV cards. Pilot-tests of EMV cards and technology were conducted from 2007 to 2009 and liability shifts were introduced in 2010. While Canada's deadline for conversion to EMV-ready POS technology is not until the end of this year, Interac reported in mid-2014 that the nation had already seen marked debit card fraud losses as a result of the ongoing transition to an EMV platform. Such losses plummeted from a high of $142 million (CAD) in 2009 to a record low of $29.5 million in 2013. Just as significantly, a mere $7.3 million (CAD) of these losses resulted from fraud perpetrated against Canadian debit cardholders within Canada itself.

Myth: Money can buy the 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 face significant liability for card present fraud, resulting in significant financial repercussions. Losses can add up per incident, enough to severely cripple the average small- or medium-size merchant and possibly even put it out of business as well as to make a sizeable dent in the finances of larger operations.

Again, while it is true that MasterCard will exempt merchants from 100 percent of data compromise penalties under certain circumstances, money can't buy that privilege. The exemption is available only if 95 percent of transactions originating in a merchant's stores are completed on EMV-compliant equipment.

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

Reality: Fraudsters continue to remain at least one step ahead of merchants, processors, card networks and other entities when it comes to finding ways to perpetrate their crimes, including the counterfeiting of cards. This means 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.
Myth: Migrating to EMV-compliant technology is too expensive.

Reality: At first blush, 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 after the liability shift takes effect. Should that occur, the initial cost of rolling out EMV-compliant hardware will seem infinitesimal compared to penalties and lost business from failure to have upgraded a non-compliant system.

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

Reality: Admittedly, many U.S. consumers are still confused about what EMV is and what it means for payments, if they have heard about it at all. However, the tides are quickly turning. With the liability shift fast approaching, consumer media are buzzing with stories and messages about EMV and its promise of enhanced payment security. As more and 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. Given a choice between patronizing any size merchant whose POS equipment configuration (e.g., EMV-compliant) doesn't require them to hand over their credit card in order to make a payment, and a retailer whose equipment does, they will choose the former providing that merchandise selection, prices and the like fall into a similar range.

In addition, tourists from nations where EMV has already become the new (or not-so-new) payment norm may be reluctant to shop at U.S. stores that do not have EMV-compliant equipment in place. So all in all, avoiding EMV migration in part based on a belief that it doesn't matter to consumers not only makes no sense; it also puts merchants at risk of sacrificing sales to competitors.

LAYING THE GROUNDWORK

Garnering knowledge about the basics of EMV and replacing misconceptions with facts can be considered the "logical" side of taking the EMV plunge. The other aspect entails laying the groundwork for implementation, specifically:

Consulting POS equipment vendor(s).

Work with these vendors to determine chip acceptance needs, whether POS devices will be standalone or integrated and what changes will need to be made to customer interaction and transactional procedures as the move to EMV is made.

Verifone recommends opting for dual-interface chip readers that accommodate contact and contactless payments, and 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. However, there are others. Notably, to qualify for relief from PCI requirements, ADC relief and the liability shift as offered by Visa, MasterCard, American Express and Discover, merchants must install dual contact/contactless terminals.

What's more, while contact chip cards will never become obsolete, installing POS terminals that also accept contactless cards is a direct path to achieving mobile NFC payment acceptance capability; no extra equipment is necessary. And of course, contactless payments enable merchants to offer rapid checkout, a "perk" that's in increasingly high demand among busy consumers.

Making the right software selection.

Consult with a vendor, such as Verifone, to find a solution that best fits individual processing needs and is certified to work with the 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 that involve 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.

No matter the caliber of a merchant's technology and stakeholder partners, providing employees with the 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, which can be kept at the point of sale for quick reference) cover:

- **Application selection and cardholder verification processes.** Employees must understand how to help customers choose the application they wish to use and guide novices through the process of pressing the correct buttons to make these choices. Explain that the terminal and the chip card will "agree" on which CVM is required in this particular instance to verify the transaction, and that this will be based on transaction specifics (e.g., amount, domestic or international transaction, whether the issuer's CVM preference can be met and other available CVM options).
- **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 through and immediately removed from the card reader, as is the practice with mag-stripe cards. Rather, they must be inserted into the terminal and remain there until the transaction is completed and the terminal has indicated to that effect. 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 there noted a high incidence of cards left behind by consumers who had forgotten to remove them from the card reader. To prevent this from occurring, train employees to remind customers to take their cards once their payments have been processed. Another way to prevent this from occurring is to 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's mag-stripe is subsequently read, the terminal reads the service code and prompts the terminal to read the card as a chip card. Personnel generally are allowed a few attempts at using the chip reader to read the chip card before the terminal prompts for a fallback read of the mag-stripe, if permitted by the issuer. If the chip card reader cannot be used, the transaction can be handled using the mag-stripe.

Educating consumers about how to complete EMV transactions is also a good idea; given how radically they differ from transactions handled with mag-stripe cards. 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 once they have paid for their purchases. 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 that demonstrate EMV transactions 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 with training 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 clearly 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, rendering 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, before completing a transaction. 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 United Kingdom, for example, saw a 79 percent 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 percent from the inception of the migration to EMV in 2008 through 2013 (from $245.4 CAD to $111.5 million CAD). CNP fraud saw a corresponding increase of 133 percent over the same time period (from $128.4 million CAD to $299.4 CAD), according to the Canadian Bankers Association.

With these limitations in mind, merchants should implement other secure technology as a part of a layered payment security solution that also comprises other components, rather than as a payment security solution in its entirety. These include:

Tokenization: Tokenization protects card data by replacing the primary PAN with a unique, randomly generated sequence of numbers and alphanumeric characters or a combination of a partial (truncated) PAN and a 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 special key, making it of no value to hackers. Under a tokenization umbrella, payment card numbers are separated from and not stored on systems and in data repositories where merchants have no need to keep them (repositories of data used for sales analysis comprises one example). This removes merchants from the scope of the Payment Card Industry Data Security Standard (PCI DSS) and protects data from compromise in the physical and remote channels alike.

Tokenization has been gaining ground among merchants not only for the above reasons, but also because the formatting of tokens occurs in a manner that's similar to the formatting of card information. This eliminates the need to make major changes in payment acceptance systems. What's more, there's 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. However, 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 when card data has been captured, but not yet authorized. 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 leeway for hackers to install malware on merchants' systems. In a nutshell, the EMV standard is mostly about securing transactions, and 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 P2PE 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 (as well as a listing on the PCI SSC website), a P2PE solution must comply with the PCI SSC P2PE Standard. Consequently, the solution encrypts cardholder data from the point at which a point-of-sale device accepts the payment card after it has been swiped through or dipped into a mag-stripe reader, to the point where the third-party payment processor or acquirer decrypts the data for processing.

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 the issuer possesses on its side the access control infrastructure needed to support the 3-D Secure authentication request through risk assessment and stepped-up authentication prompts.

Early versions of 3-D Secure had several limitations, but fundamental changes designed to improve its effectiveness have been implemented. For instance, merchants were initially compelled to invoke the protocol with every CNP transaction or none at all. Today, they typically 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. EMVCo is currently in the process of developing a new specification for 3-D Secure and expects to release a draft specification by the end of 2015.

THE LAST WORD

Just as it has taken hold in other parts of the world, EMV is gathering steam in the U.S. While merchants may be tempted to delay migration to an EMV platform for as long as possible, this is a short-sighted 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, our POS hardware and software payment solutions meet your needs. Our VX Evolution, MX Solutions 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. Whether it's customer fraud, data and ID theft or other external threats, Verifone's understanding and industry vigilance has 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.

http://www.verifone.com/products/hardware/multimedia/

COUNTERTOP DEVICES

Designed with the Merchant in Mind

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

http://www.verifone.com/products/hardware/countertop/

PIN PADS

Performance and Value

Regardless of the size of your enterprise, we offer a PIN pad point-of-sale device to meet your needs. Verifone PIN pads support PCI 3.X, end-to-end encryption and remote key management.

http://www.verifone.com/products/hardware/pin-pad/

UNATTENDED DEVICES

Reliability and Flexibility

Provide reliability, security and convenience in unattended environments. Whether indoor or outdoor, our secure and rugged self-service payment systems provide convenience for customers and can help generate incremental revenue.

http://www.verifone.com/products/hardware/unattended/

PORTABLES

Rugged Payment Solutions Go Anywhere. Anytime.

Our portable payment solutions deliver the extended coverage and flexibility that merchants need to accept payment anytime, anywhere. Portables are designed for rugged environments including restaurant and hospitality where drops and spills are common, as well as transit and outdoor retail where multiple wireless connectivity options are needed. Regardless of your business type, you'll be able to accept any form of electronic payment including NFC, mobile wallets, EMV and mag-stripe.

http://www.verifone.com/products/hardware/portable/

EMPOWERING THE MOBILE PAYMENT REVOLUTION

Mobility has transformed the way merchants and retailers view their business – enabling them to accelerate sales, elevate service and boost revenues. Mobile payment technology provides a new level of consumer interaction that empowers a sales person to truly engage with customers to provide convenience and better shopping experiences.

As innovators and pioneers in the mobile payment space, Verifone has built a portfolio of mobile hardware devices to suit the needs of many based on merchant feedback and technology advancements. We offer solutions for all segments of the mPOS environment from large retailers to small merchants – enabling payment mobility anywhere and everywhere. The full line of devices works with Apple® iPad®, iPod touch®, iPhone® and other smartphones and tablets.

http://www.verifone.com/products/hardware/mobile/

NETWORKING DEVICES

Powerful Networking and Transaction Routing

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

http://www.verifone.com/products/hardware/networking/

PETROLEUM POS SYSTEMS

Today's Best Technology, Flexible for the Future
Whether you're a single island gas station store or a multi-island gas and convenience store, Verifone offers cost-effective, end-to-end payment solutions designed to fit your business' needs. As the petroleum and convenience store industry grows and embraces new technology, Verifone is there to provide customers, big and small, with the point-of-sale solutions that keep business running.

http://www.verifone.com/products/hardware/petro-pos-systems/

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 securely protect data from the point of capture to the processor. By eliminating usable data from the entire data lifecycle, there's essentially nothing meaningful for thieves to compromise.

Your customers' data, whether transmitted from a card or mobile device, is protected from the point of capture.

http://www.verifone.com/products/security/

QUESTIONS & ANSWERS

THESE ARE ACTUAL QUESTIONS & ANSWERS FROM VERIFONE WEBINARS GIVEN FROM FEBRUARY 2012 TO PRESENT.

1. General
2. Liability & Security
3. Transactions
4. Contactless / Non-contactless
5. Standards, Compliance & Approvals
6. Issuers
7. Rates & Fees
8. NFC
9. Tip Adjust
10. Apple Pay
11. Devices/Product-related

GENERAL

HOW LONG WILL IT TAKE TO PROCESS EMV CONTACTLESS AND EMV CONTACT TRANSACTIONS? HOW DOES THIS COMPARE TO THE TIME TO PROCESS A TRANSACTION COMPLETED WITH A TRADITIONAL MAG-STRIPE CARD?

Transactions completed using chip cards in general take a few seconds longer to process than transactions completed using mag-stripe cards because of the additional required security steps, for instance, requesting and validating the cryptogram. However, completing EMV contactless transactions is said to be a faster process than completing contact EMV transactions (30 to 40 percent, according to Chase and 53 percent, according to American Express).

CAN CHIP CARDS BE USED FOR PURPOSES OTHER THAN PAYMENTS?

Yes. Because the chip is essentially a tiny computer, it can be used in a wide variety of applications beyond payments. Loyalty applications are a good example; the chip can store loyalty program credentials and other related information. In another example, chip cards can support transportation applications, including fare collection, ticketing and gas station/fleet. Currently, no issuers are issuing cards with more than one application. Issuing cards with payment and other type of application would require coordination between suppliers as well.

WHAT WOULD PREVENT A CHIP CARD WITH A BROKEN CHIP FROM BEING DUPLICATED?

The mag-stripe on an EMV chip card can also be duplicated just as it can on a single mag-stripe card.

THERE HAS BEEN SOME PRESS COVERAGE CLAIMING THAT CHIP CARDS PRODUCED IN THE U.S. ARE UNRELIABLE. IS THIS TRUE?

This is a gross generalization. While there have been incidents of thwarted EMV transactions due to defective chips, these have been few and far between. It is more likely that difficulties encountered in using EMV-enabled cards to complete transactions stem from improper operation of point-of-sale equipment (e.g., consumer understanding how to insert the card).

WHAT IS THE LIKELIHOOD THAT A CHIP IN A CHIP CARD WILL BECOME DAMAGED? IF A CHIP CANNOT BE READ, WHAT SHOULD HAPPEN NEXT?

Chips are fairly resilient to damage, especially as they are well-embedded in the card. If the chip malfunctions, the merchant should perform a fallback transaction using the mag-stripe. There would be no concern about liability for a fraudulent transaction in such a situation because EMV-capable technology was in place and did not cause the merchant's inability to process the transaction in EMV mode.

WOULD A STOLEN (OR LOST AND FOUND) CHIP CARD BE USEABLE AT ALL?

Not if the theft or loss has been reported. However, until that occurs, a fraudster could conceivably use such a card at a merchant that has not made the move to EMV and is still processing cards using mag-stripes.

MAG-STRIPE CARDS ARE DUPLICABLE WITH HANDHELD MAG-STRIPE READERS, BUT CAN CHIP CARDS BE DUPLICATED?

No. As their name indicates, EMV-enabled cards contain microprocessor chips that store information securely and carry security credentials that are embedded at the time each card is personalized for an individual cardholder using user-specific keys. The creation of these credentials helps to prevent fraudsters from creating counterfeit cards ("cloning").

WHY ARE SOME NEW CARDS AUTHENTICATED USING CHIP AND PIN AND OTHERS, USING CHIP AND SIGNATURE? IS CHIP AND SIGNATURE AUTHENTICATION MORE PRONE TO FRAUD?

Issuers determine whether the chip cards they issue will be authenticated via chip and PIN or chip and signature. Most chip cards issued in the U.S. are authenticated via chip and signature, a trend many attribute to the fact that the need to program chip and PIN cards with a PIN before sending them to cardholders adds to card issuance costs. Some issuers also reportedly want to keep the authentication process simple for consumers, at least through the first wave of EMV migration. They believe this is better accomplished through chip and signature authentication because consumers are already accustomed to providing a signature for credit card transactions.

However, it is true that while chip cards afford a far greater measure of security than their mag-stripe counterparts, chip and PIN authentication has less fraud than chip and signature authentication.

HOW ARE CHIP CARD TRANSACTIONS AUTHORIZED ONLINE? AND WHAT HAPPENS WHEN A CHIP CARD TRANSACTION IS AUTHORIZED OFFLINE?

In an online authorization scenario, transaction information is sent to the issuer, along with a transaction-specific cryptogram. The issuer either authorizes or declines the transaction in real time. In an offline EMV scenario, the chip in the card and the point-of-sale terminal communicate and harness issuer-defined risk parameters that are set in the card to determine whether the transaction can be authorized. Chip cards can be configured to allow both online and offline authorization, depending on the circumstances.

IF A CARD HAS A CHIP, CAN THE CARD NUMBER BE ENTERED MANUALLY?

Manual card number entry may occur if the chip is physically damaged or cannot be read by the card reader. In situations where there is a chip read error, the terminal will display a message instructing the customer to re-insert the card a number of times (generally, two to three). If the card still cannot be read, then mag-stripe will be read and the transaction treated as a "technical fallback." Manually keying in transactions is an option, but it could have liability shift consequences.

IF A CHIP CARD'S NUMBER WERE ENTERED MANUALLY, WOULD AUTHENTICATION REQUIRE A SIGNATURE INSTEAD OF A PIN?

CVM selection is automatic process between the terminal and the card. If the auto-selected CVM cannot be processed, the terminal should go to the next secure form of CVM. This will automatically occur within the terminal application and kernel.

LIABILITY & SECURITY

IF A MERCHANT DOES ALL CNP THROUGH A TERMINAL, HOW DOES EMV LIABILITY AFFECT THEM? WHY WOULD THEY NEED TO GET A NEW EMV TERMINAL?

EMV is card-present only.

IF A CUSTOMER FORGETS THEIR PIN AND A MERCHANT RUNS THE TRANSACTION USING MAG-STRIPE, DOES LIABILITY SHIFTS TO THE MERCHANT IN EVENT OF COUNTERFEIT CARD?

No, the liability will be the issuer's.

WILL VERIFONE VX 520 NON-CONTACTLESS TERMINALS EXPOSE MERCHANTS TO LIABILITY FOR FRAUDULENT TRANSACTIONS UNDER THE LIABILITY SHIFT PARAMETERS BECAUSE THEY DO NOT SUPPORT THE CONTACTLESS METHOD OF PAYMENT ACCEPTANCE?

Yes. Each brand has a unique set of incentives and parameters around the liability shift that may require a hybrid device that supports both contact and contactless functionality.

DOES THE EMV LIABILITY SHIFT APPLY TO STOLEN CARDS THAT HAVE MERELY BEEN STOLEN, RATHER THAN COUNTERFEITED?

Each card brand has its own rules for the liability shift. Generally Visa does not apply this liability for fraudulent transactions to lost or stolen cards and the other card brands do.

AS MERCHANTS MIGRATE TO EMV, HACKERS WILL LOOK TO EXPLOIT LOWER-HANGING "FRUIT," STEALING DATA GLEANED FROM CARD-NOT-PRESENT (CNP) TRANSACTIONS. WILL TWO-FACTOR AUTHENTICATION BE USED IN THE FUTURE TO ADD ANOTHER MEASURE OF SECURITY TO THESE TRANSACTIONS?

This is very likely, as a number of entities are working on solutions that fit the mold. However, there is an interim solution, and it's called 3-D Secure. Promoted 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 the issuer possesses on its side the access control infrastructure needed to support the 3-D Secure authentication request through risk assessment and stepped-up authentication prompts.

Early versions of 3-D Secure had several limitations, but fundamental changes designed to improve its effectiveness have been implemented. For instance, 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. EMVCo, which manages the EMV standard, is currently in the process of developing a new specification for 3-D Secure and expects to release a draft specification by the end of 2015.

IF A MERCHANT AND AN ISSUER HAVE ACHIEVED THE SAME DEGREE OF COMPLIANCE WITH THE EMV STANDARD, WHICH PARTY IS LIABLE IN THE CASE OF CARD-PRESENT FRAUD?

If the issuer has issued chip cards, and the merchant has implemented technology that is EMV-capable (and accordingly, processes chip card transactions in contactless or contact mode or both), the liability remains the same as before the shift went into effect and does not fall on the merchant's shoulders.

HOW CAN MERCHANTS COMPLY WITH CHARGEBACK LIABILITY RULES IF ISSUING BANKS ARE RESPONSIBLE FOR DISTRIBUTING CHIP CARDS?

There is no such thing as "chargeback liability rules," but there is an upcoming liability shift. As of October 2015, liability for fraudulent credit and debit card transactions shifts from issuers to merchants, unless those merchants have migrated to POS technology that accommodates credit and debit cards manufactured in compliance with the EMV standard. As long as a merchant has implemented EMV-compliant point-of-sale technology, it is EMV-compliant and free from liability for fraudulent card-present transactions. Issuers' initiatives on the chip card front, or lack thereof, have no impact here.

IS MERCHANTS' RELEASE FROM LIABILITY FOR FRAUDULENT CARD-PRESENT TRANSACTIONS DEPENDENT ON THE TERMINAL, OR WHETHER A CHIP CARD WAS PRESENTED AT THE POINT OF SALE?

Merchants' liability, or lack of liability, for fraudulent card-present transactions depends solely upon whether or not they have migrated to EMV-enabled technology that accommodates payments made with chip cards. This means that no matter the type of card with which a fraudulent transaction was completed, merchants are not liable if their terminals can handle chip card payments.

DOES THE FACT THAT A MERCHANT'S HARDWARE IS CAPABLE OF PROCESSING CHIP CARD TRANSACTIONS RELEASE IT FROM LIABILITY FOR A FRAUDULENT CARD-PRESENT TRANSACTION COMPLETED WITH A MAG-STRIPE CARD—AND FOR PAYING ANY ACCOUNT DATA COMPROMISE PENALTIES?

Yes. To be a bit more specific, as of the October 2015 liability shift date, MasterCard will exempt merchants from 100 percent of account data compromise penalties if at least 95 percent of MasterCard transactions that originate in their stores are handled on EMV-compliant point-of-sale terminals. Visa will only hold merchants accountable for card-present counterfeit fraud losses if their terminals are not EMV-compliant; "the party that is the cause of a chip card transaction not occurring" assumes the liability. Please read the exact card brand rules to get more information.

WHAT IS DUPLICATE CARD FRAUD, AND DOES THE LIABILITY SHIFT APPLY TO IT?

Duplicate card fraud is the actual reproduction ("cloning") of fake credit and debit cards. Merchants are released from liability for fraudulent card-present transactions completed with these cards providing that they have migrated to an EMV-enabled payment platform.

TRANSACTIONS

CAN THE PIN BE BYPASSED FOR AN EMV TRANSACTION?

Yes, if the merchant and acquirer allow for PIN bypass, meaning the consumer chooses to bypass the PIN entry prompt. However, please ask your acquirer processor if they support this function in their Verifone application.

DOES AN EMV DEVICE REQUIRE KEY INJECTION TO PROCESS EMV DEBIT TRANSACTIONS?

Online PIN CVM (independent of debit or credit) does require a key be injected because the device is encrypting the PIN entered by the consumer similarly as the debit card PIN on a mag-stripe card today. If the merchant is accepting an offline PIN CVM (independent of debit or credit), the device does not require key injection because the PIN is not being transmitted but verified locally on the terminal.

FOR PAY AT THE PUMP, WILL THE CARD NEED TO REMAIN IN THE TERMINAL WHILE THE CUSTOMER IS PUMPING THEIR GAS?

The card will only need to remain inserted until the EMV processing is completed.

WHAT IF THE CARDHOLDER ENTERS AN INCORRECT PIN?

For online or offline CVM, the cardholder will be able to re-enter the PIN based on the parameter setting for PIN retries. If the PIN is still not correct, the transaction will decline. The cardholder will be able to select PIN bypass if it is merchant and acquirer enabled.

WHY DO WE NEED A SEPARATE PIN PAD TO PROCESS TRANSACTIONS INSTEAD OF AN INTERNAL ONE?

If the CVM is either online or offline PIN, the PIN must be entered on the same device as the card is inserted or tapped according to EMVCo specifications.

WITH SOME BANKS ISSUING CHIP AND PIN CARDS AND OTHERS ISSUING CHIP AND SIGNATURE CARDS, HOW WILL MERCHANTS KNOW WHETHER CUSTOMERS SHOULD ENTER THEIR PIN OR PROVIDE A SIGNATURE TO COMPLETE CHIP CARD TRANSACTIONS?

The terminal will prompt the customer to enter a PIN into the PIN pad or provide a signature to complete the transaction.

SUPPOSE A MERCHANT ATTEMPTS TO PROCESS A CHIP CARD PAYMENT ON EMV-COMPLIANT EQUIPMENT, BUT THIS DOES NOT WORK SO IT ATTEMPTS TO SWIPE THE MAG-STRIPE INSTEAD. WILL THE POINT-OF-SALE SYSTEM DOCUMENT THAT THE MOST SECURE FORM OF TRANSACTION PROCESSING WAS INITIATED FIRST?

Yes.

ARE MERCHANTS PROHIBITED FROM REMOVING CARDS FROM CUSTOMERS' HANDS AND PRESENCE DURING CHIP CARD TRANSACTIONS?

No. While in many instances store employees, rather than customers, swipe mag-stripe cards through a card reader during transactions and then hand them it back to customers, this is not the case in an EMV scenario. Rather, customers completing payments insert their chip cards into a slot in the card reader and leave them there until the transaction is completed.

MUST MERCHANTS WHO MANUALLY CAPTURE THE LAST FOUR DIGITS OF CUSTOMERS' CARDS FOR ADDED SECURITY CONTINUE TO DO SO FOR CHIP CARD TRANSACTIONS?

Yes, but this is not a requirement.

WILL RECEIPTS GENERATED BY EMV-COMPLIANT TECHNOLOGY INDICATE THAT A TRANSACTION WAS COMPLETED WITH A CHIP-ENABLED CARD?

Yes. However, the breadth of information on the receipt varies based on the acquirer and must follow Reg. E requirements.

HOW LONG DOES IT TAKE FOR MERCHANTS TO PROCESS CONTACT CHIP CARD TRANSACTIONS?

Transactions completed using chip cards in general take a few seconds longer to process than transactions completed using mag-stripe cards because of the additional required security steps. However, processing contact chip card transactions takes a bit more time process than processing contactless chip card transactions. According to Chase, contactless transactions take 30 to 40 percent less time to process than contact transactions and American Express claims this figure is closer to 53 percent.

WHAT WILL HAPPEN IF A CHIP CARD IS SWIPED AT THE POINT OF SALE, AND WHAT MESSAGE WILL CONSUMERS SEE?

If a consumer attempts to swipe a chip card rather than insert it, a message instructing him or her to insert the card instead will be shown. EMV-enabled point-of-sale terminals have a slot into which consumers must insert their chip cards to initiate a transaction; this replaces the swiping step.

HOW WILL CARD-NOT-PRESENT, ONLINE AND PHONE TRANSACTIONS EXECUTED WITH CHIP CARDS BE PROCESSED WHEN THE CVV NUMBER CHANGES AND THE CARDHOLDER CANNOT GIVE THE CVV NUMBER TO THE MERCHANT?

The CVV (1) number does not change. A CVV is a unique code encoded in the mag-stripe and chip. 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 static data authentication (SDA), dynamic data authentication (DDA) or a combination of DDA with application cryptogram generation (CDA). Dynamic data is unique to each transaction, so it can't be used more than once even if fraudsters manage to steal it.

CONTACTLESS / NON-CONTACTLESS

WHAT IS A KERNEL?

An EMV kernel is software that resides on the terminal and complies with debit/credit network and brand for contact and contactless requirements.

IS THERE A DIFFERENT CHIP IN THE EMV CONTACT-READ CARDS AND THE EMV CONTACTLESS CARDS?

No.

IF YOU GO TO USE A DUAL-INTERFACE CARD BY INSERTING IT, WILL IT READ THROUGH CONTACTLESS BEFORE YOU GET IT INSERTED?

It depends on which CVM is desired by the merchant.

WILL ATTACHING A CONTACTLESS PIN PAD TO A NON-CONTACTLESS TERMINAL CONVERT IT TO A CONTACTLESS EMV CONFIGURATION?

The PIN pad must be capable of EMV support in order to support a contactless EMV transaction.

WHAT IS THE RELATIONSHIP BETWEEN EMV AND CONTACTLESS TRANSACTIONS?

Issuers are now issuing EMV cards that support contact and/or contactless EMV transactions. Contactless EMV transactions use the ISO/IEC 14443 protocol for communication, with EMVCo having defined the EMV Contactless Communication Protocol Specification that is common for all payment brands. EMVCo has also published specifications for contactless POS readers that work with the payment brands' contactless applications. The EMV specifications provide a basis for contactless EMV payments, but do not specify all payment application functionality. Payment brands can implement contactless payment for EMV transactions to function in both offline and online transaction environments and to leverage the EMV cryptogram security function to validate the authenticity of the card and the transaction.

HOW IS IT POSSIBLE TO PREVENT THE THEFT OF INFORMATION FROM CONTACTLESS CHIP CARD TRANSACTIONS AS IT IS TRANSMITTED OVER THE AIRWAYS?

At at the card level, each contactless card has its own unique built-in secret "key" that is used to generate a unique card verification value or a cryptogram that exclusively identifies each transaction. No two cards share the same key, and the key is never transmitted. At the system level, payment networks can automatically detect and reject any attempt to use the card, so even if a fraudster "reads" the information from a contactless transaction, or even numerous transactions from the same card, the information would be useless.

WHEN COMPLETING CONTACTLESS CHIP CARD TRANSACTIONS, MUST CUSTOMERS WAIT UNTIL THE SALE IS TOTALED UP TO TAP THEIR CARD ON THE READER, OR CAN THAT TAKE PLACE AT ANY TIME?

Customers must wait until the sale is totaled. In every contactless chip card transaction, all of the items being purchased are rung up, and a total is calculated. Only at this point does the customer tap the contactless chip card on the reader, which then lights up and beeps as the chip is read. A receipt is printed if the merchant has set up the system to generate one.

QUESTIONS & ANSWERS

STANDARDS, COMPLIANCE & APPROVALS

WHAT IS THE DIFFERENCE BETWEEN LEVEL 1 AND LEVEL 2 EMV CERTIFICATIONS?

The Level 1 Type Approval process tests compliance with the electromechanical characteristics, logical interface and transmission protocol requirements defined in the EMV Specifications. Level 2 Type Approval tests compliance with the debit/credit application requirements as defined in the EMV Specifications. Please visit the Terminal Type Approval for more information.

HOW DOES EMV AFFECT INTERCHANGE QUALIFICATION RULES AS STATED BY THE CARD BRANDS?

It does not at this time. Each merchant type should be following the interchange qualification rules (see visa.com, etc.) for more information.

WHO SETS THE PARAMETERS FOR PROCESSING "NO CVM" (CARD VERIFICATION METHOD) TRANSACTIONS?

Parameters for processing "no CVM" transactions vary by merchant, issuer and card brand. If the amount of a transaction (typically in a low-risk vertical market, such as a fast food restaurant) falls at or below that set by the given card brand and issuer, no additional verification is required and the transaction is considered "no CVM."

WHEN WILL THE U.S. HAVE AN EMV STANDARD IN PLACE FOR STANDALONE "PAY ON FOOT," OR POF TERMINALS, SUCH AS THOSE USED IN PARKING APPLICATIONS?

There is no set date for this as of yet. However, a standard is in the works.

IS PCI VALIDATION WAIVED AFTER THE OCTOBER 2015 DEADLINE IF EMV REQUIREMENTS ARE MET?

No. EMV compliance and compliance with the Payment Card Industry Data Security Standard (PCI DSS) are two entirely different things. Deploying EMV-capable technology does not satisfy any PCI requirements, including requirements contained in the newest version of the standard, known as PCI DSS 3.0. It also does not reduce PCI scope in any way.

HOW DOES THE CERTIFICATION PROCESS WORK WITH VERIFONE TERMINALS?

Verifone receives specifications from each processor and must follow and certify to each specification. Verifone parameters are set and determined by the required setup designated by the acquirer processor. Once certification is received, we publish the device listing, host and application listing to our client database. Applications can be class A or class B certified. Class A certification means that the acquirer processor wholly supports the application and device. Class B certification means the application can be used for transaction processing but must be supported by a third party.

ISSUERS

ARE ISSUERS REQUIRED TO ISSUE DUAL-INTERFACE CARDS, OR IS THIS VOLUNTARY?

Issuers have the option to offer dual-interface cards, cards that support contact and contactless EMV transactions alike. However, there is no mandate that obligates them to do so.

Supporting dual-interface cards adds complexity to EMV implementation and increases the cost issuers must pay for each card. Consequently, issuers in most countries around the world waited until a second wave of EMV implementation by merchants to see whether merchants are able to support contactless EMV

WHICH CARD NETWORKS ARE NOW EMV-ENABLED?

Visa, MasterCard, JCB, Union Pay, American Express and Discover are all EMV-enabled. However, it is up to the issuer to issue EMV-capable cards and if the need for faster payment processing, a "perk" of contactless payment technology, justified the higher costs.

ISSUERS DECIDE WHETHER TO ISSUE CONTACT CARDS, CONTACTLESS CARDS OR DUAL-INTERFACE CARDS. BUT ARE MERCHANTS OBLIGATED TO SUPPORT CONTACTLESS EMV PAYMENTS?

No, but it may be required to qualify for certain incentives. Each brand has a unique set of incentives and parameters around the liability shift that may require a hybrid device that supports both contact and contactless functionality.

However, it's a good idea to do so, and here is why: The Payment Card Industry Data Security Standard (PCI DSS) includes an audit requirement for merchants; submitting to audits as prescribed by the PCI DSS is necessary in order to achieve PCI compliance. However, incentives introduced by Visa and MasterCard allow merchants to apply for relief from the audit requirement for PCI compliance if at least 75 percent of Visa transactions and/or 75 percent of MasterCard transactions processed in their stores originate from EMV-compliant POS terminals that support both contact and contactless payments.

Merchants are also entitled to relief from 50 percent of account data compromise penalties if at least 75 percent of Visa transactions and/or 75 percent of MasterCard transactions completed at their establishments originate from terminals with contact and contactless payment acceptance capabilities. Additionally, merchants that accept American Express cards are eligible for relief from PCI DSS reporting requirements if 75 percent of American Express transactions handled at their locations are able to process both contact and contactless chip card transactions.

WHAT IS THE BREAKDOWN OF U.S. ISSUERS THAT HAVE ROLLED OUT CHIP AND PIN CARDS AND CHIP AND SIGNATURE CARDS?

Only a handful of issuers that offer chip cards have introduced chip and PIN cards rather than chip and signature cards. Issuers in this group, most of which have only launched chip and PIN cards in some of their credit and debit card lines, include American Express, Bank of America, Barclaycard, Capital One, JPMorgan Chase, Citi, Diners Club, Discover, Synchrony Bank, USAA, US Bank and Wells Fargo.

WHICH ENTITY HOLDS ACTUAL RESPONSIBILITY FOR MANUFACTURING CHIP CARDS?

Chip cards are manufactured by many approved facilities throughout the world.

DOES DISCOVER ISSUE EMV CARDS? MY OLD DISCOVER CARD HAS EXPIRED, AND THE REPLACEMENT DOES NOT HAVE A CHIP IN IT.

Yes. Discover has publicly stated that it will be issuing chip cards throughout the year and is already doing so. Discover cardholders can request a chip card on the Discover website or call the number on the back of their card to initiate receipt of a Discover chip card.

HOW CAN A MERCHANT COMPLY WITH CARD BRANDS' REQUIREMENTS FOR EXEMPTION FROM LIABILITY FOR CARD-PRESENT FRAUD IF CHIP CARDS AREN'T BEING ISSUED?

The assertion that chip cards aren't being issued is untrue. A recent poll by the Payments Security Task Force (PST) indicates that banks and issuers are quite serious about issuing chip cards. Based on the poll, the PST estimates that by the end of 2015, EMV chips will be found in 63 percent of credit and debit cards, issued by eight financial institutions that account for 50 percent of U.S. payment card volume. Applying this EMV share to the entire U.S. card base (approximately 1.2 billion general-purpose credit and debit cards), it's reasonable to conclude that 800 million chip cards may have been distributed in the U.S. when 2015 draws to a close.

However, whether or not chip cards are being issued has no impact on merchants' obligation to comply with the EMV standard if they want to avoid liability for fraudulent card-present transactions completed at their establishments. Point-of-sale equipment that can accommodate chip cards (and still accommodate mag-stripe cards) is widely available.

WILL CHIP CARDS ISSUED IN THE U.S. BE OF THE CHIP AND PIN OR CHIP AND SIGNATURE VARIETY?

U.S. issuers are issuing both types of cards. However, most appear to be gravitating toward chip and signature cards because they believe it's best to make the transition to chip cards as easy as possible for consumers. Most, if not all cardholders are already accustomed to providing a signature when they make a credit card purchase. Additionally, issuers must assign a PIN to chip and PIN cards before mailing them.

WHAT IS THE US DEBIT COMMON AID?

The Common AID was developed by the EMV Migration Forum to allow for interoperability within debit networks using a common infrastructure and having less impact to existing systems. Is it not the only way to achieve this goal.

WHAT ABILITY DO VERIFONE DEVICES HAVE FOR THE MERCHANT TO SELECT EITHER THE GLOBAL AID OR THE COMMON AID FOR PIN DEBIT ROUTING?

AID selection is set by the merchant and/or acquirer.

RATES & FEES

WILL THE EMV LIABILITY SHIFT CAUSE CHANGES IN INTERCHANGE RATES?

As of today, interchange rates will neither increase nor decrease as a result of the EMV liability shift.

WILL THE ADVENT OF CHIP CARDS ELIMINATE CROSS-BORDER FEES?

A cross border fee is the fee charged to a merchant when a customer uses a credit card as payment for purchases or services from an issuing bank not located in the same country as the merchant's processing account. Since 2005, MasterCard and Visa have made the cross-border fee applicable whenever a merchant accepts an international credit card for payment. This fee is charged by the issuing bank and passed on to the merchant as an assessment for the use of the international credit card processing network--whether or not there is a need for currency conversion to complete the transaction. The adoption of chip cards should not have any bearing on cross-border fees.

NFC

WHAT IS THE CONNECTION BETWEEN EMV ADOPTION AND NEAR FIELD COMMUNICATIONS (NFC) MOBILE PAYMENTS?

NFC is the two-way communications between a smart phone and a smart terminal. NFC-enabled mobile devices are used to accept mobile contactless payments, as well as for other mobile applications, like mobile couponing and loyalty programs. Migrating to a contactless EMV-enabled point-of-sale platform opens doors for building a future-proof payment acceptance infrastructure that supports NFC. 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 spur the launch of NFC mobile contactless payments in Europe and Canada, where an EMV-based payments infrastructure is already in place. Verifone believes the same will happen in the U.S.

CAN CONSUMERS OBTAIN RECEIPTS FOR NFC TRANSACTIONS?

Contrary to what some may assume, yes. Existing technology allows merchants to send digital receipts for NFC transactions to customers' smartphones. Customers can also request paper receipts at the point of sale.

TIP ADJUST

IS IT TRUE THAT IT IS IMPOSSIBLE TO ADJUST TIPS ON RESTAURANT PAYMENTS MADE WITH CHIP CARDS, AND THAT THIS IS A SECURITY FEATURE OF THESE CARDS?

No. However acquirers are implementing this functionality differently so check with your acquirer on specifics.

WHAT SPECIAL ADJUSTMENTS IN POINT-OF-SALE TECHNOLOGY MUST RESTAURANTS MAKE IN ORDER TO BE EMV-COMPLIANT?

Restaurants that allow customers the option of paying at the table, rather than bringing the check, will need to make some adjustments. If the customer has a chip card, it will not be feasible to allow servers to walk away with it as has been done in the past. To be compliant, restaurant owners will need to upgrade to chip card enabled wireless, Bluetooth or mobile/tablet POS applications to provide “pay at the table” processing solutions.

DOES THE AMOUNT THAT IS REQUIRED BEFORE THE CARD IS INSERTED NEED TO BE THE FINAL TRANSACTION AMOUNT TO THE CARDHOLDER’S ACCOUNT?

Different merchant category codes have different requirements. The merchant should follow interchange qualification rules as they do with mag-stripe today.

DOES THE CARD NEED TO BE PRESENT WHEN THE SECOND TRANSACTION (AS AN EXAMPLE, FOR TIP ENTRY) IS PROCESSED?

The cardholder validation method (verifying the CVM) is a different process than authorizing the transaction. An EMV transaction includes CVM and transaction authorization. Therefore, the card does not need to be present for tip adjust (just as today with mag-stripe); the cardholder is already verified in the initial transaction.

DO THE EMVCO SPECIFICATIONS ALLOW TRANSACTIONS TO BE ADJUSTED?

EMVCo is silent on this U.S. requirement.

MUST RESTAURANTS THAT ACCEPT CHIP CARD PAYMENTS ABANDON OR OPT NOT TO DEPLOY “PAY AT THE TABLE” TECHNOLOGY, AND ONLY ACCEPT PAYMENTS AT THE FRONT COUNTER, AS IS THE CASE WITH THE DENNY’S RESTAURANT CHAIN?

Restaurants can opt to deploy any payment methods that they desire to run their business.

WHY DO SOME VERIFONE APPLICATIONS NOT SUPPORT TIP ADJUST?

Verifone follows acquirer processor requirements for tip adjust and many other functions for both EMV and non-EMV transactions. The acquirer owns the liability for the merchant account and Verifone certifies each application according to their specifications and needs.

IS IT TRUE THAT IF A MERCHANT IS SET FOR ONLINE PIN AS THE PRIMARY CVM (CARDHOLDER VERIFICATION METHOD), TIP ADJUST IS NOT ALLOWED?

Similarly to a debit PIN transaction, where the PIN is entered and sent to the issuer for approval, some acquirer processors may not allow the tip to be adjusted. Please check with your acquirer processor for specifics.

QUESTIONS & ANSWERS

APPLE PAY

WHY DO CARD NUMBERS CHANGE DURING APPLE PAY CONTACTLESS TRANSACTIONS?

Card numbers do not actually change during these transactions. When a consumer first signs up for Apple Pay, the card information is immediately encrypted and securely sent to the appropriate credit card network. Once the validity of the account has been determined, a token that is used in place of the actual credit card number is transmitted back to the point-of-sale device and stored in the Secure Element of the mobile device on which Apple Pay has been installed. Apple refers to this as a unique Device Account Number.

HOW DOES APPLE PAY WORK WITHIN THE CONTEXT OF EMV?

Apple Pay is based on near-field communication (NFC) technology for proximity payments and a secure element. It leverages industry-standard contactless EMV protocols over NFC (it is, however, also compatible with non-EMV mag-stripe-based contactless emulation.) Apple Pay is compliant with the EMVCo tokenization framework and works with a tokenized primary account number (PAN) and transaction-specific dynamic security code, or cryptogram. The PAN is never stored on the user's device or passed to the point of sale terminal, ensuring security.

IS A PARTICULAR APP NEEDED TO ENABLE APPLE PAY TO WORK ON VERIFONE POINT-OF-SALE DEVICES?

No, a specific application is not required. Apple Pay harnesses standard MasterCard, Visa, American Express and soon Discover applications.

DOES AN APPLE PAY TRANSACTION QUALIFY AS A CARD-PRESENT TRANSACTION?

An Apple Pay transaction completed in-store is considered a card-present transaction. However, in-app transactions do not fall into the same category.

DEVICES / PRODUCT-RELATED

DOES A CASH ADVANCE DEVICE NEED TO HAVE EMV CAPABILITY TO QUALIFY FOR THE CARD NETWORK/BRAND INCENTIVES?

Yes.

WHY DO SOME VERIFONE APPLICATIONS NOT SUPPORT TIP ADJUST?

Verifone follows acquirer processor requirements for tip adjust and many other functions.

HOW DO CHIP CARD TRANSACTIONS INITIATED ON TERMINALS WITH DIAL-UP CONNECTIONS, SPECIFICALLY THE VX 520, WORK? WILL PROCESSING THESE TRANSACTIONS TAKE LONGER THAN PROCESSING TRANSACTIONS USING IP CONNECTIVITY?

Chip card transactions initiated on terminals with dial-up connections, such as the EMV-compliant Verifone VX 520, are completed in the same manner as chip card transactions initiated on terminals with IP connectivity (which the VX 520 also supports). Transaction authorization takes a bit longer when dial-up mode is used and one to two seconds when IP mode is used.

HOW WILL EMV WORK ON MOBILE POINT-OF SALE-DEVICES USED IN-STORE?

The process will be the same as for stationary terminals, with the chip card inserted into a slot in the device to start the card verification process and left there until the transaction has been completed. In a contactless mobile transaction, the customer holds his or her smartphone to a payment terminal and awaits payment confirmation.

IS VERIFONE'S E335 MOBILE POINT-OF-SALE (MPOS) PAYMENT TERMINAL AN EMV-ENABLED OPTION?

Yes. The e335, which pairs with the Apple® iPad® mini and leverages the high-speed Apple Lightning™ connector for rapid transaction completion, processes payments made with EMV-enabled chip and PIN cards. It also supports payments made with mag-stripe cards and NFC/contactless payment acceptance technology. This device features a built-in PIN pad and 2-D laser barcode imager.

CAN POINT-OF-SALE TERMINALS WITH NEAR FIELD COMMUNICATIONS (NFC) CAPABILITIES PROCESS CONTACTLESS CHIP CARD TRANSACTIONS?

Yes.

WHAT IS THE ADVANTAGE OF VERIFONE'S VERISHIELD TOTAL PROTECT WITHIN THE CONTEXT OF EMV?

VeriShield Total Protect provides an extra layer of data protection that is not afforded by EMV. For example, EMV'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, rendering 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, before completing a transaction. VeriShield Total Protect combines best-of-breed tokenization and encryption technologies, in essence picking up where EMV leaves off and eliminating useable cardholder data from point-of-sale applications, networks and servers.

HAVE VERIFONE'S MX 800 SERIES TERMINALS FOR THE PETROLEUM AND CONVENIENCE MARKETS RECEIVED LEVEL 1 AND LEVEL 2 APPROVAL FROM EMVCO?

Yes. All four options in the MX 800 series: the full-color MX 850, wide-screen MX 860, full-screen MX 870 and the MX 880, which has a full touchscreen and keypad, also meet all global security requirements and have PCI PED (PIN entry device) 2.0 approval.

DOES THE VERIFONE MX 915 PIN PAD ACCOMMODATE CHIP CARDS, OR WILL IT REQUIRE MODIFICATION FIRST?

The MX 915 PIN pad, which offers a space-saving form factor, is configured to support chip and PIN payments. It is also NFC-integrated to capitalize on the coming wave of NFC (near-field communications) payments.

HOW CAN MERCHANTS OBTAIN LEVEL 1 AND LEVEL 2 LETTERS OF CERTIFICATION FROM EMVCO FOR THE VERIFONE VX AND MX DEVICES?

Most merchants don't need these letters; vendors and solution providers do. Merchants need only ensure that the EMV-capable technology they deploy has been certified by EMVCo, which administers the EMV standard, as well as by the card brand(s) accepted at their locations. However, EMVCo includes a listing of certified devices on their website. Letters can be obtained from your Verifone representative if they are required by the acquirer.

CAN VERIFONE VX 805 AND VERIFONE VX 820 PIN PADS BE CONNECTED TO THE VX 510 DUAL COMM AND THE VX 570 DUAL COMM COUNTERTOP UNITS TO ALLOW FOR COMPLIANCE WITH THE EMV STANDARD?

All four of these devices have already received EMV Level 1 and EMV Level 2 approval from EMVCo. Please check with your acquirer for certification of these devices.

QUESTIONS & ANSWERS

MUST CONVENIENCE STORES DEPLOY LOCKING STANDS AS PART OF THEIR COMPLIANCE WITH THE EMV STANDARD?

No. The only thing they must do is to migrate to new point-of-sale technology so that it accommodates transactions completed with chip cards, or upgrade their existing technology to enable it to do so. Like other merchants, convenience store operators must, in order to comply with the EMV standard and therefore remain free from liability for fraudulent card-present transactions, make either type of change by October 1, 2015. Convenience store operators with a petroleum component do have until October of 2017 to transition the card readers on automatic fuel dispensers to EMV-capable mode.

WHICH PARTICULAR VERIFONE PRODUCTS SUPPORT APPLE PAY?

All contactless-enabled Verifone products can be used to accept payments via Apple Pay.

DOES VERIFONE'S MX 860 HARDWARE SUPPORT CONTACTLESS TRANSACTIONS?

Yes. The MX 860, which features a 480x272 wide screen color display and full-motion video, does handle contactless chip card transactions.

WHICH TERMINALS ARE EMV-ENABLED?

Please visit the Verifone Zone www.verifonezone.com and view the latest certification/approval matrix for processor approvals by device type. Visit verifone.com for other industry and country specific items.

CASHBACK helios® automated simplicity