PETRO POS

WHEN DO I NEED TO BE EMV COMPLIANT?

Petroleum pay at pump merchants must support EMV by October 2017 however in-store transactions must have been enabled for EMV by October 2015.

WHAT TYPE OF PIN PAD DO I NEED FOR EMV TRANSACTIONS?

You will need a PIN pad that has an EMV reader installed. The MX915 and MX925 PIN pads come with a built in EMV reader. For the MX800 series product line (MX880, 870,860, and 850) you will need an EMV reader attached. Contact your service contractor if you need to upgrade your existing hardware.

I HAVE A SUPPORTED PIN PAD - DOES IT NEED TO HAVE NEW SOFTWARE LOADED TO IT?

Yes. The software loaded on both the MX900 series and MX800 series PIN pads must be loaded with EMV enabled software.

WILL I NEED TO UPGRADE MY POS SOFTWARE TO WORK WITH EMV?

Yes. The POS software must be on a software version that supports EMV. A software upgrade may be possible through Verifone's Remote Software Delivery (VRSD) feature. If you wish to learn more about VRSD navigate to the support.verifone.com website > Petro & Convenience> Product Pages – Verifone Remote Software Delivery.

ONCE THE SOFTWARE IS INSTALLED ON MY POS, WHAT IS NEEDED FOR CONFIGURATION?

Configuration of EMV will be made available via Configuration Client or Sapphire Configuration Manager, depending upon your POS site controller. Parameters for enabling EMV will be in the Payment Controller section.

DO I NEED TO CONTACT MY FRONT END PROCESSOR (FEP) TO ENABLE THIS FEATURE?

If you are using the Buypass network for processing cards it will be necessary for you to contact your processor for additional information on EMV setup prior to performing the update. No other card processing networks require this at this time.

WILL THE OPERATIONS ON THE POS CHANGE WHEN A CASHIER RINGS UP A CREDIT OR DEBIT SALE?

No. The process of selecting the MOP for credit or debit will be the same on the POS.

HOW WILL THE TRANSACTION BE DIFFERENT FOR THE CUSTOMER?

The customer will be prompted to slide their card or insert the card into the EMV reader. If their card is enabled for EMV, then they will be prompted to insert their card if they attempt to use the mag stripe reader. Once they insert the card into the reader, it must remain inserted until they are prompted to "Remove Card." While their card is inserted into the reader they will be prompted on the PIN pad to select credit/debit, approve amount, sign for the transaction, and/or enter a PIN.

HOW DOES THE PIN PAD KNOW THE CUSTOMER NEEDS TO INSERT THEIR CARD?

The type of card determines if the PIN pad will prompt for the customer to use the EMV reader. The PIN pad simply reads the cards data to determine if it's an EMV card or not.

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.

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").

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.

WHAT IS "NO CVM"?

No CVM is a cardholder verification method that requires no verification from the consumer.

CAN AN EMV CARD BE CREDIT OR DEBIT?

Yes an EMV card can be issued as either credit or debit. The card will continue to have on its face the "credit" or "debit" designation.

HOW ARE CHARGEBACKS AFFECTED BY EMV?

Chargebacks should lessen with EMV because counterfeit fraud is reduced. Other chargeback reasons will continue.

DOES A DEVICE HAVE TO HAVE A PCI PTS-APPROVED PIN PAD TO ACCEPT A CVM THAT IS PIN PREFERRING?

Yes. A PCI PTS-approved PIN Pad is required for any PIN entry for EMV.

WHAT IS FALLBACK?

As defined by EMVCo and the payment networks, fallback should only occur when the terminal cannot read the card's chip due to technical issues with the chip. Any other scenario is not a fallback transaction. If a merchant is using a phased approach to EMV deployment and the merchant chooses to override the chip service code on the card, then (pursuant to EMVCo specifications and/or payment network rules) the terminal must reflect the terminal entry capability as mag-stripe only. Failure to do so will result in the transaction being incorrectly flagged as fallback.

LIABILITY & SECURITY

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

No, the liability will be the issuer's.

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.

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 requirement.

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.

CAN THE CONSUMER INSERT THEIR CARD BEFORE THE AMOUNT IS KNOWN?

Yes, the consumer can insert their card at any time before the amount is entered and processing of the card begins.

CAN AN EMV CARD BE CHANGED VIA SCRIPTING AT THE POS?

Yes, if the issuer and issuer processor support it, the card can be updated via scripts sent online to the POS from the issuer.

DOES THE TERMINAL STILL REQUIRE BIN MANAGEMENT?

The terminal application continues to use BIN management to assign a card type to the transaction.

WHAT ARE THE COMMON APPLICATION ERROR MESSAGES FOR AN EMV TRANSACTION?

Here are five common error messages:

1. CHIP CARD ERROR

The chip on the card is unable to be read. The card may not be inserted all the way – ask the cardholder to push the card into the device until it "clicks". If a card cannot be read, please contact your merchant services provider for assistance.

2. CARD NOT SUPPORTED

The card type is not supported in the application. Contact your merchant services provider for assistance.

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."

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.

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.

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.

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.