First Data
b›yond the transaction

A First Data White Paper

EMV and Encryption + Tokenization: A Layered Approach to Security

Introduction

Several card brands have taken the position that EMV is the preferred way forward for reducing payment card fraud at the point of sale (POS) in the United States. EMV is already an accepted standard in every major market except the U.S., and it has proven its worth in other regions. In the U.K., for example, payment card fraud losses reached a 10-year low in 2011, and experts credit this achievement largely to the use of "Chip and PIN," a form of EMV-enabled card authentication.[1] Other regions that have implemented EMV have experienced similar results.

Recognizing the positive outcomes elsewhere, Visa and MasterCard have announced EMV initiatives in the U.S., with requirements and deadlines that affect merchants, issuers, acquirers/processors, and ATM operators.

Visa, for example, is encouraging U.S. merchants to accept EMV-enabled transactions by offering an incentive: merchants that process at least 75 percent of their Visa transactions in any given year through EMV-enabled POS terminals that support both contact and contactless cards will be exempt from validating PCI compliance that year.[2] (Note that merchants are still required to adhere to all PCI Data Security Standards (DSS) to protect sensitive data, and this has implications beyond EMV which we discuss below.)

Visa also is enacting a fraud liability shift that will affect most merchants beginning October 1, 2015.[3] If a contact chip card is presented to a merchant that has not adopted, at minimum, contact chip terminals, then liability for counterfeit fraud may shift from the card issuer to the merchant's acquirer.

MasterCard, too, has initiatives to promote EMV adoption by both merchants and card issuers. In alignment with Visa's date of October 2015, MasterCard plans to shift liability to merchants who have not upgraded their POS terminals to process transactions made with EMV cards if a customer pays with such a card and fraud occurs.

In light of these developments, merchants need to understand the business and security implications of moving to the EMV standard, as well as what EMV will—and won't—do to help merchants. While EMV is a global standard that is proven to reduce card fraud, it isn't the all-encompassing security remedy that the payments industry would like to have. Additional layered safeguards are still needed—in particular for data security beyond the POS, and also for eCommerce and other card-not-present (CNP) situations.

The goal of this paper is to explain where EMV fits into the payments security spectrum and to highlight the additional measures that provide security where EMV does not.

[1] Financial Fraud Action UK, "UK payment card fraud drops to 10-year low," 7 March 2012
[2] Find Visa's full announcement regarding EMV implementation at http://corporate.visa.com/media-center/press-releases/press1142.jsp.
[3] Fuel-selling merchants will have an additional two years, until October 1, 2017, before a liability shift takes effect for transactions generated from automated fuel dispensers.

What is EMV?

EMV is the technical interoperability standard that ensures chip-based payment cards and terminals are compatible around the world. The term refers to *E*uropay, *M*asterCard and *V*isa, the three companies that originally developed the specifications in 1994. Today the EMV standard is managed by EMVCo LLC, which is equally owned by American Express, JCB, MasterCard and Visa.

A chip-based payment transaction occurs when a microprocessor (smart chip) embedded in a plastic card or a personal device such as a key fob or mobile phone connects to an EMV-enabled POS terminal. The terminal can be either contact or contactless; many POS machines have both. The smart chip in the payment instrument securely stores information about the cardholder's account and the issuer's payment application, and it performs cryptographic processing for validating the integrity of the card number and certain static and dynamic data used in the transaction. This provides a strong form of card authentication, validating the legitimacy of the payment type being used.

EMV employs either a signature or an offline PIN to authenticate the cardholder. In a "Chip and PIN" environment, the user of the card enters a PIN to the POS terminal rather than using a signature to complete the transaction. The PIN entered by the cardholder is validated against either the PIN stored on the chip or at the processor to ensure that the card is not being used by an unauthorized party. While many geographical regions use a "Chip and PIN" version of EMV, there is an ongoing debate about whether a "Chip and Signature" implementation is acceptable—at least initially—for the U.S. market.

For a more detailed explanation of EMV, please read EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions.

EMV benefits for card fraud protection

Undoubtedly, a combination of card number validation via the chip and authentication of the user via PIN provides stronger protection against common consumer-level attacks such as fraudulent use of lost or stolen cards, counterfeit cards and skimming (whereby the magnetic stripe of a card is read without the consumer's knowledge). In an "online authorization" environment, EMV enhances the security of the payment transaction by attaching a dynamic cryptogram to each authorization and clearing transaction. This offers some protection against tampering of card and POS data during transaction processing. You can think of this as a unique password for the card that is only good for a single use. A separate process called Offline Data Authentication provides security against skimming and counterfeiting for a merchant performing a card transaction without an online issuer host data connection (commonly referred to as an "offline transaction"), a common authorization process outside of the U.S.

The primary motivation for implementation of EMV by some of the networks and issuers is the belief that it is fundamentally more resistant to fraud than magnetic stripe cards. Given that the U.S. market is the largest market in the world for the use of payment cards, as well as the only major payment market that has either not implemented or begun rolling out EMV, the potential to reduce fraud in the U.S. system is appealing.

However, it is possible for a card issued from an EMV-enabled country to be used fraudulently where EMV is not supported. In the most common scenario, a card number from an EMV card is counterfeited onto a magnetic stripe

card and used either in a country that doesn't have EMV terminals (such as the United States) or in a card-not-present environment (such as an eCommerce website). Enabling EMV within the U.S. market would further narrow the places where "card transplant" fraud can occur.

Additionally, the increased security and authentication measures in the EMV system provide the basis for a liability shift in the payments process. In the current U.S. market model, the issuing banks usually bear the overwhelming majority of costs associated with payment card fraud. The consumer and merchant are typically not held responsible for fraudulent transactions. In most EMV-enabled countries, the consumer is often held liable for a fraudulent transaction unless it can be proved he/she was not present for the transaction, did not authorize the transaction, and did not inadvertently assist the transaction through accidental PIN disclosure. Further, EMV deployments in other parts of the world have shown precedent for holding merchants liable for any fraud that occurs on systems that are not EMV capable. The combination of reduced fraud and externalizing the costs associated with fraud make EMV an attractive proposition for issuing banks and card brands.

For merchants, the use of chip-enabled cards means greater security and more streamlined processing, especially when chip is combined with PIN authentication, which can reduce fraud. Merchants are likely to experience other benefits as well, including fewer chargebacks, increased opportunity for self-service and portable POS stations, marketing opportunities tied to mobile payments, more streamlined check-out with contactless "tap and go" payments, and loyalty program applications integrated onto the smart chips of merchant-specific payment devices. Merchants should explore all the potential opportunities that smart cards enable beyond security at the POS.

Vulnerabilities that EMV doesn't address (or may make worse)

EMV represents vast improvements over the basic security that is inherent to the decades-old legacy technology of magnetic stripe cards, but is fundamentally designed as an authentication technology rather than a data security technology. Accordingly, the implementation of EMV alone does not protect the entire payment transaction process.

In particular, there are key areas of vulnerability in the payments process that EMV alone does not address:

1. From the point of card insertion or tap, when the card data is transmitted in the clear to the processor or is later stored by the merchant post-authorization
2. Other transactions where a chip-enabled card is not present

Let's have a look at each of these issues.

Card data security during and after the transaction process

The singular focus on card-level fraud leaves a key gap in today's EMV implementations. EMV does not address merchant-specific risks such as the interception of card numbers in transmission on the merchant network or attacks against repositories of card information within the merchant, acquirer, processor, network or issuer environment. The PCI Security Standards Council notes: "in EMV environments, the PAN [primary account number] is not kept confidential at any point in the transaction."[4] The largest breaches of card information in the U.S. have come from vulnerabilities within the merchant or processor environment that EMV does not address.

Currently, in the majority of both EMV and non-EMV transactions, payment card information is sent from the point-of-capture to the acquirer/processor "in the clear," i.e., in an unencrypted form. Historically, when the majority of transactions traversed private phone lines, this was less problematic. However, as more and more terminals and point-of-sale systems have begun using Internet technology for data transmission, the ability to capture that data "in flight" has been exploited by criminals to steal millions of card numbers from unsuspecting merchants. While a dynamic cryptogram provides some level of protection, the payment card information still travels in the clear and could theoretically be counterfeited onto a magnetic stripe or used in a card-not-present environment. The primary method of eliminating this form of attack is to encrypt the payment card information at the point-of-capture, rendering the data unusable to thieves.

Another key point of exposure is that many merchants retain payment card data after the transaction in long-term data stores. Small merchants hold hundreds of card numbers on their terminals or in their point-of-sale systems. Large retailers have data warehouses containing hundreds of millions of card numbers that they use for marketing and analysis of customer purchasing behavior. The massive volume and value of this information makes these data stores a prime target for criminals.

eCommerce and other CNP fraud

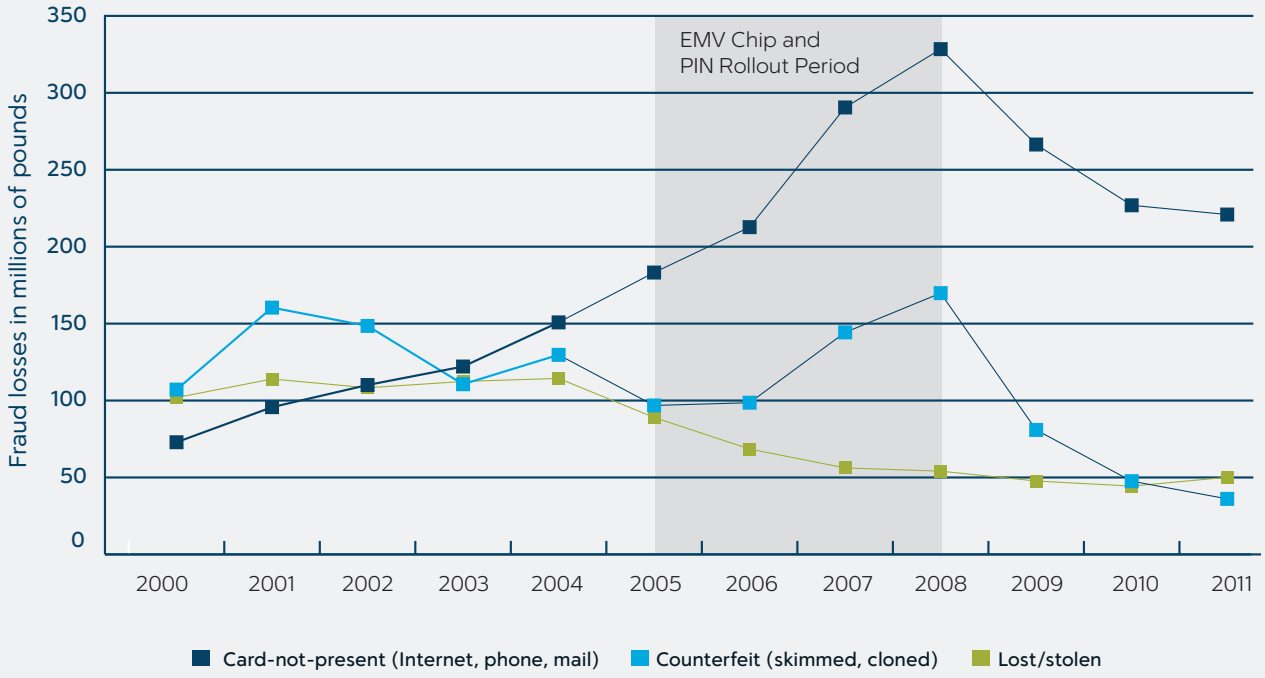
The simplest method for circumventing EMV is to use a stolen card number in a place where EMV validation does not occur, such as in an eCommerce transaction.

EMV is designed for instances where a payment instrument is presented in person. Recall from the definition of EMV above that the smart chip in the card (or fob or phone) must *connect* with a reader in the POS terminal. The connection can either be physical (i.e., touching) or wireless using near-field communication (NFC) technology over distances of mere inches. As a result, EMV does not address the fraudulent use of payment data when there is no direct connection, such as when the data is entered into an eCommerce application or given over the phone or through the mail—in other words, card-not-present situations.

In fact, EMV rollouts in other countries have shown that CNP fraud tends to increase, at least initially, when smart card implementations drive criminals away from the physical terminals and toward CNP uses. This was the case in the UK, which experienced an increase in CNP fraud during the time (2005 to 2008) that EMV Chip and PIN was rolling out throughout the country. CNP fraud began declining again once stringent fraud detection measures were implemented for the CNP channels. (See Figure 1 and Table 1 on the following page.)

[4] PCI Security Standards Council, "PCI DSS Applicability in an EMV Environment, A Guidance Document, Version 1," 5 October 2010

FIGURE 1: ANNUAL FRAUD LOSSES ON UK-ISSUED CARDS 1999 TO 2010



Source: The UK Cards Association, 2012

TABLE 1: ANNUAL FRAUD LOSSES ON UK-ISSUED CARDS 1999 TO 2010 IN MILLIONS OF POUNDS (£)

Fraud type	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
CNP	72.9	95.7	110.1	122.1	150.8	183.2	212.7	290.5	328.4	266.4	226.9	220.9
Counterfeit	107.1	160.4	148.5	110.6	129.7	96.8	98.6	144.3	169.8	80.9	47.6	36.1
Lost/stolen	101.9	114.0	108.3	112.4	114.4	89.0	68.5	56.2	54.1	47.7	44.4	50.1

Source: The UK Cards Association, 2012

Encryption + Tokenization provides card data security

While EMV primarily focuses on card fraud at the consumer level or in the consumer-merchant exchange, the dual technology solution of encryption + tokenization taken together solves for many of the other data security problems specific to the merchant community.

First encrypt...

Anytime that live cardholder data is in the clear, it is extremely vulnerable to theft. Of course, cyber thieves know this and they look for ways to grab a copy of that data for nefarious use. For example, it's possible for a thief to siphon off the card data as it is transmitted in plain text from a card reader to the POS server or the merchant's central server. (This is what is believed to have happened in data breaches involving Hannaford Bros., TJX and the Dave & Buster's restaurant chain.)

The first leg of the data security solution, encryption, protects card data from the point-of-capture and maintains this protective state throughout the transaction. Encryption is the process of using algorithmic schemes to transform plain text information (i.e., the PAN) into a non-readable form called ciphertext. A key (or algorithm) is required to decrypt (or unencrypt) the information and return it to its original plain text format.

The point-of-capture can be the swipe of a magstripe card; the insertion, tap or wave of a chip-enabled card or other payment instrument; or the manual entry of data into a terminal (such as when a sales clerk types the account number) or into a web-based form (such as for eCommerce). Once encrypted, any data that may be intercepted within the merchant's POS system or during transmission to the acquirer/processor cannot be used without the master key, which itself is safely stored in the processor's vault.

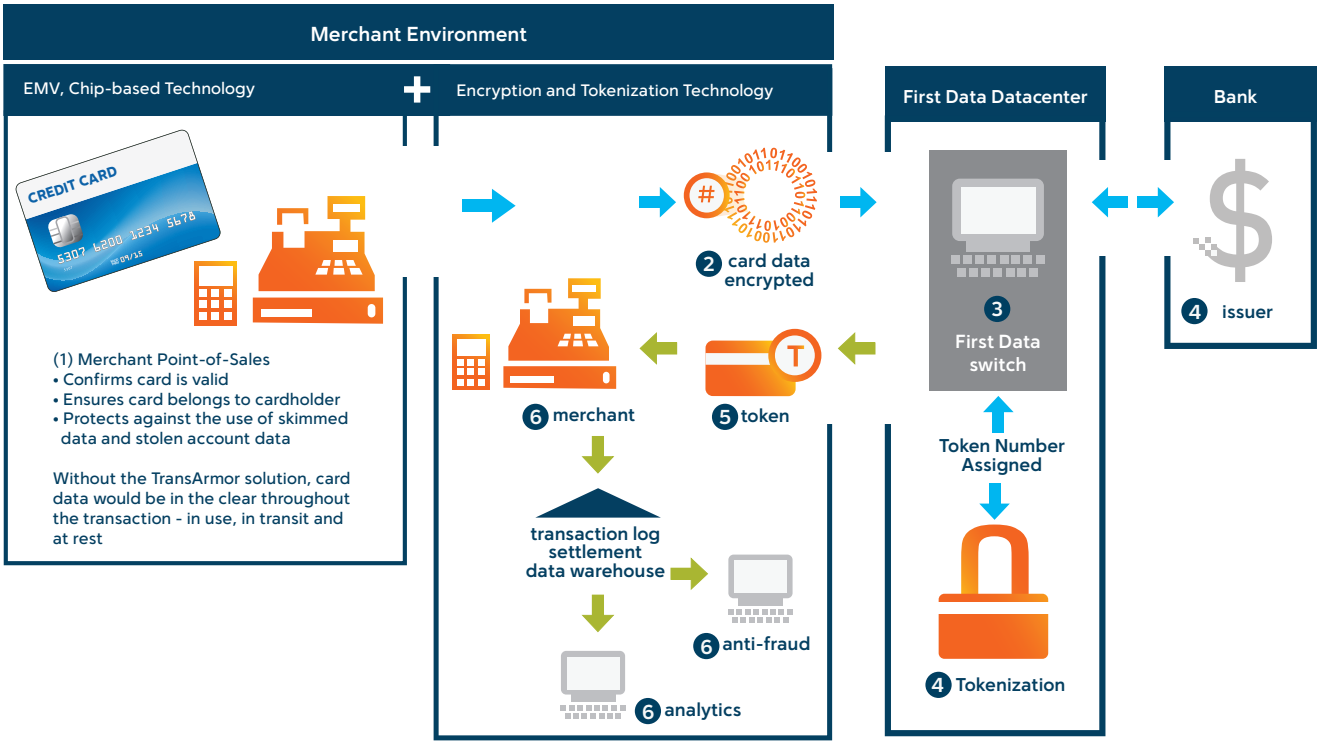
Encryption of either the data itself or the transmission path the data takes along the network, or both, can vastly reduce the vulnerability of the data, which in turn reduces a merchant's business risks.

...then tokenize

The second component of the solution, tokenization, returns a "token" to the merchant in lieu of the live credit card number in the authorization response. Tokenization is the process of replacing sensitive data with surrogate values that remove risk but preserve value to the business. To tokenize a payment transaction, the PAN is sent to a centralized and highly secure server called a "vault" where it is stored securely in a PCI-compliant environment. Immediately after authorization from the card issuer, a random, unique, token number is generated and returned to the merchant's systems for use in place of the PAN. A secure cross-reference table is established to allow authorized look-up of the original PAN, using the token as the index. Without authorization to access the vault and look up the PAN, the token value is meaningless; it's just a random number. If the token is stolen or otherwise accessed by an unauthorized user, it alone cannot be used to perform a monetary transaction.

The token can be used just like the original card number for business functions such as returns, sales reports, marketing analysis, recurring payments, and so on, but cannot be used to conduct a fraudulent transaction outside the merchant environment. The aim of tokenization is to remove the card information from the merchant environment as completely and quickly as possible (thus addressing the root cause of data security issues) while maintaining existing business processes.

FIGURE 2: HOW DOES A LAYERED SECURITY SOLUTION WORK? EMV + TRANSARMOR



1. EMV card is presented to merchant and is inserted or tapped / waved
   - Card and cardholder are validated
   - Card data sent in the clear without the TransArmor solution
2. PAN is encrypted using session encryption and sent to First Data
3. Encrypted session is received at First Data datacenter
4. Card number is passed to bank for authorization and SafeProxy server for tokenization
5. Authorization and Multi-Pay Token are returned to the merchant
6. Multi-Pay Token is stored in place of the card number in all places
7. New financial transactions including sales, adjustments, refunds and settlement use the Multi-Pay Token instead of the PAN

For more information about using encryption + tokenization solutions together, read What Thieves Don't Want You to Know: The Facts About Encryption and Tokenization.

Multi-pay tokens further reduce merchant risk

The original concept of the token meant that the merchant could not use this random number to perform a subsequent financial transaction because it is not a valid PAN. However, a multi-pay token adds the ability to perform an authorized financial transaction under strict control measures within the merchant environment. The merchant submits a token that it already has on file for a specific consumer/card to a processor with access to the vault to retrieve the PAN and complete the transaction. By using this kind of recurring token in the payment authorization process, the merchant reduces the risk of having the real PAN stolen as it is being collected from the consumer or stored by the merchant.

Multi-pay tokens are especially valuable in eCommerce and other CNP environments that tend to store payment card information in a wallet or on their website for repeat customers. The multi-pay token allows a merchant to tokenize the payment card information, associate that token with the consumer profile stored on the merchant side, and then use the token with the processor gateway that holds the token vault in order to run subsequent transactions. This is done without the need to prompt the customer for his card account number again, and without having to store the actual card number.

The merchant's initial transaction with the consumer's payment card uses the real account data, but for all subsequent transactions (for example, to process refunds and credits) that use the same payment card, the merchant can use the token instead. A multi-pay token is unique to a specific card used with a specific merchant. This ensures that one and only one authorized merchant can ever use the token to process subsequent transactions. Merchants can further defend against CNP fraud by combining the use of multi-pay tokens with a hosted payment page. This removes the need for merchants to capture card data within their environment, minimizing the risk of card data being stolen (which has the further impact of reducing the number of stolen cards in circulation).

Multi-pay tokens are also especially effective in bringing the online world together with the brick and mortar world. First Data's TransArmor multi-pay tokens, for instance, return the same token for the same card, regardless of the method of entry (card not present or card present). This is a powerful differentiator from gateway-based tokenization systems that cannot extend the tokens beyond the gateway, or associate those online transactions with transactions happening in the merchant retail locations.

For more information about multi-pay tokens, read Tokenization and eCommerce: Using Multi-Pay Tokens to Reduce Security Risks and PCI Costs.

Tokens replace legacy data in storage

Beyond encrypting and tokenizing data for transactions at the point-of-sale, merchants also need to consider the risk of stored primary account numbers (PANs) in their card data environment (CDE). To help prevent potential breaches and reduce PCI scope and maintenance costs, merchants need to completely remove legacy or stored PAN data from the CDE and replace it with tokens. The tokens can then be used to perform customer analytics and understand consumer buying behavior. What's more, replacing PAN data with tokens reduces a merchant's burden of PCI compliance by taking sensitive data out of the CDE.

Most tokenization systems are "go forward" only—that is, they can tokenize new transactions but have no capability to tokenize existing cardholder data in the merchant environment. This is another key issue to consider, since merchants have often invested significant time and money in building these valuable repositories of customer history, and understandably seek to maintain and analyze that data in an essentially risk-free manner by replacing the risky cardholder data with multi-pay tokens.

How Encryption + Tokenization fits with EMV

The primary strength of EMV is its ability to perform authentication of the cardholder, which happens to be the primary point of fraud vulnerability in an end-to-end encryption + tokenization solution. At the point of sale, cardholder verification and issuer authentication begin at the issuer, through card personalization--even before the consumer presents the card to a merchant POS. This expands the scope of end-to-end security to include the card itself.

The security capabilities of an encryption + tokenization solution are complementary to those delivered by EMV and are relevant to merchants regardless of a potential future EMV adoption. The need for additional protection is echoed by the PCI Security Standards Council, which states: "native EMV transaction data requires protection beyond what is inherently provided by EMV itself."

With an integrated encryption + tokenization solution, a software-based implementation of encryption can be installed on the majority of PCI-compliant terminals or point-of-sale systems to protect card data in transit. The payment card information can be encrypted at the point-of-capture for secure transmission without the need for replacing existing hardware. For merchants concerned with making a capital investment that might be rendered obsolete if EMV becomes required in the U.S., software-based encryption offers the ability to protect one of the weakest points in their environment today without fear of the changes tomorrow might bring. If EMV does become standard in the U.S., merchants will be able to continue to use the encryption on the EMV-compatible terminals that they deploy, and tokenized data-at-rest will continue to secure data warehouses and storage devices.

The value of tokenizing payment data-at-rest in the merchant, acquirer, network and issuer environments cannot be overstated, and is relevant regardless of the existence of EMV-based security controls. A card-based tokenization solution offers merchants the ability to purge their entire environment of payment card information while still supporting existing business processes such as returns, recurring billing, and customer analytics. The merchant loses nothing except the risk associated with keeping the card data that had previously powered those processes.

Combating Online Fraud: Tools for Detecting and Preventing Fraudulent Transactions

Although the United States is one of the last remaining G20 countries to adopt EMV, this market has the benefit of learning from other regions' experience implementing the technology. Global experience has demonstrated that EMV chip technology is effective at reducing fraud at the POS but can also drive higher CNP fraud. Along with bringing in EMV at the POS and securing card data with encryption + tokenization, merchants need to address the issue of card-not-present fraud strategically, with additional security layers such as fraud protection solutions and increased verification methods. With the right tools and technologies, merchants can apply these strategies to safely conduct business online without simply accepting fraud as a "cost of doing business."

Merchants of all sizes are susceptible to online fraud. Fortunately, powerful tools and technologies for fraud management are now available and affordable for all. Address Verification Service (AVS) and Card Verification Value 2 (CVV2) are two

simple and common ways to verify the legitimacy of cardholders and cards in CNP situations. MasterCard Secure Code and Verified By Visa are other fraud prevention tools that are available, as well as sophisticated fraud management solutions that allow merchants to implement multiple functions within their business to help reduce CNP fraud, including:

- **Automated transactional risk scoring**, which involves calculating the potential fraud risk of a transaction based on multiple data factors. The calculated score serves as a relative risk indicator and determines "next steps" for that transaction according to a merchant's preferred operating procedures.
- **Real-time categorizing and resolution** places transactions with risk scores exceeding certain thresholds into different categories for further action. Solutions that operate in-line with the payment authorization flow require minimal intervention by the merchant and streamline business processes.
- **Post-purchase transaction management** solutions allow merchants to review and analyze the transactions that fall between the "accept" and "reject" thresholds. This helps the merchant to resolve chargebacks and disputes efficiently as well as understand transaction trending over an extended period of time.
- **Adjustments to fraud rules and parameters** are useful because fraud trends evolve rapidly and detection tools need an equally quick response to remain effective. The anti-fraud tools should be referenced against reports and analytics on a regular basis, and merchant staff should be trained to react to immediate critical occurrences, such as a sudden attack from a fraud ring in a particular geographical location. These may require significant but temporary changes to the existing fraud settings.

By integrating these fraud management tools into checkout processes, any sized eCommerce business can become more empowered to fight fraud—and fraud management thereby becomes an intuitive, practical, controllable business process.

For more information about combating eCommerce fraud, please see Strategies for Reducing the Risk of eCommerce Fraud.

Conclusion

Merchants are a primary target for criminals intent on stealing payment card information. Regardless of the possible future implementation of EMV, there remains an immediate need for increased security in the merchant community. There are viable solutions available today that enhance security and reduce fraud risk in our payment systems. These solutions can be implemented independently of EMV today, and should be utilized in combination with EMV when it becomes standard.

The key learning as it relates to the inherent vulnerabilities in each solution is that there is no magic bullet that solves for every aspect of data security. Layering the various components together is far more effective at thwarting fraud than using any single component individually. When enacted, EMV will solve for fraud at the card and cardholder level. Encryption protects card data in transit from the point-of-capture to authorization. Tokenization protects data-at-rest in post-authorization data stores and applications. And a variety of merchant-level tools and technologies protect against card-not-present fraud. All are needed to preserve the integrity of electronic payments and reduce the vast sums that are lost to payment fraud today.

To learn more, visit firstdata.com or contact your sales representative to schedule an expert evaluation of your current security and compliance situation and needs.

The Global Leader in Electronic Commerce

Around the world every day, First Data makes payment transactions secure, fast and easy for merchants, financial institutions and their customers. We leverage our unparalleled product portfolio and expertise to deliver processing solutions that drive customer revenue and profitability. Whether the payment is by debit or credit, gift card, check or mobile phone, online or at the point of sale, First Data helps you maximize value for your business.

2647