HISCOX

encourage courage®

EMV REFERENCE GUIDE (FAQS)

Matthew Donovan
Product Head
Cyber and Data Risks
Hiscox USA

matthew.donovan@hiscox.com

David Navetta
Co-Chair
Data Protection, Privacy and Cybersecurity Practice
Norton Rose Fulbright

david.navetta@nortonrosefulbright.com

The 2016 Hiscox EMV Reference Guide

This reference guides was compiled with the knowledge of leading experts in cyber liability.

Understanding the new regulations in place concerning credit card liability can help merchants minimize their exposure and the impact of credit card breaches after the 2015 EMV Liability Shift.

Hiscox
Encourage Courage

General Information Concerning EMV

WHAT IS EMV?

EMV is a global standard for secure card-present payment card transactions utilizing microchip technology embedded in debit and credit cards. It gets its name from the companies that originally developed the technology, EuroPay, MasterCard and Visa. The standard is also referred to generally as 'Chip and PIN' or 'Chip and Signature.'

EMV technology has been widely adopted outside of the United States. In fact, the U.S. is one of the few industrialized nations that has not fully transitioned to this technology standard.

What is the difference between a card-present transaction and a card-not-present transaction (CNP)?

Card-present transactions involve the use of a physical card that is presented and read using a physical point-of-sale device. Typically, cardholders must present their card (via swipe if the card has a magnetic stripe and via 'dip' if EMV technology is embedded) at a POS terminal to effectuate the transaction. Prior to October 2015, issuing banks, and not merchants, were generally liable for chargebacks based on card-present transactions arising from counterfeit cards used at a merchant's store.

In contrast, CNP transactions do not involve the use of a physical payment card. To effectuate a CNP transaction, cardholders provide the cardholder data from their payment cards to an interface such as a website shopping cart for online transactions or a call center representative for purchases made over the phone. Merchants, and not issuing banks, are generally liable for chargebacks arising from CNP transactions, but merchants can dispute chargebacks.

How is information typically sorted on a magnetic stripe credit card?

A magnetic stripe may be found on the reverse side of almost all traditional, non-EMV enabled payment cards—and many chip-enabled payment cards as well, at least for now. This magnetic stripe (or magstripe) stores various account details that may be shared with a merchant at the time of sale by swiping the payment card through a magstripe reader, thereby providing the merchant with information necessary for it to verify, process, and complete the transaction. This served as the primary mechanism by which payment card transactions were accomplished prior to the EMV shift. Now, merchants are being incentivized by the payment card brands to process payment card purchases by accessing similar transaction data that is encoded directly onto a microchip embedded into the plastic of newer payment cards enabled with EMV technology.

What information is stored on payment cards and does it vary between traditional, magstripe payment cards versus those with chip-and-pin technology?

Various data elements are required for a merchant to process payment card transactions; these data are necessarily encoded onto all payment cards, along with an assortment of other account details and transaction data that varies across the payment card industry.

In the case of traditional, non-EMV payment cards, multiple data sets, or 'tracks,' may be encoded onto a single magnetic stripe–typically two, known as tracks 1 and 2–which allows for the segmentation of account details and transaction data across the two tracks. There are important distinctions, along with some overlap, between the data elements that are stored on tracks 1 and 2:

TRACK 1

Data includes the primary account number (PAN), the payment card expiration date, the CVV/ CVC2/CVV2/ CID code, and the account holder's first and last name;

TRACK 2

Data also includes the primary account number (PAN), the payment card expiration date, the CVV/ CVC2/CVV2/CID code, but does not include the account holders name.

As to newer payment cards enabled with EMV technology, the same track-1 data elements—save for the CVV code—that are encoded onto the magnetic stripes of traditional (non-EMV) payment cards are also stored on EMV-enabled payment cards, encoded directly onto the card's microchip. It should be noted that many EMV-enabled payment cards still include a traditional magstripe in addition to chip-and-pin technology to accommodate the payment card industry's transition to EMV-compliant technology.

Is there more or less financial exposure associated with the compromise of track 1 versus track 2 data?

The potential financial exposure associated with the compromise of track 2 data and chip-enabled payment card data may be somewhat less severe than where track 1 data is put at risk. This is because most, but not all, of the 47 U.S. states that have enacted breach notification laws define 'personal information' to include an individual's name in addition to some other sensitive data element—payment card details, for example. As such, in most of those states, the breach notification laws will not have been triggered, and the costs inherent to providing individual or substitute notice will not necessarily be incurred. However, data thieves and fraudsters may still use track 2 data to create counterfeit cards and otherwise engage in fraudulent transactions. While notice may not be necessary in most U.S. states, merchants who suffer data breaches affecting track 2 data may still face legal liability.

How does EMV work?

The EMV technology includes a computer chip embedded in each payment card that can store information securely and perform cryptographic processing during a payment transaction. The goal of EMV technology is to decrease the amount of card-present payment card fraud due to counterfeit cards.

Unlike current magnetic stripe cards—where a customer 'swipes' the payment card through the POS device that reads cardholder data off the magnetic stripe—the new EMV technology will require the customer to insert ('dip') the card into a POS terminal so information from the chip can be read during the transaction. The chip provides dynamic authentication information that changes for each transaction, unlike the current magnetic stripe method with static authentication data embedded in the stripe.

As a result, even if the authentication data in a chipped card is captured due to a security breach, it cannot be used to create counterfeit cards for future transactions. In contrast, because the cardholder data from a magnetic stripe is static, it can be copied into a counterfeit card and reused for future transactions.

What are the obstacles to adoption of EMV in the United States?

There are several factors that have inhibited and continue to inhibit adoption of EMV in the U.S., including:

MERCHANT AWARENESS

A primary hurdle to the widespread implementation of EMV-compliant technology in the U.S. is merchant awareness and understanding of the new technology and the related EMV-liability shift. One independent analyst and consultancy found that 30.2% of merchants reported that they had never heard of EMV at the beginning of this year (2015), and a further 36.8% report they have no interest in launching EMV in the future. The card brands and payment processors are taking steps to promote industry-wide awareness, but dissemination of that information, and then action upon it, will inevitably take time.

THIRD PARTY SERVICE PROVIDERS AND PROCESSORS READINESS

EMV-compliant POS software developers are behind the curve as well; not all POS systems have been (or will be) upgraded to accept EMV-enabled payment cards, leaving some merchants hoping to achieve EMV compliance with few options: move to a new payment application vendor and absorb new overhead costs, or wait until their current POS software vendors catch up with the EMV-migration trend. Other vendors in the payment processing ecosystem may also not be ready for EMV. For example, in a Strawhecker Group industry survey, 68% of merchant respondents cited processor readiness as a significant barrier to adoption of the new system. Contributing to this dilemma, EMV-enabled hardware is in short supply.

COST AND BUSINESS DISRUPTION

Merchants interested in outfitting existing POS systems with EMV-compliant terminals, assuming EMV-enabled software is available, will be required to invest substantial resources in new technology and endure potential business disruption. A single EMV-compliant POS terminal can range in cost from $100 to $600, with necessary software upgrades, employee training, and other financial considerations adding to the marginal cost. Delays and confusion around implementation can cause business disruption and financial loss. Obviously, the financial imposition inherent to becoming EMV compliant can be onerous and, in some cases, might weigh against doing so from a rational business perspective.

CONSUMER ADOPTION

While the merchant population has been slow to accept and implement EMV technology, consumers are even further behind in awareness and education. (Recall that the EMV-Liability Shift has no impact on the consuming public). With respect to consumer adoption, merchants may take a ‘if-it’s-not-broke-don’t-fix-it’ attitude, especially if the merchants believe customer irritation will arise.

Hiscox | Encourage Courage

EMV Security and Fraud Prevention

What is being done to accelerate adoption of EMV in the United States?

Visa, MasterCard, Discover and American Express have all issued rules and guidelines for processors and merchants to support EMV chip technology. New card brand programs that became effective in October 2015 provide merchants with incentives designed to accelerate merchant and industry migration to EMV-compliant POS and card technology.

What kind of fraud does EMV aim to prevent?

Chip-enabled cards are intended to reduce counterfeit card-present fraud. However, they do not reduce CNP fraud since the authentication information contained in the chip is not necessary to effectuate a CNP transaction.

From a security perspective, what is the difference between EMV technology and magnetic stripe technology?

Magnetic stripe cards utilize cardholder data encoded on the card's magnetic stripe to authenticate a transaction. If criminals can obtain the cardholder data related to a payment card by breaching a merchant's security, they can create counterfeit cards with the stolen cardholder data embedded in the counterfeit card's magnetic strip and use that card for fraudulent card-present transactions.

In contrast, the chip embedded in EMV-enabled cards provides dynamic authentication information that changes for each transaction. As a result, even if the authentication data is captured due to a security breach at the merchant's site, it cannot be used to create counterfeit cards for future transactions. As such, EMV-enabled cards significantly reduce counterfeit card-present fraud.

If a merchant adopts EMV does that mean it no longer has to worry about a security breach?

No. EMV-enabled cards still transmit cardholder data when used at a POS terminal, including name, primary account number, expiration data and security code. As such, if a merchant has been breached, attackers still may be able to capture cardholder data before it is encrypted and sent to the merchant's processor (e.g. using a memory scraper or similar malware).

While attackers will not be able to use the intercepted cardholder data to create counterfeit cards that work, they could still use the stolen cardholder data for CNP transactions (e.g. at Amazon.com).

Does EMV technology actually reduce card-present counterfeit fraud?

Yes. Countries where EMV technology has been implemented on a widespread scale have experienced significant reductions in fraud from counterfeit card-present fraud:

- across Europe, card-present counterfeit fraud has declined by roughly 35-percent since 2007;
- the U.K. has observed a 56-percent reduction in counterfeit fraud since EMV technology began taking hold in 2005;
- canada has seen a similar decline, with counterfeit fraud being cut in half since the roll-out of chip-and-PIN technology in 2008;
- in Australia, the occurrence rate of counterfeit fraud has dropped by some 38-percent.

While these statistics demonstrate a universal reduction in counterfeit card-present fraud resulting from adoption of EMV technology, fraudulent CNP transactions increased as EMV was adopted in these countries.

If EMV does not prevent CNP fraud due to security breaches, won't the criminals just make more fraudulent CNP payment card purchases online or over the phone?

Potentially, yes. In fact, we have seen a shift from card-present counterfeit fraud to online CNP fraud in many countries where EMV technology is widely used: in Canada, for example, the 50-percent drop in counterfeit (card-present) fraud realized since 2008 was accompanied by a 133% spike in CNP fraud; likewise, CNP fraud in the U.K. has doubled since 2005, while it has increased across Europe by around 25%.

That said, there are ways to minimize online CNP fraud including through tokenization and the use of independent payment gateways (in both cases, the online merchant's systems never receive actual payment card data).

What is the relationship between EMV and PCI-DSS?

The Payment Card Industry Data Security Standard (PCI-DSS) is the security standard merchants contractually agree to comply with when they accept credit or debit card payments for their goods and services. PCI-DSS is intended to reduce the risk that a merchant will suffer a data breach of its payment card processing systems that leads to the theft of cardholder data and subsequent fraudulent payment card activity. Notably, merchant adoption of EMV technology is NOT required by the new PCI-DSS.

EMV technology provides an additional level of authentication at the POS terminal that reduces the risk of card-present counterfeit fraud that may be perpetrated at other merchants' locations. Unlike PCI-DSS, EMV technology does not reduce the risk of a data breach of a merchant's payment card processing environment. Cardholder data transmitted from a chip-enabled payment card can still be captured by hackers that have gained access to a merchant's POS systems or other parts of its payment card processing environment.

What is PCI-DSS validation relief and how does it incentivize EMV compliance?

Under card brand operating regulations, merchants are generally required to maintain PCI-DSS compliance. Merchants subject to PCI-DSS are required to validate and report their PCI-DSS compliance to the card brands on an annual basis by various means, including by completing a self-assessment questionnaire or by having a PCI-DSS Qualified Security Assessor conduct an audit and file a Report on Compliance with the card brands. The annual assessment and validation process can be onerous and expensive for merchants.

To incentivize EMV-compliance, the card brands have created programs that relieve merchants of certain PCI-DSS validation requirements. For example, Visa's Technology Innovation Program (TIP) allows merchants to, in effect, opt out of PCI-DSS validation if the merchant processes at least 75% of their transactions through EMV-enabled POS terminals. To qualify for TIP and receive its benefits, U.S. merchants must meet all of the following criteria:

- the merchant must have validated PCI-DSS compliance within the previous twelve months or have submitted to Visa (via their acquirer processor) a defined remediation plan for achieving compliance based on a gap analysis;
- the merchant must have confirmed that sensitive authentication data is not stored. As defined in the PCI-DSS, this includes the full contents of magnetic-stripe, Card Verification Value 2 (CVV2), and/or PIN data;
- at least 75% of the merchant's total (chip and magnetic-stripe) transaction count must originate from fully enabled, dual-interface (contact/contactless) terminals that are capable of processing complete chip transactions; and
- the merchant must not be involved in a breach of cardholder data. A breached merchant may qualify for TIP if it has subsequently validated PCI-DSS compliance.

Under AMEX's reporting relief program, a merchant is eligible to receive relief from PCI-DSS reporting requirements if, at the locations where 75% of the merchant's transactions occur, the merchant's POS terminals are able to process American Express EMV chip-based contact and contactless transactions.

A merchant that wants to become EMV-compliant may not be able to because of hardware shortages, software implementation by vendors, processor readiness and other related issues. Do merchants have any defense or recourse against the EMV liability shift if their inability to become EMV-compliant is caused by third parties or factors outside of their control?

Unfortunately, no. The current EMV liability shift process for the card brands does not appear to take these factors into account.

Hiscox | Encourage Courage

The 'EMV Liability Shift' and Other EMV-Adoption Incentives

In general, what liabilities do merchants face with respect to fraudulent card-present counterfeit payment card transactions?

Prior to October 2015, because of the card brands' 'zero liability' policies, merchants that accepted counterfeit payment cards for the purchase of goods or services from their establishment were not liable for chargebacks arising from sales made using the counterfeit payment cards. As detailed below, the EMV Liability Shift will result in a reallocation of these risks under some circumstances.

In general, what liabilities do merchants face when they suffer a security breach that compromises cardholder data?

Most of the major card brands have implemented a contractual and regulatory infrastructure enabling them to seek recovery or contribution for costs incurred as a result of fraudulent credit card activity. Generally, card brands may be able to offset these fraud-related expenses through fines, penalties, and assessments levied upon merchants found to be noncompliant with PCI-DSS industry standards.

Fines and penalties are typically punitive in nature and stem from a merchant's non-compliance with PCI-DSS; whereas, assessments are compensatory, designed to cover increased operating expenses, card re-issuance costs, and fraud recovery.

Under Visa's Global Compromised Account Recovery process (GCAR), for example, Visa can levy an assessment against a non-compliant merchant that includes fraud recovery (i.e. an amount to reimburse issuing banks for fraud perpetrated on cards subject to a data breach) and operating expense recovery amounts (i.e. an amount to reimburse issuing banks for the costs to reissue payment cards subject to a data breach).

In general, what incentives have the card brands implemented to spur adoption of EMV in the United States?

The card brands have created multiple incentive programs to encourage merchants and issuing banks to adopt and implement EMV technology, including:

- the EMV Liability Shift, which reallocates chargeback liability associated with counterfeit credit cards to the entity (either the merchant or the relevant issuing bank) with the least secure EMV-technology;
- fraud and operating assessment relief, which relieves an EMV-compliant merchant of fraud recovery and operating expense assessments that card brands levy on merchants in the wake of a payment card security breach suffered by the merchant;
- PCI validation relief, which relieves an EMV-compliant merchant of the need to validate its PCI-DSS compliance on an annual basis.

Notably, the various incentives and programs of the card brands may vary and it is important to review each card brands' program rules to fully understand their requirements, how they operate, and the scope of relief provided.

What is the EMV 'liability shift'?

As of October 1, 2015, many of the card brands have instituted a 'liability shift' policy as an incentive for both merchants and card issuers (banks, credit unions, etc.) to increase card security and reduce counterfeit fraud. In its simplest terms, the 'liability shift' means that, as between a merchant and card issuers, liability for counterfeit card-present transactions will reside with the party using the least secure EMV-related technology. In general the liability shift works as follows:

- after October 1, 2015, if a merchant that has failed to install an EMV-compliant POS system accepts a counterfeit payment card at its store that relates to a particular issuing bank, the merchant (and not the issuing bank) will be liable for chargebacks arising from the transaction, assuming the issuing bank has implemented chip-enabled payment cards. Prior to the liability shift the issuing bank would have been liable for the chargeback.

- In contrast, after October 1, 2015, if a merchant that has installed an EMV-compliant POS accepts a counterfeit payment card related to an issuing bank that has not issued chip-enabled payment cards, the issuing bank (and not the merchant) will be liable for the chargeback.
- If there is a 'tie' between a merchant and issuing bank with respect to EMV compliance, the pre-October 2015 issue would not be liable for counterfeit card-present fraud.

Note that, as between the card brands, there is some variation in the details of the scope and effect of this liability shift. For example, Visa's liability shift applies to fraud-related costs incurred as a result of counterfeit card activity, but not for fraud stemming from lost or stolen cards; whereas other card brands, including American Express, Discover, and MasterCard, shift liability under some circumstances for fraud relating to lost or stolen cards; MasterCard also plans to extend the impact of its liability shift to ATM counterfeit cards (effective October 2016). Merchants should seek additional information from the payment brands they accept to determine their specific EMV-compliance requirements and the scope and effect of the liability shift.

If an issuing bank has issued all of its cards with EMV chips, how is counterfeit fraud still possible?

During the interim period between migration from magnetic stripe technology to full adoption of EMV technology, EMV-compliant payment cards will include both a magnetic stripe and an EMV-enabled chip. In addition, EMV-compliant hybrid POS terminals will still allow cards to be swiped in order to read the magnetic stripe.

As such, during this interim period, some chip-enabled cards will be swiped into compromised POS terminals and the cardholder data from those swipes can be used to create counterfeit magnetic stripe cards. In addition, criminals that steal payment card information from CNP transactions (online and otherwise) will still be able to create counterfeit magnetic stripe cards that can be used to purchase goods and services at POS terminals that accept magnetic stripe cards. In other words, until every merchant and issuing bank in the U.S. adopts EMV-compliant technologies, card-present counterfeit fraud will continue to exist.

What do merchants need to do in order to become EMV compliant? Is there a certification process?

Each of the card brands has developed an EMV-certification process that sets forth the EMV-related requirements merchants must satisfy in order to become 'EMV-compliant' and avoid the liability shift. While each of the card brand's EMV-compliance certification program may vary, in general, to become EMV-compliant merchants must apply for and receive certification through its acquiring bank, which entails three phases:

- Hardware Certification: employing EMV-enabled terminals that are certified by EMVCo (comprised of the major card brands acting as member organizations), as well as by each card brand (in an individual capacity) that the merchant will use to process payments;
- Software Certification: implementing payment application software that is also certified as EMV-compliant; and
- End-to-end Certification: holistic testing and approval of point-of-sale configuration, where the card brands check and confirm the integrity of the payment chain as a whole.

The certification process and level of involvement will vary across merchants, depending largely upon the size and complexity of the merchant's business; the timeframe to completion can take anywhere from a few weeks to several months.

On a practical level what costs do merchants face to become EMV-compliant?

In short, merchants will have to invest in new hardware and software to become EMV-compliant. The ultimate costs will vary depending on the size of the merchant and the complexity of its POS environment.

Will the EMV liability shift work to incentivize merchants to adopt EMV-compliant technology?

Maybe, but it may depend on the circumstances of the particular merchant. For example, merchants that sell expensive consumer goods (e.g., computers, televisions, stereos) often have higher chargeback rates. In contrast, merchants that are smaller businesses or that sell essential goods, such as food, may have very low chargeback rates. As such, if the financial benefit of avoiding chargebacks does not exceed the costs to implement new EMV-compliant technology, some merchants may choose to avoid EMV compliance and continue to accepted magnetic stripe cards.

If a merchant is EMV-compliant and suffers a data breach, does that mean the merchant is not responsible for PCI fines, penalties or assessments?

No. In general, EMV-compliant merchants can still be liable for PCI fines, penalties, and assessments if they suffer a data breach. However, some of the card brands have developed temporary 'safe harbor' programs that allow merchants to avoid fraud and operating expense assessments if a merchant meets certain EMV-related requirements.

What are operating expense and fraud assessments?

The card brands have enacted various recovery programs that require merchants to pay issuing banks for card reissuance costs arising out of, and fraud perpetrated on cards taken during, a payment card data breach, including:

- Visa GCAR (Global Compromised Account Recovery)
- MasterCard ADC (Account Data Compromise)
- AMEX DSOP (Data Security Operating Policy)
- Discover DISC (Discover Information Security and Compliance)

How do the EMV safe harbors impact operating expense and fraud assessments against merchants?

While merchants that suffer security breaches involving payment card data are, generally, liable for potentially significant fraud and operating expense recovery assessments, EMV-complaint merchants benefit from another liability-based incentive intended to influence the EMV-Migration. For example, under Visa's GCAR process, merchants can avoid liability for GCAR assessments if the merchant generated more than 95% of their card-present transactions from EMV-enabled payment terminals at least thirty days before the data breach. Under MasterCard's ADC program, if at least 95% of MasterCard transactions originate from EMV-compliant POS terminals, the merchant is relieved of 100% of account data compromise penalties.

Hiscox
520 Madison Avenue
32nd floor
New York
NY 10022

T 646 442 8322
www.hiscoxbroker.com

Matthew Donovan
Product Head
Cyber and Data Risks
Hiscox USA
matthew.donovan@hiscox.com

David Navetta
Co-Chair
Data Protection, Privacy and Cybersecurity Practice
Norton Rose Fulbright
david.navetta@nortonrosefulbright.com