A Heartland Payment Systems **White Paper 2014**

Heartland Secure.

By: Michael English
Executive Director, Product Development

Heartland Secure.

Heartland Secure™ is a comprehensive card data security solution that combines three powerful technologies working in tandem to provide merchants with the highest level of security available against card-present data fraud.

Featuring the only warranty in the data security industry, this exclusive solution is designed to provide merchants with security against point-of-sale (POS) intrusions, data skimmers, crimeware, miscellaneous errors, insider misuse and other common sources of data fraud by eliminating the opportunity for criminals to monetize card data.

Offered to Heartland customers for no extra service fees, Heartland Secure combines:

- EMV electronic chip card technology to prove that a consumer's card is genuine.
- Heartland's E3™ end-to-end encryption technology, which immediately encrypts card data as it is entered so that no one else can read it.
- Tokenization technology, which replaces card data with "tokens" that can be used for returns and repeat purchases, but are unusable by outsiders and have no value.

Why is Heartland Secure Needed?

As per Robert O. Carr, chairman and CEO of Heartland Payment Systems, "Security breaches against large retailers like Target and Neiman-Marcus get most of the publicity, but there were nearly 150 security incidents with confirmed data losses in the U.S. retail sector alone in 2013. Most of these attacks targeted small companies that simply can't afford the cost of PCI-DSS penalties. We designed Heartland Secure as a comprehensive security solution for customers using POS and other card-present processing methods. We're so confident in this system that we offer the only warranty in the industry."

According to the Verizon 2014 Data Breach Investigations Report[1], the American retail and accommodation sectors – including restaurants, hotels, grocery stores, gas stations and other brick-and-mortar outlets – suffered 285 security breaches with confirmed data losses. The data indicates that the vast majority of these breaches occurred against companies with fewer than 1,000 employees.

In their introduction, Verizon states that 2013 could be characterized as "a year of transition from geopolitical attacks to large-scale attacks on payment card systems." The report also said 2013 would be remembered as the "year of the retailer breach." POS intrusions accounted for 31 percent of the 148 retail breaches, with payment card skimmers accounting for another six percent. POS intrusions accounted for 75 percent of the 137 accommodation sector breaches.

[1] Verizon 2014 Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/2014/

EMV[2] and Security

Visa, MasterCard, Discover and American Express announced that EMV chip card acceptance is coming to the United States, the last major country in the world to migrate to EMV.[3] Card issuers such as Capital One, Bank of America, Citi, Chase and others have begun issuing chip cards to their customers.

Each EMV card being issued has a microprocessor chip embedded in the card as well as a magnetic stripe located on the back of the card. The card can be used as an EMV card or magnetic stripe card for payment, depending on the capability of the terminal. Acquirers such as Heartland have been mandated to support EMV transaction acceptance and were required to certify our hosts for EMV acceptance by April 1, 2013. In addition to the acquirer mandate, Visa, MasterCard, Discover and American Express have instituted a liability shift for fraudulent transactions that occur at the point of purchase beginning October 1, 2015[4] for non-AFD (Automated Fuel Dispenser) terminals and October 1, 2017 for AFDs. Merchants that do not have a terminal or POS system capable of reading EMV cards will be responsible for chargebacks of fraudulent transactions beginning October 2015. The liability shift only applies when an EMV card is presented at the POS, otherwise the current liability in place for magnetic stripe card transactions remains. It is important to note that EMV acceptance is not a government or card brand mandate for merchants.[5]

Using EMV improves the security of a payment transaction in a number of ways:[6]

1. EMV provides a cryptographic card authentication that protects a merchant and issuer against the acceptance of counterfeit cards
2. EMV offers cardholder verification by supporting offline or online PIN. PIN helps authenticate the person tendering the card is in fact the cardholder, thus protecting the merchant against accepting lost and stolen cards
3. EMV cards include several means of transaction authentication that help safely authorize transactions

Every EMV card issued includes a secure embedded microprocessor chip that has a variety of hardware and software detection methods that immediately react to tampering attempts and delete the cardholder's information stored in the chip.[7]

EMV technology largely eliminates skimming and counterfeiting associated with magnetic stripe cards. EMV cards use a unique key to generate a cryptographic value called an Authorization Request Cryptogram (ARQC) that is sent to the card issuer along with the transaction data in the authorization message. The ARQC helps the issuer verify that the card is authentic. Using that same transaction data, the issuer generates another cryptographic value called an Authorization Response Cryptogram (ARPC) that is sent back to the card in the response message. The ARPC verifies the issuer is authentic to the card. The combination of the ARQC and ARPC help reduce the chance that a counterfeit card is being tendered.[8]

[2] EMV Essentials for the U.S. Merchant, A Mercator Advisory Group Research Brief Sponsored by Heartland Payment Systems, January 2012

[3] http://www.emv-connection.com/emv-101-fundamentals-of-emv-chip-payments/

[4] http://usa.visa.com/download/merchants/bulletin-us-acquirer-mandate-080911.pdf

[5] http://www.mastercardadvisors.com/_assets/pdf/emv_us_aquirers.pdf

[6] http://www.smartcardalliance.org/pages/slideshows-20120409?template=slides

[7] http://www.gemalto.com/companyinfo/smart_cards_basics/benefits.html and http://www.sans.org/reading-room/whitepapers/authentication/smart-cards-secure-they-131, Page 12

[8] EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3, November 2011, Application Cryptogram and Issuer Authentication, Page 89

EMV helps protect the issuer and merchant by ensuring that an EMV card was presented at the point of purchase for tender. Upon completion of an EMV transaction, the card generates a Transaction Certificate (TC)[9] value that provides evidence to the issuer that the card was present and was used for payment. This certificate can be sent in settlement as a record of the entire transaction.

EMV also helps combat replay attacks[10] through use of an Application Transaction Counter (ATC)[11] that is leveraged by the issuer to verify the following:

- Proving that the ATC of the current transaction is not the same as the ATC of the previous transaction guards against replay attacks
- Ensuring the ATC is always incrementing and not going backwards will help stop from accepting a fraudulent card for a purchase
- Checking that an ATC is incrementing too much indicates a fraudulent card is being tendered

Every EMV card issued in the United States will feature a card security code (Visa calls theirs an iCVV - ICC Card Verification Value). The card security code is stored in the card's secure microprocessor chip.[12] It's similar to the card security code that is found in a magnetic stripe but is a different number than the one used for the magstripe. Additionally, chip cards contain a service code value that identifies the card as being EMV capable. The benefit to a merchant? A thief can't simply skim the magnetic stripe of an EMV card and use it to create another magnetic stripe card that is used at another EMV-enabled terminal. It won't work because the verification value and the service code of the two aren't the same. An issuer will catch a fraudulent transaction when tendered at an EMV-enabled POS system. However, that counterfeit magstripe card could be used at a non-EMV capable terminal.

Can EMV stop counterfeiting of the chip? The simple answer is yes. Creating a counterfeit EMV card is unlikely because the unique microprocessor chip inside each EMV card leverages dynamic data elements specific to the transaction or generated by the card for each authorization. This makes counterfeit card creation virtually impossible. But, what about the exposed primary account number (PAN) and expiration date that can be pulled off an EMV card? That exposed card data can be used for eCommerce fraud if the merchant doesn't request the card security code (CVV2) or Address Verification Service (AVS).

E3 is end-to-end encryption

E3 encrypts cardholder information at the earliest point of the transaction – at card swipe, key entry, tap or insertion. Terminals and customer card entry devices carrying the E3 brand feature a tamper-resistant security module housed within the terminal, reader or PIN pad so that the device can't be converted into a skimming instrument. Unlike less secure solutions that rely solely on hardware or software encryption alone, E3 provides protection by encrypting cardholder data in a protected hardware enclosure, ensuring sensitive information is useless to would-be hackers. If the retailer's network or POS system is compromised, the stolen encrypted card information is useless and cannot be monetized.

[9] An Application Cryptogram generated by the card when accepting a transaction. EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3, November 2011, Definitions, Page 19

[10] A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

[11] EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3, November 2011, Application Transaction Counter Considerations, Page 147

[12] Visa Smart Debit/Credit (VSDC) U.S.A. – Issuer Implementation Guide for VIS, Version 1.4.1, Version 1.0, February 2011. Please also reference MasterCard M/Chip Requirements, September 20, 2013

E3 is an Identity-Based Encryption (IBE)[13] scheme where Format-Preserving Encryption (FPE)[14] is used to encrypt the cardholder's account number and discretionary data within the E3 branded device's tamper-resistant security module.[15]

E3's Value Proposition

Over 50,000 merchants in the United States benefit from E3's encryption security in the following ways:

- E3 removes consumer card data from the merchant's environment by encrypting the cardholder's primary account number (PAN) and discretionary data
- E3 eliminates the risk of hackers monetizing stolen card data. Hackers cannot profit from encrypted card information.
- E3 is a strong response to "all organizations should assume they've been hacked," as written by the authors of the Cisco 2014 Annual Security Report[16]
- E3 reduces a merchant's PCI scope as documented in a white paper written by Coalfire[17]

PCI is a great best practice guideline and helps protect cardholder data in a merchant's environment. However and from a merchant's perspective, if they adopt E3 and tokenization as well as enforce commonsense restrictions that reduce the chance of writing down cardholder information, they cannot lose card data, making PCI non-compliance irrelevant.

E3 encrypts and protects EMV clear text data

Implementing a payment system using only the EMVco and Card Brand EMV specifications leaves a customer's primary account number (PAN) and discretionary data exposed and in the clear. In the event that crimeware has found its way into the retailer's POS system or network, the cardholder data could be hacked and used fraudulently at the merchant eCommerce site not requiring AVS or CVV.

E3 offers an additional layer of security for EMV transactions. As the EMVco specifications are presently written, when an EMV transaction is processed at the point of sale the transaction is sent in the clear to the acquirer or processor for authorization. E3 encrypts the EMV transaction in the same way it encrypts a magnetic stripe transaction, thus protecting the cardholder information. E3 converts the confidential cardholder data into a meaningless number. The encrypted cardholder data is protected throughout the life of the transaction – at inception, within the POS system, while traveling in the retailer's network and when the transaction is transmitted to the acquirer. This end-to-end protection keeps the cardholder's data safe and prevents criminals from monetizing it.

But what about the magnetic stripe that is included with all EMV cards? Can that magstripe be skimmed and used to create a counterfeit magnetic stripe card? Yes. A thief can copy an EMV card's magstripe, create a magstripe counterfeit card and use it at a non-EMV terminal. As of today, E3 also encrypts magstripe cards on EMV cards and is another reason why EMV terminals need E3 – for EMV and magstripe acceptance.

[13] http://www.voltage.com/technology/identity-based-encryption/

[14] http://www.voltage.com/technology/format-preserving-encryption/

[15] TRSM (tamper resistance security module)

[16] https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

[17] Heartland Payment Systems E3™ MSR Wedge Technical Assessment White Paper, Coalfire, January 4, 2011

Tokenization eliminates the need to reuse the EMV card number

Tokenization and E3 work together to make an EMV transaction safe. Tokenization removes any direct reference to the card number by substituting the consumer's card number with a token. Tokens replace the need to reuse card data in two ways:

1. as a reference number when the retailer needs to perform a post-sale transaction such as a void or refund
2. as a representative of the card for future transactions such as card on file, recurring payments or customer analysis

Tokenization complements E3. E3 protects the card number during the tender and authorization process. Tokenization protects the card number after the initial sale has been finalized and when the card is needed for future transactions.

Combined benefits of E3, EMV and tokenization for merchants

There is no one solution to payment transaction security. While EMV, E3 and tokenization are effective individually, when combined they form a team that takes clear text card data out of the transaction and merchant ecosystem. The combination of EMV, E3 and tokenization provide the following benefits to merchants:

- EMV and E3 remove the ability to skim and monetize card data through verification and encryption
- EMV and E3 eliminate the opportunity for "man-in-the-middle" attacks
- E3 and tokenization remove card data from the merchant's environment
- E3 eliminates the risk of monetizing stolen card data
- E3 and tokenization are a definitive response to "all organizations should assume they've been hacked," Cisco 2014 Annual Security Report
- E3 and tokenization reduce a merchant's PCI scope as per Coalfire's study
- Heartland does not believe a merchant should pay more for transaction security and does not charge additional for E3 encryption, single-use tokenization or processing of an EMV transaction

[13] The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections between computer systems and relays messages between them, making them believe that they are talking directly to each other when in fact the entire conversation is controlled by the attacker.

[13] https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

[13] Heartland Payment Systems E3™ MSR Wedge Technical Assessment White Paper, Coalfire, January 4, 2011