Debunking EMV Myths

Version 1.0

Date: March 2019

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body focused on supporting the introduction and implementation of new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the U.S. The Forum is the only non-profit organization whose membership includes the whole payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry.

Additional information can be found at http://www.uspaymentsforum.org.

EMV is a trademark owned by EMVCo LLC.

The U.S. Payments Forum has used best efforts to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. The U.S. Payments Forum disclaims all warranties as to the accuracy, completeness or adequacy of information in this document. Comments or recommendations for edits or additions to this document should be submitted to: info@uspaymentsforum.org.

Introduction

EMV chip technology has become ingrained in the U.S. payments infrastructure. Still, there are misperceptions about the technology, its security features and impacts on fraud. The U.S. Payments Forum has created this guide to provide accurate information for all stakeholders communicating about contact and contactless chip technology, including card issuers, retailers and the media.

Myths and Facts

MYTH #1

EMV will eliminate all payments fraud.

FACT

EMV chip technology was introduced specifically to eliminate the growing issue of counterfeit card-present fraud and has been extremely effective. The technology combats counterfeit card-present fraud by creating a unique one-time code for each transaction. This dynamic code decreases the value of card data and eliminates the ability for thieves to use a counterfeit card at a chip-enabled terminal.

To protect payments outside of card-present transactions, such as card-not present fraud, merchant identity fraud, phishing and more, experts recommend a layered security approach. Other technologies and approaches such as encryption, tokenization and multi-factor authentication can be combined to create a wider-reaching fraud mitigation strategy.

MYTH #2

Chip card transactions use encryption technology.

FACT

EMV chip technology improves the security of a payment transaction by using cryptographic card authentication that helps protect against the acceptance of counterfeit cards. EMV does not encrypt any card data (sensitive or otherwise) during the chip transaction process.

Encryption is another cryptographic method that should be layered with chip technology for additional transaction security in order to effectively protect sensitive cardholder data from compromise.

MYTH #3

EMV was implemented in the U.S. to shift fraud liability from one party to another.

FACT

EMV chip technology was introduced as a solution to eliminate in-store counterfeit fraud, after it had proven its effectiveness in global markets. As a way to incentivize both merchants and issuers to make the transition to the more secure technology, the party with the less-secure technology is responsible for the cost of a fraudulent transaction. If both parties upgrade to chip technology, they both benefit from eliminating the possibility for counterfeit card-present fraud.

MYTH #4

EMV only prevents fraud with chip and PIN.

FACT

It is sometimes reported that only chip used with a PIN prevents fraud. This is inaccurate. The chip on its own is the primary mechanism for preventing card present counterfeit card fraud. EMV chip technology provides dynamic data for every transaction to the card issuer to validate that the genuine card was presented to the merchant. This is what makes chip technology secure and effective without the need to use PIN. Adding PIN to the security features of EMV adds another layer of security to address lost and stolen card fraud.

MYTH #5

Payment fraud just shifted to card-not-present (CNP) and net fraud is going up.

FACT

With chip card payments reducing fraud at the point of sale, criminals are looking for new avenues – including buy online pick up in store (BOPIS) fraud, CNP e-commerce fraud and at the Automated Fuel Dispenser (AFD) where EMV chip upgrades have not yet occurred. However, merchants are staying vigilant and are taking a systematic, multi-layered approach using tools such as advanced authentication, fraud tools and tokenization together to create successful fraud reduction programs. As a result, statistics are actually showing that the overall proportion of CNP fraud is actually staying relatively even – and perhaps even decreasing – as a percentage of online sales [1].

[1] Aite Group 2017. Recently-updated projections from Aite Group emphasizes the correlation between the growth in fraud in the card-not-present channel and similar growth in transaction volume over the past five years, and predicts a similar trend through 2020.

MYTH #6

A thief can easily electronically pickpocket your contactless card/device.

FACT

While smart phone applications that enable the phone to read some of the data from a contactless enabled card or device do exist, they can only read the account number and expiration date. Plus, the thief would need to be physically close to the card to get this information. (Source: Mastercard)

MYTH #7

If a thief does intercept your contactless information, they can create a counterfeit card and successfully use it to conduct in-store transactions.

FACT

When you make a contactless transaction, the payment device – card, mobile device or wearable – provides the payment terminal with a dynamic, one-time use code necessary to successfully complete the transaction. Even if a thief had your contactless card information, they would not be able to create a counterfeit card that could replicate the one-time code needed for a successful in-store transaction. The information is also not sufficient to create and use a magnetic stripe card for a transaction.

MYTH #8

Even if a thief can't counterfeit your contactless card, they can make purchases online or by phone.

FACT

For a purchase to be authenticated and authorized via phone or online, typically several pieces of information must be presented – including the three-digit code on the back of a card and the cardholder's name and billing address. Since the card or device does not send the code, billing address or zip code information or name over the contactless interface, the thief won't have the information typically needed to conduct payment transactions, either in person, on the phone or online. (Source: Mastercard)

MYTH #9

In addition to stealing your card data, thieves can also steal your identity.

FACT

There is a clear distinction between identity theft, where a consumer's identity is assumed by another individual for criminal purposes, and payment card fraud, where a consumer's card information is compromised and used to make unauthorized purchases. Contactless cards and devices do not transmit information about the cardholder such as name or address to mitigate the chance of identity theft.

MYTH #10

Thieves can create usable counterfeit cards through shimming.

FACT

Shimmed data, which is stolen through a hard-to-detect device attached to a terminal, cannot be used to create a usable magnetic stripe counterfeit card. While shimmers that collect card data from an EMV chip card inserted in a terminal exist, the usefulness of the data collected is severely limited because EMV chips use dynamic data that is unique for every transaction. The result of this dynamic data is called a cryptogram, which is created using secret cryptographic keys, each specific to individual card, securely stored in the chip and only known to the card and the issuing bank. EMV chip cards, have multiple measures to prevent external access and copying of its keys. Without the chip's cryptographic keys, it's not possible to create a functioning counterfeit version of a chip card to be used through the contact or contactless interfaces.

Issuers applying appropriate security controls easily determine counterfeit attempts and block such transactions, rendering these cards useless. Issuer banks and merchants also use 3D Secure, CVC2, address verification and other techniques to prevent shimmed data from being used for fraudulent internet transactions.

MYTH #11

Cardholders are responsible for purchases made by thieves if they steal your card information.

FACT

Issuers have zero liability policies, so cardholders are not liable for fraudulent charges. For specific policy information, cardholders should contact their bank.