Contactless Payment Security Questions & Answers

The Smart Card Alliance developed this document to address questions about contactless payment security. The questions and answers below apply to contactless payment using contactless payment devices that have implemented payment applications from the global payment networks (i.e., American Express, Discover, MasterCard and Visa).

1. What is a contactless payment?

A contactless payment is a payment transaction that does not require physical contact between a consumer's payment device and a point-of-sale (POS) terminal. The consumer holds a payment device (such as a contactless or dual-interface chip card or mobile device) in close proximity to the terminal (less than 1-2 in. away), and payment account information is transmitted wirelessly, over radio frequency (RF).[1] The consumer's contactless payment device can assume a variety of form factors, including cards, Near Field Communication (NFC)-enabled smart phones, and wearables. Contactless transactions generate a unique code for each transaction.

Additional information about contactless payments can be found in the Smart Card Alliance white paper, "Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers."[2]

2. How do contactless payments relate to the EMV migration in the U.S.?

As merchants migrate to EMV, in many cases their new POS equipment already comes with the ability to perform contactless EMV transactions. If merchants choose to enable contactless functionality (in conjunction with their payments processor), the POS infrastructure will be ready to accept contactless payments using either dual-interface chip cards or NFC-enabled mobile devices provisioned with a mobile EMV payment application. Contactless EMV transactions are fast (tapping on the terminal rather than swiping or inserting) and maintain the high EMV security standard, delivering convenience and ease of use for consumers and providing card-present fraud protection for merchants.

3. What is NFC technology and how does it relate to contactless payment?

Simultaneously with the U.S. move to EMV chip card payments, NFC technology is emerging as a useful accessory for consumer transactions. NFC is not a payment technology; it is a set of standards that enables proximity-based communication between consumer electronic devices such as mobile phones, tablets, personal computers or wearable devices. An NFC-enabled mobile device can communicate with a POS system that currently accepts contactless payment cards. Contactless payment transactions can be made using NFC-enabled devices that are provisioned (in other terms "loaded") with a mobile payment application and are processed the same as contact and contactless EMV chip card transactions.

---

[1] This document defines contactless payments as using radio frequency communications that are compliant with the ISO/IEC 14443 or Near Field Communication (NFC) standards. Other types of proximity payment technologies can be used but they are not covered in this document and will have different capabilities and security features.

[2] http://www.smartcardalliance.org/publications-contactless-emv-payments-benefits-for-consumers-merchants-and-issuers/

4. How do mobile wallets work with contactless payment?[3]

Card information must be loaded (or "provisioned") into a mobile wallet in order to make a contactless payment. Depending on which mobile wallet is used, there are various ways of loading card information, including typing the information on the phone, taking a picture of the card with the phone's camera, or receiving the card information securely over-the-air from the wallet provider and/or financial institution. Once the card information is validated into the mobile wallet, the mobile device can conduct a contactless payment transaction using NFC, which uses the same standard communications protocol as contactless chip cards. As additional security, the mobile wallet application may require "unlocking" before making a contactless payment (e.g., by entering a code on the phone or providing a fingerprint). The mobile wallet may also support additional features including integrated support for loyalty programs or for receiving and/or redeeming coupons. In addition, a consumer device cardholder verification method (e.g., fingerprint) may also be able to be used for the transaction.

5. *What is tokenization and how does EMV tokenization[4] (e.g., payment tokens) work with contactless payment?*

Tokenization is a form of data protection where sensitive information – the consumer's primary account number (PAN, the number on the front of the card) – is replaced with a different numeric value, which is called a token. In a payments scenario, the payment token is used in place of the actual account details through all of the various payment systems involved in a transaction. Tokens have limited use, making tokenization a very effective tool for minimizing cross-channel fraud and the impact of data breaches. Today, tokenization is commonly used for contactless mobile payments, but is a technique that can also be employed for contactless card payments.

6. Are contactless payment transactions secure?

Yes. Contactless payments protect customers' personal information and are a secure way to conduct payment transactions. The primary difference between a contactless payment and other commonly used methods is that the contactless payment device uses RF technology to send payment account information to the merchant's POS terminal, instead of requiring the payment card's chip to be inserted or magnetic stripe to be swiped. Contactless payment devices are designed to operate at very short ranges – less than 1-2 inches – so that the consumer needs to make a deliberate effort to present the card or mobile device to the POS reader to initiate the payment transaction. Please see question 7 below for more details on how contactless cards and mobile devices are protected against accidental or fraudulent reading attempts.

As contactless payment devices are designed to exchange information with a payment terminal using RF technology, the financial payments industry has designed multiple layers of security throughout the traditional credit and debit payment systems to protect all parties involved in the payment transaction. Most of these protective measures are independent of the technology used to transfer the consumer payment account information from the payment card or device to the merchant POS terminal (i.e., swiping, inserting or tapping) and are used for EMV chip, magnetic stripe, and contactless transactions. For example, online authorization, risk management and real-time fraud detection systems are used to

---

[3] Additional information can be found in the Smart Card Alliance white paper, "EMV and NFC: Complementary Technologies Enabling Secure Contactless Payments," December 2015, http://www.smartcardalliance.org/publications-emv-and-nfc-complementary-technologies-enabling-secure-contactless-payments/.

[4] Additional information can be found in the Smart Card Alliance webinar, "EMV Tokenization," November 2016, http://www.smartcardalliance.org/activities-events-webinar-emv-tokenization/

detect potential fraudulent activity for any credit or debit card payment transaction. Plus, as with traditional credit and debit cards, consumers are not liable for fraud.

7. How are contactless payment transactions made secure?

For contactless payments, the financial industry uses advanced security technologies both on the contactless device as well as in the processing network and system to prevent fraud. While implementations differ among issuers, examples of security measures that are being used include the following:

- *Industry standard encryption*. Each contactless device must have its own unique secret key that uses standard encryption technology to generate a unique card verification value, cryptogram or authentication code that exclusively identifies each transaction. No two devices share the same key, and the key is never transmitted.
- *Dynamic data*. Every contactless payment transaction includes dynamic data that is unique for that transaction. Stolen or intercepted transaction data can't be used for other transactions.
- *Authentication*. The issuers verify that the contactless payment transaction has a valid card verification value, authentication code or cryptogram before authorizing the transaction. Therefore, at the system level, issuers have the ability to automatically detect and reject any attempt to use the same transaction information more than once.
- *Confidentiality*. The processing of contactless payments does not require the use of the actual cardholder name in the transaction. In fact, best practices being used within the industry do not include the cardholder name in the contactless chip.
- *Control*. Cardholders control both the transaction and the contactless device throughout the transaction. Cardholders do not have to hand over either a device or their account information to a clerk during a contactless transaction.

Mobile devices can also provide an additional level of security through tokenization and additional types of cardholder verification.

8. Can card information be read from the contactless payment card or device without the consumer knowing?

Contactless payment devices are designed to be read when in close proximity to a capable payment terminal device. The contactless payment devices, as well as the terminals and network, have been designed to ensure that the customer initiates the transaction by holding the contactless payment device within 1-2 inches of the payment terminal. In the event that a motivated individual did read the information from a contactless payment device, the security features designed into the device, the payment terminal and the payment system (see questions 6 and 7) would mitigate against the information being used for fraudulent transactions.

The information accessible through the contactless interface is limited only to a contactless-based payment transaction. For example, personal information such as the cardholder name cannot be read. In reality, the industry has only seen incomplete demonstrative attempts to read information from contactless-enabled cards, not used to conduct actual fraud, including in countries with years of mature contactless deployment where almost every consumer has at least one dual-interface chip card in their wallet. Furthermore, contactless-enabled devices such as mobile handsets have additional protection: the contactless payment modes are disabled until the consumer uses a passcode or biometric identifier (e.g., fingerprint, iris scan).

9. Can information that is read from the contactless payment device be used to create fraudulent transactions?

See questions 6 and 7 for examples of the security measures that are used at the device and system level to prevent fraudulent transactions.

The cardholder information that is used during a contactless payment transaction is of little to no use in creating fraudulent payment transactions. Any information from a contactless payment transaction that can be intercepted or stolen is insufficient to create a fraudulent card or conduct a fraudulent payment transaction. For fraudulent card-not-present transactions (e.g., Internet and telephone purchases), almost all merchants require the security code from the back of the card and/or the zip code, both of which are not available in a contactless payment transaction.

10. Should consumers be worried about carrying contactless cards or take any special precautions?

Consumers should not be worried about carrying contactless cards because of all the security features incorporated into the cards and payments infrastructure. Consumers should take the same precautions with a contactless card or contactless payment device as they would with any personal financial information, such as not leaving their card or device unattended.

If a consumer believes their card account or their information has been put at risk, they should contact the issuer. Additionally, liability policies which protect consumers for traditional consumer credit and debit accounts also apply to contactless transactions.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.