# Contactless Payments Security Questions & Answers

Recent media reports have raised questions about the security of contactless payment transactions and the risk of fraud to consumers. This document was developed by the Smart Card Alliance to address questions about contactless payment security. The questions and answers below apply only to contactless payment using contactless smart card technology, as implemented by American Express, Discover, MasterCard, STAR and Visa.

### 1) How is contactless payment different than RFID?

Both contactless payment devices and radio frequency identification (RFID) tags use radio frequency (RF) technology. However, RFID tags are typically cheap, read-only, low memory devices that can be read over greater distances and that have no or minimal security. Contactless payment cards and devices contain secure microprocessors and memory, have the ability to perform cryptographic processing, have multiple functions, and are required to operate within much smaller distances than RFID tags.

In addition, contactless payments devices and the payments processing networks and systems have specifications and security standards above and beyond those used in basic RFID applications to ensure the integrity and security of the cardholder data and payment transaction.

### 2) Are contactless payment transactions secure?

Yes. Contactless payment, as implemented by American Express, Discover, MasterCard, STAR and Visa, protects customers' personal information and is a secure way to conduct payment transactions. The financial payments networks used to process contactless payments are the same networks that process millions of magnetic stripe transactions securely today. The primary difference is that the contactless payment device (card, fob or other form factor) uses RF technology to send payment account information to the merchant's point-of-sale (POS) terminal, instead of requiring the payment card's magnetic stripe to be swiped. Contactless payment devices are designed to operate at very short ranges – less than 2-4 inches – so that the consumer needs to make a deliberate effort to initiate the payment transaction.

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 and are used for both magnetic stripe and contactless transactions. For example, online authorization, risk management and real-time fraud detection systems are used to detect potential fraudulent activity for any credit or debit card payment transaction. Plus, the liability policies which protect consumers from fraudulent transactions on traditional consumer credit and debit accounts also apply to American Express, Discover, MasterCard, STAR and Visa contactless transactions.

### 3) How are contactless payment transactions made secure?

For contactless payments, the financial industry uses added security technology 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*. At the card level, each contactless card can have its own unique built-in 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 cards share the same key, and the key is never transmitted.
- *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 card throughout the transaction. Cardholders do not have to hand over either a card or their account information to a clerk during a contactless transaction.

**4) 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 2-4 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 2 and 3) would mitigate against the information being used for fraudulent transactions. In reality, the industry has only seen this attack carried out in demonstrations, not used to conduct actual fraud.

**5) Can information that is read from the contactless payment device be used to create fraudulent transactions?**

See questions 2 and 3 for examples of the security measures that are used at the card 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. The security implementation currently used by the different payment brands causes the contactless device-generated transaction information to change every time a reader reads the device. This transaction information is generated using a strong encryption key that is known only to the financial issuer. Issuers can verify this dynamic card information before approving a payment transaction from an authorized reader.

Established best practices can be used by Internet and telephone/mail order merchants to prevent the use of stolen card data, including requiring the card verification value/card verification code/card ID that is printed on the card and/or the cardholder zip code for address verification to complete any purchase. None of this information is used in a contactless payment transaction so would not be available for an Internet or phone purchase.

The industry has not seen attacks on contactless payment cards result in actual fraud.

**6) What steps can consumers take to protect their contactless payment cards?**

While all the issuers continue to enhance and evolve their security to meet the challenges of protecting their customers' sensitive information, there are additional ways consumers can minimize the risk of having their payment card data read by a potential thief by taking a few common precautions, such as not leaving their contactless payment card or key fob unattended

for a length of time. Consumers should take the same precautions they would with any other type of payment card.

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 American Express, Discover, MasterCard, STAR and Visa contactless transactions.

**7) Should consumers be worried about carrying contactless cards?**

No. Because of the many layers of security throughout the payment system that limit fraud with all payment cards and the unique security features used in contactless payment transactions, there have been no reports of this type of actual fraud.

*This Q&A document has recently been updated as a result of media reports describing concerns about RFID fraud, sometimes referred to as so-called "electronic pickpocketing."*

## *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.