



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 Contactless Payments Council 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, MasterCard and Visa.

1) Are contactless payment transactions secure?

Yes. Contactless payment, as implemented by American Express, MasterCard and Visa, is secure. 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 radio frequency (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.

The financial payments industry has designed multiple layers of security throughout the traditional credit and debit payment systems to protect all parties involved in a 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 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 for traditional consumer credit and debit accounts also apply to American Express, MasterCard and Visa contactless transactions.

2) 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.

- At the card level, each contactless card can have its own unique built-in secret "key" that uses standard 128-bit encryption technology to generate a unique card verification value or a cryptogram that exclusively identifies each transaction. No two cards share the same key, and the key is never transmitted.
- At the system level, payment networks have the ability to automatically detect and reject any attempt to use the same transaction information more than once. Thus, even if a fraudster should "read" the information from a contactless transaction, or even multiple transactions from the same card, this information would be useless.
- The processing of contactless payments does not require the use of cardholder name exchanged between card and terminal. In fact, best practices being used within the industry do not include the cardholder name in the contactless chip.
- Some contactless payment cards and devices do not include the cardholder's account number, but use an alternate number that is associated with a payment account by the

issuer's backend processing system. This alternate number would not be able to be used in other payment transactions (e.g., with a magnetic stripe card or on the Internet).

In addition, cardholders control both the transaction and the card throughout the transaction. Cardholders do not have to surrender either a card or their account information to a third party during a contactless transaction.

3) Can card information be read from the contactless payment card or device without the consumer knowing?

While it is technically possible for a contactless payment card or device to be read illicitly, this scenario is unlikely. In the event that a criminal 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 4) would prevent the information from being used to create fraudulent contactless transactions.

Contactless payment devices are designed to be read when placed in close proximity to a contactless payment terminal. Scenarios that result in unauthorized exposure of the payment information are difficult to carry out in the real world. They would require illicit readers to be placed within inches of the contactless card or device carried inside a person's closed wallet or purse, or to be placed in the retail environment within range to eavesdrop on transactions. Similarly, exposure of the information may be possible while the device is being mailed to the consumer; however, issuers are using techniques such as including RF shields in the mailing envelope, removing the cardholder name from the contactless chip and using alternate account numbers to eliminate this risk.

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

Contactless payment information as read from a contactless payment device by an illicit reader cannot be used to create fraudulent contactless transactions, or to create a counterfeit payment card. See question 2 for examples of the security measures that are used at the card and system level to prevent fraudulent transactions.

Even if contactless payment information is read illicitly, it is of no use in creating a fraudulent contactless payment transaction. The security implementation currently recommended 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.

If a criminal tries to pay for any purchase using a magnetic stripe card programmed with illicitly captured contactless payment information, the transaction will be denied by the issuer authorization system. Criminals will also not be able to create counterfeit contactless payment devices using the illicitly captured information as they would not have access to the issuer's strong encryption key.

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

As with all credit and debit payment cards, consumers can minimize any 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 be aware of this potential risk as they should be aware of other external risk factors that pertain to their personal information.