



## Smart Card Alliance Contactless Payment Security Statement

*The Contactless Payments Council of the Smart Card Alliance prepared this statement in response to recent reports that question the security of contactless payment cards and devices.*

Contactless smart card technology includes strong security features optimized for applications involving payment and identities. Every day tens of millions of people around the world safely use contactless technology in their passports, identity cards and transit fare cards for secure, fast and convenient transactions.

Regarding recent questions raised about contactless payment as offered by American Express, MasterCard and Visa, multiple layers of security protect these transactions, making them safe for consumers and merchants. Some of these features are in the contactless smart card chip and some are in the same networks that protect traditional credit and debit card transactions.

Nothing in the recent reports supports the conclusion that a criminal could successfully complete a fraudulent contactless payment transaction in the real world. One reason is that the researchers conducted these tests in a lab setting using only contactless cards and readers and did not interact with the payment networks in any way. One cannot draw valid conclusions about the security of a payment *network* if you ignore the network.

Further, the researchers did not discover anything new. The payment brands and card issuers already understand how the technology works through their own research, and they designed security into the payment systems based on their prior knowledge of how contactless chips work and how the payment system might be attacked. However, each payment brand implements differently the security features available in the card or the network, so there is no one explanation of how payment transaction security works.

One example that is a common best practice for all the payment brands is the use of a unique contactless payment transaction identifier or security code. In this case, the contactless payment smart chip calculates a unique numeric value, or security code, that serves as a proof of authenticity for each transaction. This feature protects against the possible replay of any transaction data to create a fraudulent transaction. Any attempt to reuse these security codes would also fail because the payment system would reject the transaction. Furthermore, the card calculates these unique identifiers using secret information that is encrypted, never leaves the card and differs from one card to the next, which prevents successful cloning of contactless cards. Thus, even in the unlikely event a

fraudster is able to record information from a contactless transaction, it would be useless.

This is only one example of many security techniques in use, but it is representative of the high levels of protection for transactions using contactless payment devices from American Express, MasterCard and Visa.

Another question raised by the researchers was the risk to consumers based on the fact that the cardholder name, account number and expiration date could be read from some cards tested.

In fact, many contactless payment cards in the market today do not include the cardholder name on the chip. As industry best practice has been evolving toward not including cardholder name in contactless transactions or on the chip, questions about this will diminish.

The contactless payment infrastructure does not rely on the electronic exchange of cardholder name information. The only information transmitted during a contactless payment transaction is the payment account information or an alternative number that is needed to complete a contactless credit or debit card transaction. The cardholder name being present is a carryover of the existing magnetic stripe card data present on most traditional credit 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.

If you have more questions please email them to us at:  
[info@smartcardalliance.org](mailto:info@smartcardalliance.org).

### **About the Contactless Payments Council**

The Smart Card Alliance Contactless Payments Council was formed to focus on facilitating the adoption of contactless payments in the U.S. through education programs for consumers, merchants and issuers. The group is bringing together financial payments industry leaders and suppliers and will be reaching out to involve the merchant community. The Council's primary goal is to inform and educate the market about the value of contactless payment and work to address misconceptions about the capabilities and security of contactless technology.

### **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>.

Media Contact: Deb Montner, Montner & Associates, 203-226-9290,  
[dmontner@montner.com](mailto:dmontner@montner.com).

# # #