Investigating the myths and realities of contactless payment

Questions & Answers

July 2013 - Updated April 2016

There has been much recent coverage in the media (press, web, blogs….) about the perceived security vulnerabilities of contactless payment - with several exaggerated cases reported in some detail.

Rather than a pragmatic analysis of risk, the vast majority of reports appear to compound inaccurate 'urban legends' – the kinds that typically appear during the introduction of any new technological innovation.

At a time when banks in particular, and the whole payment industry in general, are investing considerable sums of money in infrastructures (payment terminals, cards, mobile phones…) that offer fast, convenient and secure contactless payments, the Smart Payment Association (SPA) feels it is important to explain exactly what contactless payment is, how it works and how secure it is.

1. What is a contactless payment?

Contactless payment offers you the opportunity to pay for goods and services without the need to insert your card into the payment terminal – or to enter a PIN code. You simply hold the card in front of the terminal (and, for the vast majority of terminals on the market, on the screen).

The typical distance between the card and the terminal is 2 to 4 cm (less than two inches). However, to keep things simple, the large payment brands have popularized the idea of touch/tapping the card onto the terminal to carry out the transaction.

As a result, contactless payment is enabling a simpler and more convenient way to pay for small purchases (typically up to the value of 20€).

Contactless payment is also possible through a mobile phone if the device has NFC (Near Field Communications) capabilities. You simply hold the phone next to the payment terminal to carry out a contactless transaction - in the same way as you would do using a conventional contactless payment card.

Contactless payment by card

2. How do I know if I have a contactless card?

Contactless payments can only be made using cards with contactless payment capabilities enabled. The payment industry has developed an internationally recognized logo that appears on such cards.

If you have this logo on your payment card, you're ready for contactless payment. If you are in doubt, or if this functionality needs to be activated prior to use, please contact your bank and/or consult its usage terms & conditions

3. How does contactless payment work with an NFC smartphone?

We recognize the mobile phone plays a hugely important role in our daily lives: it wakes us up with its alarm clock, we check our daily schedule through its diary, it guides us towards our next destination thanks to inbuilt GPS and much more besides. So why shouldn't it allow us to pay for goods and services, or to receive discount vouchers and promotions that are automatically redeemed during payment? It should!

As a result, a few years ago the payment industry, in a joint effort with the mobile world, began discussions about how to securely enable payments with a mobile phone.

Through this development the term NFC was born. It is a way of carrying out transactions and services in the 'near field' (or short distance) of typically just a few centimeters.

This NFC technology is now stable, and is being introduced by banks and mobile telecom operators in many countries across the world.

Contactless payment by phone

4. How do I know if a given store accepts contactless payment?

The major payment brands, such as Visa or MasterCard, have prepared various advertising and signage packages to highlight whether stores accept contactless payment. You'll usually see a sticker affixed on the store's door if contactless payment is accepted – similar to those advertising debit or credit card acceptance.

In addition, you can tell by looking on the payment terminal itself. If it has contactless capability, and your purchase is below the standard level of 20€, the terminal's screen will display a specific logo inviting you to pay by contactless. Depending on the terminal model, you may also see little lights glitter above the screen.

You can therefore touch/tap your card (or NFC phone) to a certified payment terminal with a visible EMV logo and make a contactless payment.

5. How does contactless payment actually work?

As you can imagine, it is quite a technical process. To simplify, your contactless payment card has an embedded antenna to establish a communication channel between the card's microchip and a payment terminal.

This antenna uses the Radio Frequency (RF) field sent by the payment terminal and converts it into electricity – which is then used to make the microchip work. Then the chip can start communicating and exchanging information with the payment terminal over this RF field. All this happens in less than 500 milliseconds, which explains why a contactless payment is so quick!

6. How secure is it?

In the same way a contact transaction (where the card has to be inserted in a terminal) is very secure, so too is a contactless transaction. The first statistics for contactless transactions corresponding to 2014 indicate a fraud level of 0,015 % (Observatoire Banque de France 2015) a figure which is an intermediate value between the fraud level for contact card payments and the one observed for cash withdraw in ATMs. Moreover this fraud is almost exclusively due to the fact that the card is lost or stolen. This confirms that the fraud originated during the transaction is marginal and it matters to understand the reasons for this:

First the distance between the card and the reader is very limited (2 to 4 cm/ 1-2 inches typically). This makes it difficult, if not impossible, for a fraudster to insert any 'listening' device in between. The same applies to mobile contactless payments using a mobile device. In that case however the vulnerabilities of the operating system of the mobile device requires the storage of the payment data in a secure environment within the mobile. Two approaches are at present used:

- a hardware environment, the embedded secure element (eSE) able to protect the payment data with a level of security equivalent to a chip card
- a software environment, the Host Card Emulation (HCE), more vulnerable which requires the use of additional countermeasures, such as the use of tokens

Second, the payment card product (contactless or mobile) itself is also protected by 'counters'. These record the number of times the card is used in contactless mode. When a specific number has been reached, the card has to be used in contact mode, using his PIN code or in some countries may still be operational in contactless mode with an online verification of the PIN code. The number of times a card can be used in a contactless mode is defined by your bank – typically 10 times.

After this successful contact transaction (when the PIN is entered), the counters are reset to allow you to use the card in contactless mode again.

So, in the very worst case of a card being stolen just after it has been reset, the thief could make a maximum of 10 transactions of no more than 20€ each time – a maximum of 200€.

However, banks are aware of this threat and are using advanced security software to detect abnormal use patterns – for example 3 or 4 consecutive contactless transactions within a period of a few minutes or hours. Normal contactless usage is lower than this, and so your bank will block any further contactless transactions. In most cases, banks offer a 100% refund on any amount stolen.

7. Could a thief 'listen' to the information sent by my card

to the terminal during a payment?

As we have discussed above, the distance between the card and the terminal is very limited, which makes it very difficult, if not impossible, to install any kind of 'interception' device able to capture the data moving from card to terminal.

Should a successful case be highlighted, it would be a simple process for law enforcement authorities to identify all the locations where fraudulent transactions were made. Indeed, to complete the transaction the payment terminal must be registered by the bank acquirer.

Some recent cases have been reported where mini-cameras were installed above the card keypad in gas station self-service payment terminals – and the thieves were easily located and arrested.

8. Could someone standing near me fraudulently carry out a face to face transaction if my card is still in my wallet or jacket?

Again, the maximum reading distance is a just few centimeters so the thief would have to get really close to you, or use an extremely big antenna powered by a very large battery. Successful attacks have been reported in academic papers, these fraud cases have been demonstrated in 'lab conditions' by universities and other research bodies, with access to expensive equipment and deep technical knowledge. While they are theoretically possible they are very unlikely to occur in the real world due to the technical complexity for the thief.
Added to this, as described previously, only a limited number of transactions can be carried out before the transaction counter is blocked - thus limiting the 'interest' in the thief investing in the technology to do so. In addition, the maximum amount by transaction is capped. Moreover the fraudulent transaction can only be presented by a registered terminal, recorded in the bank's system (hour, minute), and cross referenced with the precise location (metro line/station) where the fraud occurred, CCTV systems would enable easy identification of a potential suspect.

9. Could someone use the retrieved information to perform an eCommerce transaction ?

In the unlikely event that a thief would take the risk to build such a complicated system, they would not be able to steal any more information than is readable by any assistant or waiter using your card in a shop or restaurant (name, card number, expiry date…).

But even this is being addressed. In the latest generations of contactless payment cards specifications issued by the major payment schemes, crucial information – such as cardholder name - cannot be read in contactless mode.

As a result, the information scanned would not be enough to re-create a fake card, or to perform fraudulent web purchases. They would have none of the data requested during an online transaction - no cardholder name, no 'clear' information of whether it is a Visa or MasterCard card, no 'CVV' 3 digit security code (that only appears on the back of the card).

10. Can contactless transactions be made by unwittingly holding a bag close to the payment terminal?

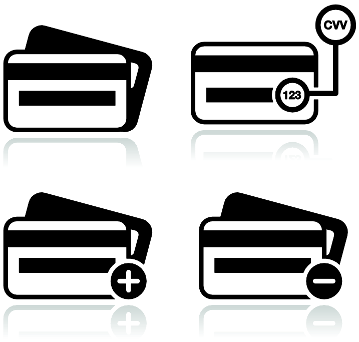
This is one of the many 'urban legends' about contactless payment that we see from time to time on the web.

First, the very short reading distance between card and terminal makes this very unlikely from a technical point of view.

Second, the payment terminal does not work alone. It must be activated by the cashier, who manually enters the amount to be paid on the keyboard, or it is automatically 'piloted' by the till sending the amount of the purchase to the payment terminal.

CVV Digit

Finally, articles or blogs also report large amounts of money being taken fraudulently or accidentally from cards. This is simply not possible as the system (card and terminal) is only set to allow transactions up to a certain amount only (typically 20€) without PIN, precisely to reduce this risk.



Any other question?

Contact SPA at

info@smartpaymentassociation.com