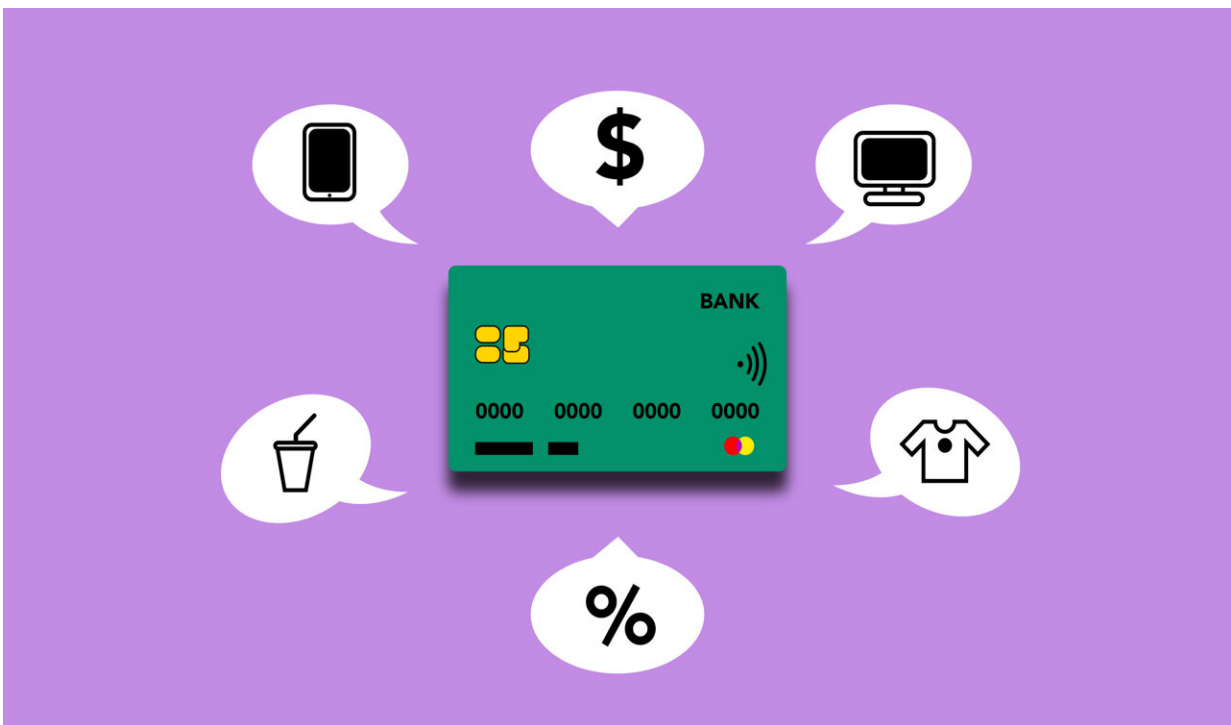# Could your contactless bank card be vulnerable to virtual pickpocketing?

March 1 2016, by Ahmad Lotfi

Credit: Monstera Production from Pexels

Thieves technically no longer need to reach their hands inside your pockets to steal the money from your purse or wallet. A recent viral photograph of someone on busy public transport with a point-of-sale card reader sparked fears that virtual pickpockets could swipe such a device against passengers' bank cards and take money from their

accounts without them realising. But how vulnerable are we to such attacks?

Contactless payment cards include a small antenna, a memory bank and an embedded microprocessor that can perform secure calculations and communications. A card reader sends out an electromagnetic field that both supplies power to the chip in the card and exchanges data with it via radio signals. When this happens, it sets up a connection that can code and decode information so payment details can be sent securely.

> What's the #legal position if you're victim of a #Digital #Pickpocket? https://t.co/MVIVC3DLUd #Contactless #Card pic.twitter.com/VyX6SVjSaw
>
> — James Teagle (@JamesLawBlacks) February 24, 2016

The fact that the chips can be passively read in this way without further action from the card's owner means that any active device brought close to the card can establish a link with it and complete a transaction. This means that the idea that you can be virtually pickpocketed by someone carrying a secret card reader is correct. But the thief would have to correctly locate where in your clothing or bag your card was and then bring their device within 5cm of it. And the likelihood of finding yourself in such close contact with someone carrying a card reader is very small.
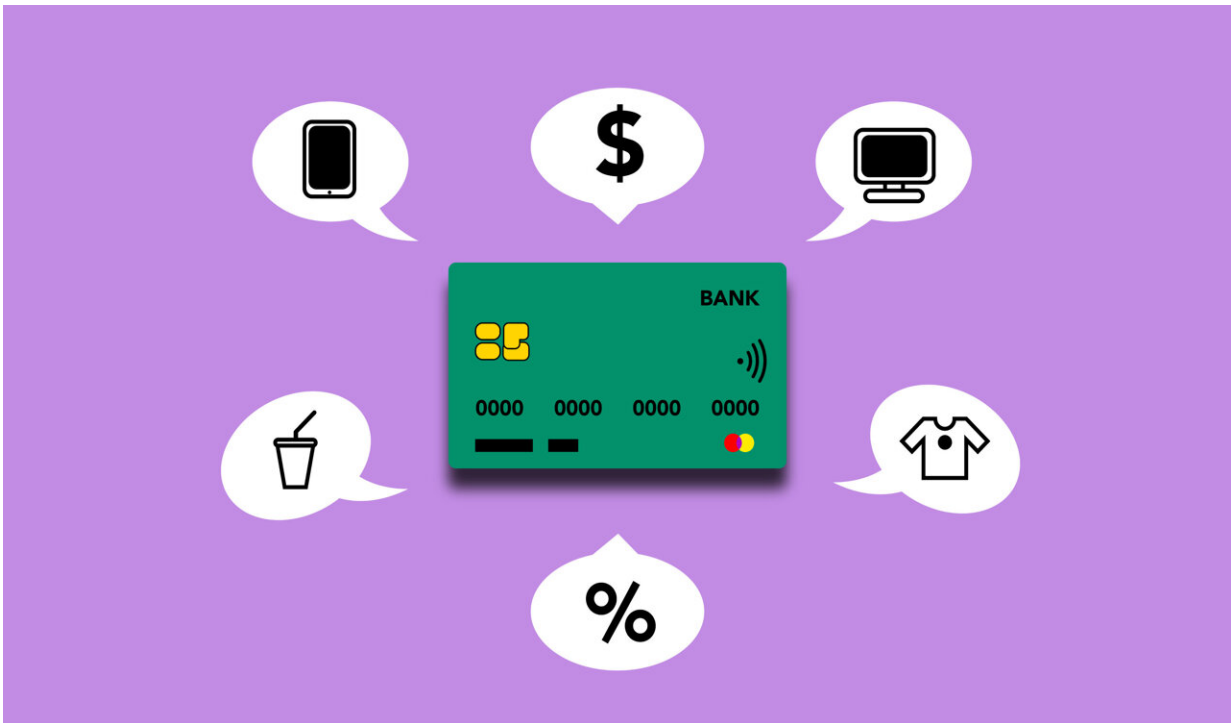
Credit: Monstera Production from Pexels

Of course, if your card itself is stolen then thieves can use it repeatedly to take money from your account. Even if you report the card lost or stolen and a block is applied to further activity, transactions can be processed by offline card readers and so won't encounter the block and so the money will still be transferred.

Minimal risk

Despite these flaws, the risks of theft remain so small compared to the total amount of usage that they're practically insignificant. There are over 79m contactless cards now in circulation in the UK (as of December 2015) and more than 140m contactless transactions are made each month. So far, errors and reported crimes have been rare. The total

annual contactless fraud loss was £153,000 compared with total spending of over £2.3 billion in 2014.

Contactless cards do come with built-in security. The chip on the card generates a unique coded message (cryptogram) and digital signatures to protect the payment from being intercepted. Banks set a limit on the number and value of transactions that can be made via contactless payment and repeated payments are forbidden.

One way of making contactless payments more secure would be to move to an active technology (as opposed to the passive chips) such as that found in smartphones or other devices that run programs such as Apple Pay or Android Pay. These devices create their own "near field communication" signals that are switched off when not being used to prevent accidental or unauthorised payments.

While you still have a contactless card, however, there is a more low-tech way of protecting your money. A metal case, protective sleeve or even some aluminium foil will prevent a device's signals from reaching the card. Or you could avoid putting your card where it can be easily accessed. Despite the minor security drawbacks, contactless cards have proven to be a very useful communication standard and provide connectivity and convenience for many innovative applications.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation