A forced PIN for all credit cards won't stop the biggest fraud

July 31 2014, by Asha Rao

A typical credit card includes your signature which anyone can copy. Flickr/Beau Giles, CC BY

Put the pen away when you next take out your credit card as from tomorrow (Friday August 1) Australians will no longer be able to use their signature when completing a transaction in a store. It's PINs only from now on, although this will apply only in store and not for online transactions.

According to PINwise, an initiative of the Australian payments card industry, using a PIN (personal identification number) for credit and debit card purchases in store is "safer and faster than signing". But is this really the case?

Both PINs and signatures are means of authentication for proving that you are who you say you are. Or in the case of credit cards, of proving to the merchant that it is your credit card and you have the right to use it.

Thus, for the usage of credit cards in store, the signature and the PIN takes the place of the password for online transactions, whereas the physical card takes the place of the "login" credentials. Now, which of these is safer – and why?

A signature is not secret

The problem with signatures is that the signature itself – the "secret" information – is written on the card, allowing a person to acquire it if they get hold of the card.

Also, when authenticating with a signature, you are expecting the merchant, a human, to actually verify that the signature matches the one on the back of the card. Aside from the fact that the merchant is not a signature expert, often there is no attempt to verify the signature.

A PIN, on the other hand, is not stored on the card, or at least, is not supposed to be stored on the card. In addition, we do not need to depend on the merchant to verify the PIN – the EFTPOS machine does that automatically – taking out the human factor, which has been shown, time and again, to be the weakest link in the security chain.

In addition, the EFTPOS machine is tamper resistant and difficult to break into it. Even if it is broken into it will wipe the information stored

in it.

A further fact is that when you use a PIN, you are technically using two-factor authentication – a physical card that you possess, and a PIN that you know (or rather, remember). Using a card with a signature is only one-factor authentication, since the signature is on the card.

Some people have suggested that having photos on the card would make them more secure than PINs. This is not necessarily the case, as again, we expect a human to check that it is your photo on the card – and as with checking signatures, humans are again the weakest link. After all it is your money, and not theirs!

Where the fraud occurs

We then come to the question of whether this change, from signatures to PINs, makes all transactions safer? Not really – it only makes "card present" transactions safer. When using your card to make online purchases, your PIN does not help.

Thus your bank or credit card company may require you to use another security factor such as a text message to your mobile phone before you can complete certain online transactions.

There is also the question of how much fraud would such a change, from signatures to PINs, reduce? According to figures from the Australian Payments Clearing Association, for the financial year ending 2013, fraudulent transactions on credit and debit cards issued in Australia exceeded A$281 million.

The majority of this was "card not present" (CNP) fraud, which increased from A$183 million to more than AU$219 million from 2012 to 2013. CNP is usually a transaction over the phone, mail or internet.

On the other hand, counterfeit or skimming fraud remained at A$37.2 million. With the move from signatures to PINs, the banks will be hoping that the latter figure decreases. Whether this will happen remains to be seen.

Is a PIN enough?

The other worry is whether a four-digit PIN is sufficient – the extra security features of locking the card after three wrong attempts goes some way to address this, but it does not prevent people using weak PINs, such as a date of birth.

We need to consider the security over the new ways of tapping a credit card on the EFTPOS terminal – the PayWave, PayPass and Tap and Go facilities. These have been introduced mainly for convenience and don't always need a PIN to complete a transaction. The banks have capped the transactions – mostly to A$100 maximum – and hence must believe that the level of fraud possible is worth the risk.

So what can we do to be more secure? The best way is to keep an eye on your transactions and report any anomalies to your bank as soon as possible.

With online banking, this is easier to do than in the past when one had to wait for the statement to arrive. Taking the extra time to make sure that the transactions are yours, and not a thief's, is worth it – it is your money, after all.

Provided by The Conversation