consult hyperion
securing tomorrow's transactions

A Touchy Subject

There are increasingly frequent claims that contactless smart payment cards are insecure because they can be read while in your wallet or pocket. Can this really be true? And if so, is this threat really any greater to consumers than what already exists? ***John Elliott*** *of Consult Hyperion investigates*

One of the most exciting new developments in payment technology has come in the form of "contactless" payments, the name given to payment card transactions that require no physical connection between the customer's credit card and the merchant's sales terminal. Instead, customers simply tap their card against a contactless card reader to make a purchase. Today, rather than only being used to buy fast food and transport ticketing, these cards are now also starting to be accepted in book shops and stationers. Latest figures from UK Cards indicate that, in the UK, there are currently more than 20 million contactless credit or debit cards issued and 80 thousand readers where they can be used at merchants.

HSBC has been the latest bank to announce that it will start replacing customer debit cards with contactless cards[1]. But, interestingly, they are allowing customers to opt out if they would rather not have the new contactless technology in their wallets. Of course, we can only speculate whether this decision has been taken because stories continue to circulate about these cards being unsafe - and HSBC wants to afford its customers peace of mind. But, what's more likely is that it's simply due to the fact that the contactless ecosystem is still in its infancy, so many HSBC customers might not benefit from having these cards in their wallets just yet, so the Bank is choosing to give its customers more choice. However, this investigation is not looking at the merits of contactless payments versus cash payments, or contactless versus Chip & PIN. The aim of this paper is to take a detailed look at the technology itself, and to establish whether the threat of 'Snooping'/'Sniffing' (where it's claimed certain card details can be read 'over the air' by fraudsters), is a major concern for consumers and to see what the risks are, if it's true.

An new industry created from fear

Ever since the banks and the financial services industry started rolling out contactless payment cards, and merchants adopted contactless payment terminals, a new security industry has grown warning us of the threat of having your card data read. In fact, you've probably seen the articles or YouTube videos that claim that your new contactless payment card details can be read by an attacker while your card is in your pocket, perhaps closely followed by a sales pitch for some sort of foil sleeve which can prevent your card from being read[2]. So as part of this investigation I thought it would be interesting to see exactly what information can be read from these cards, what kinds of fraud an attacker might conduct with it, and how these risks of contactless data loss compares with if your card were stolen or cloned.

[1] http://www.guardian.co.uk/money/2012/may/09/hsbc-joins-contactless-payments-movement
[2] http://wreg.com/2012/01/10/electronic-pickpocketing-goes-viral/

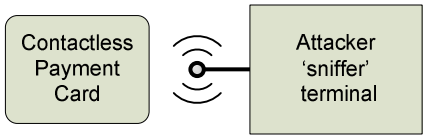


Figure 1: Attacker home-made terminal can read some data from your payment card in your pocket

What can be read?

When a card conducts a transaction with a card reader, the reader is the master and the card is the slave. So, to some extent, the card will do what it is told, and this involves giving up some information about the card. The necessary specifications are easily obtained and the kit is cheap, so it is not hard to make your own contactless payment card reader to obtain the free-read data from all contactless cards to which you can get close enough (less than 10 cm is what the standard says, but attackers can increase the power of their reader and extend the range)[3]. The table below shows the information that can be read from the contactless chip, and compares it with related information that can also be read by visual inspection from the face of the card i.e. if you lost your card or it was stolen and used for fraud.

Data/information available on a bank card	Card face data (visually available)	Chip data available over the contactless interface
Primary Account Number (PAN). The long number across the middle of the card which identifies the issuing bank and the account which will be used to ultimately pay.	PAN	PAN
The name of the cardholder	Cardholder Name	Some early contactless cards do allow it to be read, but increasingly this is not the case.
Expiry Date: The date after which the card is no longer valid.	Expiry date	Expiry date

[3] The ISO/IEC 14443 Proximity Card standard is used, the same as that used for many contactless transit cards.

Data/information available on a bank card	Card face data (visually available)	Chip data available over the contactless interface
Security Code: A code which is not allowed to be stored by merchant systems but is used for 'card not present' (CNP) payment authorisation. Knowing this code is supposed to indicate that you are in possession of the card, rather than just having a copy of the card details from merchant records.	Security Code (going by various names such as CVV2 (Visa), CVC2 (MasterCard), 4BDC (Amex))	The security code printed on the card and used for card not present transactions is **not** available over the contactless interface.

Let's look at each data element in turn:

Cardholder Name

The UK Cards Association recommends that cardholder name is not provided via the contactless interface. So, it should not be possible to be sniffed by our attacker with his homemade reader. Recently, it has been shown that some contactless payment cards in the field do allow the cardholder name to be read[4]. This will probably be prevented in the next generation of these cards, and other current cards already do not allow the cardholder name to be read. However, your name is written on the face of your card and so might be observed by someone each time you take out your card to use it, so can easily be obtained whether you're paying via contactless, Chip & Pin or using the magstripe.

PAN

In contrast, the PAN *can* be read covertly from any contactless payment card while the card is in your pocket. The PAN is the long number, again also found on the card face and it is comprised of several components including numbers identifying your issuing bank, the bank product, your account within the bank and a check digit at the end so that a computer can tell if the PAN has been entered incorrectly when used online.

Expiry Date

The expiry date can be read, and is the same as the one printed on the face of the card.

Security Code

Finally, a security code cannot be read over the contactless interface by an attacker. Associated with a payment card are several security codes, which are all different from each other. The idea is that they help show that the card is actually present at the time of a transaction:

- There is one printed on the card (usually on the back), sometimes called CVV2. This is the one that you should be asked for (last 3 digits) when you make a payment on the internet or over the phone.

[4] http://www.theregister.co.uk/2012/03/29/visa_cards/

- There is one in the card magnetic stripe, sometimes called CVV. This is read when your card is swiped in a magnetic card reader and cannot be read from any other source. The idea here is to prevent a fraudster from making a magnetic stripe card clone of your card if they only collect your other card details from, say, an internet merchant.
- There is one on the chip that is used on the contactless interface, sometimes called iCVV. If a fraudster reads your iCVV, they do not have your CVV2 or your CVV and so do not have enough information to successfully clone your chip data into a magnetic stripe card, or make an internet or telephone payment, provided that the merchant follows the payment scheme rules and asks for the CVV2 when all purchases are made. More on this below.

According to payment scheme rules, the merchant is not allowed to store any of these security codes with your other card details. If they break this rule, the payment schemes would investigate and could result in heavy fines and loss of the ability to accept payment cards.

So, how scary is that?

Well, the short answer is, that's not very scary at all, for the cardholders, and the threat is much greater should you physically lose your card and a fraudster uses it, than if information was obtained contactlessly. But, let's now look at a few frauds discussed in the press recently that attackers might want to try, and see whether they can do it with the data sniffed from your contactless payment card as easily as they can with physically having all your card data.

Privacy and identity threats

There are some people who don't like their name being available from their payment cards in the same way that I don't like my name and address being available from my UK Driving Licence. It can be argued that there is no need at all for cardholder name to be available from the face of the card. There might be a bright future where anonymity is preserved, but right now this is the way it is – as soon as you use your card (Chip & Pin or contactless), that information can be viewed by anyone who wants to look, cashier or fraudster. So, if you don't want anyone to be able to read your name or your card number, then you should not use payment cards at all. Every time you do a Chip & PIN transaction, these are captured by the merchant. However, for contactless transactions, cardholder name is not used, so it could be argued that things are moving in the right direction with the introduction of this technology in helping to preserve identity.

Cloning your contactless payment card

This is perhaps the hardest attack to carry out because the attacker would need to know how to program a contactless chip (which is no mean feat) and would also need more data than he has obtained from reading your card. When the reader does a transaction with your card, the card chip is required to perform cryptographic operations that prove it has secret cryptographic keys that are only known to the card-issuing bank. For each transaction, the cryptographic calculation required by the terminal changes, based on transaction details, so it has to be calculated each and every time and cannot simply be stored in advance by an attacker.

Therefore, cloning your contactless card using only the details the attacker has sniffed from your contactless card is not possible. These are the same reasons that Chip & PIN cards cannot be cloned. The chip provides an extra level of difficulty for attackers.

Making a counterfeit magnetic stripe card with your details

Magnetic stripe cards use older technology that preceded chip payment cards like Chip & PIN and the new contactless payment cards. However, modern payment cards still have the magnetic stripe so that the cards can be used around the globe at merchants where chip card terminals don't yet exist (e.g. much of the US). It is also there as a fall back in case a chip card terminal fails, so the card is swiped and your signature is provided as authentication.

If you have someone's payment card, it is trivial to copy the magnetic stripe details and write them to another magnetic stripe card of your own[5] before giving it back. This was a very common fraud before chip cards, known as skimming. However, the information needed to correctly populate a magnetic stripe requires more data than the attacker has managed to read from the contactless payment card in your pocket. In particular, the Security Code required to make the magnetic stripe data (CVV) is not readable. The iCVV held inside the chip card is different from the security code printed on the card face (CVV2) and different again from the one held in the physical magnetic stripe details (CVV).

Therefore, making a magnetic stripe card using only the details the attacker has sniffed from your contactless card is possible, but the details would be wrong and should be detected when you go to use it. I say *should,* because merchant terminals that accept magnetic stripe cards should go online to allow the card-issuing bank to verify that all the details are correct. This process should spot the missing cardholder name and also the wrong security code and the payment transaction should be declined. If the attacker is lucky enough to find a payment terminal that accepts magnetic stripe cards without going online to check, then they could conduct a fraudulent transaction. However, in this case, it is the merchant or their Acquiring Bank who would be liable, as they had not followed payment scheme rules/guidelines and checked the transaction details online. And you, the consumer who had some of your contactless card details sniffed, would not be liable for a penny.

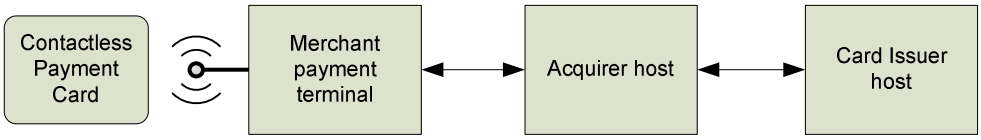


Figure 2: Online payment card transactions are sent from merchants to acquirers to check details with the card-issuing bank

Making a fraudulent payment with your card details

The final attempted fraud we will look at is the attacker using your sniffed card details for a 'card not present' (CNP) transaction, say, to purchase something on the internet or over the phone. The schemes say that in order for a merchant to accept a CNP transaction without being liable for fraud, they must collect all of the following:

[5] E.g. using a MSR206 reader/writer, http://us.ute.com/products_info.php?pc1=74&pc2=148&rbu=5&pid=386

- Cardholder name
- Billing address
- PAN
- Expiry date
- Printed security code (CVV2)

Once again, as outlined in the earlier table, our attacker only has two of these by sniffing your contactless payment card. The idea is to require so much information that an attacker would not bother to find it all out. In order to make a fraudulent transaction using only your contactless card information, he would need to find a merchant that is prepared to accept only PAN and Expiry date and these are increasingly hard to find. However, as Channel 4 News recently reported, some merchants as big as Amazon are accepting purchases without requiring the full details that the payment schemes dictate.[6] We tested this and it was indeed true. It is not clear how long this has been going on and how long it will be allowed to continue. However, again because payment scheme rules/guidelines have not strictly been followed, this makes the merchant (Amazon) liable for any fraudulent cards that they accept. However, the success of Amazon would indicate that this can be a risk worth taking. It should be remembered that in the case of internet purchases, the attacker has to supply an address at which they wish to receive the goods, so this adds an extra level of security checks.

Our verdict: are we safe from sniffing?

So, the question remains: how much do contactless cardholders really need to worry about 'sniffing' or 'snooping'? According to the payment scheme rules, cardholders are protected against both of these threats – provided that they do not break the rules (such as revealing their PIN). After all, debit and credit card transactions of all types come with their own risks, just as walking down the street with a wallet full of cash can open you up to a risk of being mugged.

However, all the examples of successful fraud outlined in this investigation are where a bank or a merchant has not fully implemented the security protocols set out and supported by the payment schemes. In these cases, the banks or merchants are taking the risk and are liable for any fraudulent payments, not the cardholder.

But the good news doesn't end there. Security concerns aside, contactless cards have been designed to speed up payment processes and ultimately make queuing for things much more efficient. As with any new payment technology, much like when cards were introduced, you're being offered more convenience, but perhaps slightly more risks, but this technology is still safer than carrying cash.

So the general rule of thumb with contactless cards, and with a 'normal' card for that matter, is to keep your card safe and close by and don't reveal your PIN to anyone. However, if you still have

[6] http://www.channel4.com/news/millions-of-barclays-card-users-exposed-to-fraud

concerns about what can be read from your contactless payment card in your pocket (i.e. your card number and name), then I suggest that you simply wrap it in a piece of kitchen foil, since that alone will prevent any reader from reading it unless the foil is removed. That should give you total peace of mind – as well as a much better alternative to the card shields vendors who will no doubt continue to fuel the misconception that contactless cards are not safe.

Acknowledgments

The author wishes to express his sincere thanks to his colleagues at Consult Hyperion for supplying and checking the facts in this article. In particular:

- Richard Allen
- Dave Petch
- Andrew Whitcombe
- Dave Birch
- Simon Laker

For more information, please contact Nick Norman, Head of Sales, Consult Hyperion

+447 966 003 332 or nick.norman@chyp.com