# [**Finder**](https://www.finder.com.au/nfc-credit-cards)

# Near Field Communication Credit Cards

## Near Field Communication (NFC) is a key element of contactless credit card and mobile payments. Read this guide to find out what it is, how it works and the way it affects your accounts.

Making tap-and-go payments with a credit card or mobile service such as Apple Pay is becoming more and more common. More than 50% of all in-store payments in Australian are now made with contactless credit cards according to multiple reports from key stakeholders including Westpac, Mastercard and Visa.

But for consumers, there’s still some uncertainty about how [contactless payments](https://www.finder.com.au/contactless-payment) work and the way they could affect our credit cards and accounts. This guide explains everything you need to know about the technology used for most tap-and-go options (NFC) so that you can understand what goes on when you use your card or phone to make a payment.

### What is NFC?

NFC, or Near Field Communication, is a type of technology that allows wireless communication between devices that are a few centimetres apart. It doesn’t require an Internet connection, and instead uses microchips to transmit data via shortwave radio frequencies.

When one NFC-enabled device is close enough to another NFC device, a connection can be established and data shared between them. For example, when you tap your credit card on a contactless card reader or when you use a transport card to catch a train or bus. In both these cases, the card communicates data to the reader to initiate and complete the transaction using NFC technology.

### How is NFC technology used in contactless credit cards?

There are currently two main brands of contactless credit cards in Australia: Mastercard PayPass and Visa payWave. American Express also provides Australian credit cards that are simply branded “Contactless” and carry the universal contactless symbol.

All of these options have NFC microchips embedded in the cards. These chips allow the cards to communicate payment data to contactless card readers so that payments can be processed.

Another feature of contactless credit cards is that transactions under $100 don’t require PIN verification. Instead, you can literally just “tap and go”.

Contactless payments are generally much faster than traditional payment options. The Smart Card Alliance, a US-based industry body, reports on its website that contactless card payments can speed up the checkout process by 30-40%. Research from American Express has also found that contactless transactions are 63% faster than cash and 53% faster than using a traditional credit card.

### Are contactless payments secure?

When NFC technology was first introduced to credit cards, some media reports raised questions about its security. In particular, could someone steal your credit card data using another NFC device?

The short answer is that it’s highly unlikely that would ever happen. The information transmitted by a credit card’s NFC chip is encrypted using the same technology as regular chip-and-PIN cards to help keep your personal information safe.

This technology also requires close proximity between devices for a transaction to occur. So even if there were a device that could get your details off a contactless credit card, it would have to be a few centimetres away from your card to actually work.

Another factor to consider is that NFC card readers are extremely sensitive and usually reject transactions if more than one signal is detected. For example, let’s say you had a tap-and-go public transport card (such as the Opal card used in Sydney or the Myki in Melbourne) and a credit card in your wallet. If you went to make a payment at the checkout without removing your credit card, most readers would pick up both NFC chips and be unable to process the transaction due to the conflicting signals. So you would have to take your credit card out and tap it against the reader to complete the transaction.

This sensitivity helps ensure that your tap-and-go payments are only processed on your selected card. It also prevents accidental double-payments if you tap twice, as readers can only process one transaction at a time.

### Contactless credit card theft

Physical theft is biggest security risk for contactless credit cards, because no verification is needed for transactions under $100. That means thieves could effectively use a card at many different locations to rack up hundreds and thousands of dollars in fraudulent charges. Key actions you can take to protect your credit card against theft include:

* Keeping track of where your card is at all times
* Not sharing your card with anyone else
* Regularly checking your mail for any new cards that may arrive
* Reporting lost cards immediately

[**Medium**](https://medium.com/@Vasco_bags/how-money-can-be-stolen-from-contactless-rfid-and-nfc-cards-cd74fea192a6)

# How money can be stolen from contactless RFID and NFC cards

Recently, a fundamentally improved version of money theft has been discovered. A new method of stealing money from cards equipped with PayWave and PayPass technologies. Criminals intercept the signals from such bank cards “out of the air” using hand-made readers.

Plastic cards with contactless RFID chips can be used only by attaching them to a PoS bank terminal. In this case, such cards in a PoS terminal “are not swiped” and not inserted.

There are methods now of money withdrawal from credit cards using the latest smartphone models, with a modification, a kind of RFID technology — the NFC device. To withdraw funds from the card, hackers just need to know the full card number and a month/a year of the end of service.

The cards of the MasterCard international system are equipped with PayPass chips, and the cards of the Visa payment system are equipped with chips with the name of PayWave. At the same time, both companies allow using their contactless technologies both on magnetic stripe cards and on newer cards with a square chip.

The convenience of using MasterCard-PayPass and Visa-PayWave systems is to simplify and speed up payments in stores. When making payments for small amounts with the cards with RFID chips, there is no need to sign on the cash receipt or enter your PIN-code into the PoS terminal.

Fraudulent schemes are meant to intercept NFC signals using illegal reader devices. RFID interceptors are highly advanced analogues of conventional contactless card POS terminals with increased functionality that capture and process electromagnetic waves. Such a device is usually equipped with an antenna, a special controller, connectors for extracting information from the reader, and pirate computer software.

To read the payment data, the fraudster will only need to have the reader approximately ten centimeters near the victim’s card.

That means, in the subway or ground transport at rush hour it will be done very easily and unnoticed. The stolen information is subsequently transferred to other participants, which the performer often does not even know. And they make clone duplicates of bank cards, which are used for cashing out black money.

The cost of an illegal RFID reader for attacking PayWave and PayPass cards is about one hundred dollars, while “kulibins” can make them out of components that can be ordered on eBay or Aliexpress.

So how can you protect your money from a hacker attack on a contactless card?

The simplest and most effective way to protect the card from a contactless reader is to purchase a special [RFID purse](https://www.kickstarter.com/projects/223985220/vasco-smart-packing-cubes-and-bags?ref=creator_nav) protecting the cards from being read. When attempting to read data, the swindlers’ machine will not be able to copy the information.

It is also advisable to have an alert set that informs of changes to the account balance using SMS messages or PUSH notifications. Alternatively, you can also reduce the amount that can be used when paying by card without specifying a PIN.

[**INVESTOPEDIA**](https://www.investopedia.com/terms/c/contactless-payment.asp)

Contactless payment is a secure method for consumers to purchase products or services via debit, credit or smartcards (also known as [chip cards](https://www.investopedia.com/terms/c/chip-card.asp)), by using [RFID](https://www.investopedia.com/terms/r/radio-frequency-identification-rfid.asp) technology or near-field communication (NFC). To make a contactless payment, a person simply needs to tap their card near a [point-of-sale terminal](https://www.investopedia.com/terms/p/point-of-sale-terminal.asp) – leading to the nickname “tap-and-go”. Since contactless payments do not require a signature or a PIN, transactions sizes on cards are limited. The allowable amount for a contactless transaction varies by country and by bank. Examples of non-credit or debit card contactless payments include transit cards, Apple Pay, Android Pay and Google Wallet

BREAKING DOWN 'Contactless Payment'

Contactless payment has become a popular payment method for smaller purchases. Most banks offer contactless payment cards and the new payment terminals are equipped for tap. Although there are still smaller shops that do not offer tap capabilities, many national chains have moved to tap capable payment terminals. The main advantage of contactless payment is that it speeds up transactions by taking out the step where a customer must enter his or her PIN. Tap customers speed up the line, so to speak, so that both the merchant and the customer see a time savings when contactless payment is used. Another benefit of contactless payment cards - at least for the banks and credit card issuers - is that consumers who tap tend to use their cards more frequently.

## Security Measures for Contactless Payment Transactions

Even with the convenience of contactless payment, many consumers are worried about the security of the cards. There have been stories in the media about criminals [skimming](https://www.investopedia.com/terms/s/skimming.asp) card data using smartphones to read the tap cards in consumers' wallets. For this reason, cardholders have zero liability if their tap card is used without their authorization. Moreover, the range at which a card can be read is very short and, even if the criminal is close enough to grab data and do a transaction, he cannot create a copy of the card. This is not true of magnetic strip cards. That said, the chip and pin card is still the most secure, as they can't be duplicated and they require data (your pin) that is not contained anywhere on the card.

If the skimmer gets your card data, his next step is to find a website that doesn't require the three digit code printed on the back of the card and run transactions under the credit limit. If a criminal steals your physical card, he'll likely head to the nearest store to buy $20 gift cards using tap. While annoying, you can dispute the transactions and get a new card issued. There are also protective card sleeves and wallets that block readers from getting to your card data in the first place.