

Looking after credit and debit cards and PINs

7 August 2017

The loss or theft of a credit or debit card can be worrying and inconvenient. But if someone also gets your PIN, you face an even greater risk of losing money. Banks typically cover any loss if you take reasonable care of your card and PIN and report any loss promptly. If you haven't taken reasonable care, you are unlikely to recover the money. Protecting your cards and PINs is therefore vital, as is selecting a secure PIN and knowing what to do if you lose a card.

Reasonable care

You need to take reasonable care of your cards, much as you do with wallets and keys. You don't need to know the exact location of your cards at all times, but you should know their general whereabouts, such as at home, in your bag or in your pocket. You shouldn't leave cards unattended in a wallet or purse, or anywhere a thief could remove them without being noticed.

It is not reasonable to leave your card:

- inside a car
- in a jacket pocket when the jacket is unattended in a public place, like a café
- in a hotel when you are out (unless it is in a hotel safe).

Remember to remove your card when using it at an ATM, shop, restaurant or any other outlet after making a purchase.

Losing a card

If you can't find your card, tell your bank as soon as possible. Banks have dedicated phone lines to report lost or stolen cards. If you are overseas, keep a note of the phone number with your travel documents.

Restricting card access to certain accounts

You can specify the accounts that are linked to a card. The fewer a thief or scammer can access, the lower any potential loss will be. Talk to your bank about which accounts should not have card access.

How to contact us

Selecting PINs

Follow these tips when making up a PIN:

- Avoid obvious number combinations or sequences (for example, 1234 or 0000).
- Avoid using birthdays, anniversaries, home addresses, parts of your phone number or other numbers easily connected with you.
- Avoid sequences that also form part of your card number.
- Use a different PIN for every card.

Protecting your PIN

Commit it to memory and never write it down. Don't tell anyone your PIN – and that includes family members, police or bank staff. Note that banks will never ask for your PIN. Never reply to any email asking for your PIN (or asking you to update your PIN). It's bound to be fraudulent.

Never store your PIN (even in disguised form) on any device, including mobile phones, computers, tablets or other electronic devices. If you have done so already, delete it and get a new PIN.

You should take reasonable care when entering your PIN at an ATM or an eftpos machine in a shop so as to stop someone from seeing it. If you think someone may know your PIN, contact your bank immediately and get a new one.

Case 1: Card left in unattended wallet

Mrs B's wallet, which contained her eftpos card, was stolen. She thought the theft happened when she got out of her car to open her workplace gates. She reported the theft to Police and made a formal statement.

The thief withdrew \$3,000 from Mrs B's account at ATMs. The loss would have been \$7,000 but for a foreign exchange bureau requiring that the thief supply identification.

The bank offered to cover half of her loss, but Mrs B complained to us that the bank should meet the full amount because she was not at fault.

We found she had not complied with the card's terms and conditions, which said she must not leave her card "in an unattended wallet, purse or vehicle or anywhere a thief could remove the card without being noticed". In our view, Ms B had not taken reasonable care of her card.

The offender also entered the PIN correctly on the first attempt. This strongly suggested she had not taken sufficient care of her number. It is all but impossible to select correct PIN numbers at random, let alone in the correct sequence.

We recommended she accept the bank's \$1,500 offer. She did so.

How to contact us

Case 2: Cryptic PIN details stored on phone

An unknown person used phone banking to transfer a significant sum of money from Mr G's account. Mr G did not understand how this could have happened and complained to us when the bank would not refund the stolen money.

We discovered he had lost his cellphone before the fraud happened, and that he had saved his phone banking registration number and PIN as a mobile number and an email address.

Mr G had attempted to disguise his telephone banking details, but the offender saw through this and accessed his account. Mr G had unintentionally given the offender the ability to commit fraud.

By recording his banking details on his phone, he had breached his bank's terms and conditions. This meant the bank did not have to reimburse the stolen funds.

Case 3: Grandmother "shoulder-surfed"

Mrs P went shopping with her teenage grandson and made a purchase at a retailer using an unshielded eftpos keypad. Unknown to her, her very tall grandson had seen her enter her PIN. During subsequent days, unauthorised transactions worth \$3,700 were made on the card. As soon as Mrs P realised her card was missing, she put a stop on it.

The bank denied the claim for reimbursement on the grounds that, by taking inadequate security precautions, she had breached the card's terms and conditions of use. It offered a goodwill payment of \$738.15.

Mrs P disagreed that she had breached the terms and conditions. She said she was unaware her grandson saw her entering her PIN. She kept the card secure, she had no reason to believe her grandson would steal from her, the PIN was not written down anywhere, and it was neither a sequential number nor easily identifiable in any other way.

We found Mrs P's grandson had almost certainly looked over her shoulder to see the PIN. The bank argued she had not taken reasonable care because the thief had learned the PIN. Our view, however, was that a customer must take reasonable care to avoid disclosing a PIN when keying it into a machine, but this would not always protect against a determined person. There is a limit to what customers can reasonably be expected to do to protect PINs, particularly when using an unshielded keypad. The standard of care required in such circumstances is that a customer must exercise a reasonable – not extreme – standard of care.

We found Mrs P had not breached her card's terms and conditions and was entitled to full reimbursement, less the standard customer liability of \$50. She and the bank accepted our view.

How to contact us