Reversing Bank Transactions

This fact sheet is for information only. You should get professional advice about your personal situation.

Main ideas

• There are 3 types of transactions that may be reversed

• Disputed credit and debit cards transaction may be 'charged back' into your account.

• Unauthorised transactions may be refunded into your account.

• Some mistaken payments can be reversed

• Act quickly – there are time limits to reverse transactions.

• You must provide good reasons for the transaction to be reversed.

In this fact sheet:

Chargebacks

Chargebacks allow you to request credit card and debit card transactions made through card schemes (such as Visa and MasterCard) be reversed.

You can ask for a chargeback in situations such as:

- the merchant (shop or service provider) did not deliver the goods or services to you

- the goods or services were not as described, counterfeit or defective
- you were charged multiple times for the same transaction
- you were charged the wrong amount
- the transaction was not authorised, or was fraudulent
- you cancelled a recurring transaction
- the merchant became insolvent.

To request a chargeback

Try to resolve the issue with the merchant first – this is the quickest and easiest way to get your money back. You may need consumer law advice about your rights against the merchant.

If you cannot resolve the issue with the merchant, contact your bank (or financial institution) immediately. Banks have a limited time to claim a chargeback, and the timeframes and the rules vary depending on the card scheme. Your bank claims the chargeback directly from a merchant's (shop or service provider's) bank.

To ask for a chargeback, write to your bank:

- Say you are requesting a chargeback of a transaction on your credit or debit card.
- Give details of the transaction, including the amount and the date.
- Give reasons why you wish to chargeback the transaction.

Keep a copy of the letter.

Whether your chargeback request is successful depends on:

- the card scheme's rules for when chargebacks can occur
- the terms and conditions of your contract with the merchant (for example, your rights to a refund or cancellation).

Get legal advice if you're not happy with the bank's response.

Unauthorised transactions

A transaction is unauthorised if you did not perform the transaction, or did not agree to someone else performing the transaction for you.

However, if the transaction was made with your knowledge and consent, then it is an authorised transaction.

Check your statements regularly to see if there are any unauthorised transactions on your account.

In general, you are not liable for unauthorised transactions. However, you may be liable for some or all of the transaction if you contributed to the loss or unreasonably delayed reporting the unauthorised transaction. Examples include:

- Giving someone authorisation codes or passwords.
- Writing your PIN on your ATM card or on a document you keep with it.
- Entering your banking login and password details on a scam website.
- Giving someone remote access to your computer (this often results in tracking programs being installed to steal log-in details and passwords).
- Downloading malicious files or software.
- Saving log-in details and passwords without adequate password protection or reasonably disguising the details, in a mobile phone which is stolen.
- Being extremely careless with your password or passcode data.
- Choosing a password that contains your birth date or name (if the bank can show they clearly warned you not to, and what would happen if you did).

You are not responsible for losses that happen after you reported the loss, theft or security breach to the bank.

You are also not responsible for transactions in some situations including:

- forged, faulty, expired or cancelled passwords, identifiers or devices
- mistakes or fraud by your bank, a merchant or their employees
- transactions using devices or passwords before you received those
- transactions incorrectly debited more than once
- losses that happen because the bank's priority number was not available, so long as you make your report reasonably quickly once you are able to get through
- any part of the loss that goes over any credit limits or other transaction limits (for example, a daily spending cap). Industry practices around reasonable transaction limits and security practices are considered if you had not set a cap
- if you had multiple security requirements in place and you didn't breach all of them (and the bank can't show you were more than 50% responsible for the loss)
- leaving your card in an ATM that did not have reasonable safety standards such as capturing cards that aren't removed after a reasonable time.

It's up to the bank to show that you likely contributed to the loss, looking at all reasonable evidence and explanations about how the loss occurred. Just because a transaction was performed using the correct device or password is not enough by itself to show that you contributed to the loss (but it can be significant factor when combined with other information or evidence).

You can read more about who is responsible for unauthorised transactions in the ePayments Code on the ASIC website.

If the bank claims you are liable for an unauthorised transaction, get legal advice.

To request a refund of an unauthorised transaction:

1. **Immediately** ring your bank. They must have a priority number so you can easily report unauthorised transactions and security breaches.
2. Tell them that there is an unauthorised transaction on your account.
3. Put a 'stop' on your account (for example, cancelling the card or disabling internet banking or online money transfers) to prevent more loss.
4. Change any passwords or PIN codes that may have been compromised, including changing your security questions.
5. Write to your bank confirming when you rang and told them about the unauthorised transaction and what the transaction was. Send this letter urgently, before the due date for payment on your credit card statement. **Keep a copy of this letter.**

You should get a written response within 21 days either telling you the outcome, or telling you they need more time to investigate.

You should get written reasons for the bank's decision, and any documents or other evidence such as transaction logs or audit trails.

To reduce the chance of unauthorised transactions:

- Do not provide authorisation codes or passwords to anyone even if you think they are from the bank, the government or some other reputable organisation.
- Keep your PIN or password secret. Do not use a PIN someone could guess, for example your birthday or part of your name.
- Never write your PIN or password on your card or on a document kept with your card. Memorise your PIN and do not write it anywhere. Do not let anyone see you entering your PIN/password at an ATM or EFTPOS machine.
- Report any unusual behaviour to your bank. For example, a merchant who passes your card through more than one piece of equipment, or who holds onto your card for an unreasonably long time.
- Use preventative measures such as multi-factor authentication, which is a security measure that requires two or more ways to prove your identity before gaining access.
- Turn on transaction notifications on your banking app or online account to be notified of transactions, or keep track of your account transaction history.
- Considering reducing your payment limits and only increase them it when you need to make a specific transaction above the limit amount.

Mistaken payments

If you make a mistake while making a payment, there are some protections under the ePayments Code. For example, if you make a typo putting in the BSB or account information and accidentally transfer money into the wrong bank account using internet banking.

The protections are not intended to cover scams where you did intend to transfer money to that account, but later realised it was a scam. They also do not cover BPAY.

Most banks, credit unions, and building societies (and other authorised deposit taking institutions) are subscribers to the ePayments Code. If the bank or financial institution is not a subscriber to the code, get legal advice if there has been a mistaken payment.

Banks generally do not check if the BSB and account number you have entered matches the name on the account. They must have a clear on-screen warning to tell you this, and that the money may go into the wrong account and may not be recovered. You must have a chance to cancel the transaction or fix the error.

To request a refund of a mistaken payment

Contact the bank as soon as you can. The bank must have a convenient process for reporting mistaken transactions. Often this will be a phone hotline (free or for the cost of a local call) that is open 24 hours, or has a way to leave messages after hours.

> The earlier you report the mistaken transaction, the more rights you have.

If the money is still in the other person's account, and both banks agree it was a mistaken payment:

1. If you reported it within 10 business days, the money must be returned to you, usually within 5 business days.
2. If you reported it between 10 business day and 7 months, the other bank must freeze the funds and give their customer 10 business days to prove the money belongs to them. If that person does not do that, the other bank must return the money to your bank within 2 business days.
3. If you report it after 7 months, the money will only be returned if the other person agrees.

If either bank doesn't agree it was a mistaken payment, get legal advice immediately.

If the money isn't in the account anymore, but the other bank agrees it was a mistaken payment, the other bank should make a reasonable effort to get the money back. For example, they may contact their customer to discuss a payment plan.

If only some of the money is still in the account, the other bank can choose whether to chase the full amount owing, return what money is there, or not return any money. But they must consider what is fair, such as:

- how much effort the bank has made to contact their customer to try and get the money back
- whether their customer is willing or able to come to a payment plan
- how long it has been since the transaction happened
- what they know about your situation.

You can also get private legal advice about court action against the person who received money in the mistaken transaction. But court action can be expensive.

If the bank refuses to reverse the transaction

Complain to the bank

You can complain directly to your bank. Contact details are on AFCA's website.

Explain why you are not liable for the transaction, or why it should have been a chargeback, or why it was a mistaken payment. Keep a copy of your letter.

Your bank should respond within 30 days.

Complain to the Australian Financial Complaints Authority (AFCA)

If the bank does not resolve your complaint, complain to AFCA as soon as possible. Time limits apply.

AFCA will look at whether your bank acted reasonably. It will consider the reasons you provided for requesting the refund and whether your complaint was made within the required time limits.

If a chargeback is rejected by the merchant's bank, the card scheme makes the final decision. AFCA cannot review the card scheme's decision, only the actions of your bank.

If your complaint is about a mistaken payment, your AFCA complaint is to be lodged against your own bank, regardless of which bank caused the problem. Both banks must cooperate in the AFCA process, and both banks are bound by AFCA's decision.

Need more help?

If the transaction relates to a scam read our Scams fact sheet for further information.

For a list of other resources, visit our Useful Links page.

Last updated: January 2025