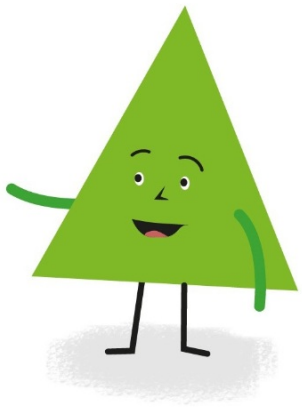
Assessing scam complaints



Scams are becoming more sophisticated, and anyone can be caught out. If you've been tricked into sending money or your bank account has been accessed without your permission, this guide explains what happens when you make a scam-related complaint to your bank, and how we assess those complaints.

What should you do first?

If you have been the victim of a scam, see these resources to find out **where to report** and **how to respond** to a scam.

Contact your bank as soon as possible. Your bank can then take steps to identify all scam payments and, if needed, secure your account to prevent further losses. If your bank accounts have been accessed, the bank may freeze your accounts until it is satisfied they are secure.

Your bank may need information from you, for example:

- the circumstances leading up to the scam
- what the scammer told you to do
- what information the scammer asked you to provide
- how payments were made, and whether they were made by you or the scammer
- whether you received two-factor authentication or verification messages
- information from the police, or your telecommunications or IT provider
- what alerted you to the scam.

You should cooperate with your bank's reasonable requests for information and respond promptly to the requests.

When should you contact us?

You can contact us about your scam complaint at any time. We expect that in most cases, a bank will communicate its decision on your scam complaint within 20 working days. If you are unhappy with how your bank investigated your complaint or the outcome, you can lodge a complaint with us.

We will assess whether the bank (or banks) met their obligations.

Authorised or unauthorised payments?

A bank's obligations differ depending on whether the payments were made with your knowledge and consent.

Unauthorised payments

If the payments were made without your knowledge and consent, under the **Code of Banking Practice** (the Code) the bank must reimburse you for the payments unless you:

- have acted dishonestly or negligently
- failed to take reasonable steps to protect your banking or
- did not cooperate and respond promptly to the bank's requests for information.

Authorised payments

Payments made with your knowledge and consent – even if you were deceived about the purpose of the payments or the identity of the person receiving the funds – are considered "authorised".

For payments made on or after 30 November 2025, banks have committed to certain scam protection measures. For such payments, we will check whether your bank:

- provided you with a warning
- provided a Confirmation of Payee service which allowed you to check the name of the person being paid matched the account name
- identified and responded to any high-risk transactions
- provided a 24/7 reporting channel for scams.

We can also consider whether the bank that received the scam payments acted in a timely way on any scam intelligence it received.

If we find that a bank has not met its Code commitments, you may be eligible for some compensation (up to $500,000).

To be eligible under the Code, you must:

- be a consumer (not a business or company)
- have made a domestic payment to a New Zealand bank account on or after 30 November 2025
- not have bought goods or services on a social media or other equivalent online marketplace
- have reported the scam to the Police and your bank within the required timeframes (within 3 months of

discovery and 12 months of the last payment)

- co-operate with your bank's reasonable requests for information and respond promptly.

You will not be eligible under the Code if you used a third-party payment service to make the payment or were dishonest or fraudulent. The amount of compensation may also depend on whether you took reasonable care when making the payments.

If you are not eligible under the Code, or the payment was made before 30 November 2025, we will assess whether the bank met its other obligations to you. For example, banks must act if they detect (or should have detected) the warning signs of a scam. If we conclude your payments raised warning signs that your bank should have detected but did not, we may find the bank is liable for some of your loss.

Call us

If you have been scammed and want to talk to us about what to do, contact our team on 0800 850 905, **help@bankomb.org.nz** or via our **online complaint form**.

See also our **quick guide** on types of scams and how to avoid them.