Amendment to the Code of Banking Practice to address fraud and scam payment protections and compensation (to apply from 30 November 2025)

What we will do for you

We'll respect your privacy and keep your information confidential. And we'll keep your information and the ways you bank with us secure.

We'll also let you know how to report a problem about the security of your banking, including our electronic banking systems.

If someone has accessed your banking without your authority or tricked you into making a payment, contact your bank immediately.

If someone has accessed and used your banking without your authority

An unauthorised payment is where you're a victim of fraud and someone has accessed and used your electronic banking or your card without your authority.

We'll compensate your loss from an unauthorised payment if you:

- weren't dishonest or negligent;
- took reasonable steps to protect your banking; and
- cooperate and respond quickly to reasonable requests for information about what happened.

If someone tricked you into making a payment under a scam

An authorised payment scam is where someone tricked you into making a payment under a scam.

To help protect customers from authorised payment scams, we and other members of the NZBA have made 5 specific scam protection commitments.

If we, or the NZBA member that received the payment you made (if that's not us), don't meet the applicable scam protection commitments, and you're eligible, we'll compensate all or some of your loss.

You're eligible for compensation of your loss from an authorised payment scam if you:

- were a consumer (as defined in the Consumer Guarantees Act) when using our banking services;
- made a domestic payment to a New Zealand bank account after 30 November 2025;
- weren't using a third-party payment service to make the payment;
- weren't buying goods or services on a social media or other equivalent online marketplace;
- weren't dishonest or fraudulent;

- reported the scam to the New Zealand Police and us within 3 months of discovery and 12 months of the last payment (if more than one); and
- cooperate and respond quickly to our reasonable information requests about what happened.

If you're eligible, whether we will compensate all or some of your loss will depend on whether you took reasonable care when deciding to make or making the payment.

We'll only compensate for authorised payment scam losses three times during our banking relationship and up to a maximum combined total of $500,000. Beyond this, each NZBA member will use its discretion.

Our scam protection commitments

1. *We will provide specific education warnings to consumers before certain payments are made*

We will ask you to confirm your payment purpose.

Based on the information you provide, we will, when appropriate, provide specific education warnings for known high-impact scam types to help consumers (as defined above) identify and avoid them, for example, investment scams.

2. *We will provide a Confirmation of Payee service*

We will offer a service to consumers for retail mobile and web banking channels to check the name of the person you're paying matches the account name.

We will provide clear information about how the service works and the risks of making a payment if you didn't receive a 'match', including where the service can't confirm the account name for any reason.

3. *We will identify high-risk transactions and respond appropriately*

We will have policies and processes to identify and respond to the risk of scams.

We will help protect you against high-risk transactions, and may use questions or real-time warnings, or delay or block transactions, among other things.

We will train frontline staff about common scams, how to keep banking safe, and to respond appropriately where there are clear warning signs you may be getting scammed.

Not all transactions will be 'high-risk'. They may include large payments, multiple payments to the same person over a short time, or certain payment types. But even these examples may depend on whether other factors are present or what your usual activity is.

4. *We will provide a 24/7 reporting channel for customers and will respond to reports of a scam within a reasonable timeframe*

We will provide clear information about what to do if you think you've been scammed, including how to stop electronic banking or block your cards, and will provide 24/7 options to report scams.

We will act quickly to protect your banking, and will investigate and seek to recover money in a reasonable timeframe.

5. *We will share information with other banks to help prevent criminal activity and to freeze funds where appropriate*

We will share data and information with other members of the NZBA to help prevent scams and recover money faster.

We will act on that scam intelligence in a timely manner, stopping payments and closing accounts identified as mule accounts where appropriate.

If another NZBA member received the payment you made, we will work with them to try to recover the money.

How we will handle compensation

You will only need to deal with us, as your bank, about any compensation for your loss.

When determining compensation, your loss is your direct financial loss from the unauthorised payment or authorised payment scam only. That's the money taken or transferred from your account minus any amounts we can recover for you.

Once we have the information we need to understand what happened (including your report to the New Zealand Police where relevant), we'll consider what happened. For authorised payment scams, that includes whether we or the NZBA member who received the payment you made (if that's not us) met the applicable scam protection commitments. We'll pay any compensation needed within 30 business days.

If you're unhappy with our compensation decision and we can't resolve your concerns, you can contact the Banking Ombudsman. For complaints about an authorised payment scam, the Banking Ombudsman can consider our actions, and whether the NZBA member that received the payment you made met the fifth scam protection commitment (set out above).

How you can help

We have included some examples of ways you can take reasonable steps to protect your banking, or ways you can take reasonable care when deciding to make or making a payment, below.

It's important to keep your banking safe and secure, and to take care when making payments.

Please follow any security steps in our terms and conditions or on our website and regularly check your accounts. And if your name or contact details change, remember to let us know.

Keep information about you and your accounts safe and your computer, mobile phone, and other devices secure, including setting an auto-lock.

Be suspicious – do not click on unknown links or download unknown software as it could be a scam. Banks never send you a link in a text message.

Please don’t let anyone else use or see your PIN or password while you’re doing your banking. Banks never ask you for your PIN or password. Don’t give other people fingerprint or facial recognition access to devices which can access your banking.

When making a payment, always pay attention to our warnings and messages. If we warn you of a risk someone is scamming you, take it seriously. And make further inquiries before paying if you don’t receive a 'match' in a Confirmation of Payee check, including where the service can’t confirm the account name for any reason.

Keep up to date on the information we send or publish about how to keep yourself and your banking safe. Do your research before making any large investments, checking the Financial Markets Authority’s website and contacting the organisation you’re investing with through their official website and phone numbers.