BOS Banking Ombudsman Scheme

Quick Guide

Anti-money laundering legislation – changes to banking

14 May 2014

The purpose of the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 is to ensure businesses take appropriate measures to guard against money laundering and terrorism financing. This enhances the reputation of individual businesses, and New Zealand as a safe place in which to do business.

The Act came into full effect on 30 June 2013, from which point banks have a legal obligation to be entirely compliant with its requirements.

It places obligations on New Zealand's financial institutions and businesses to detect and deter money laundering and terrorism financing. It also requires banks to gather more customer information to secure New Zealand against criminal use of our banking systems. This increase in information-gathering may cause customers some inconvenience, but is a legal requirement for banks, and non-compliance can result in prosecution.

What does the Act require banks to do?

Banks are now required by law to be more stringent when verifying customer identity, and need information from independent and reliable sources to do this.

The Act requires banks to collect more information about their customers to:

- ensure their understanding of a customer's business with them is accurate
- assist them in assessing the customer's risk profile
- help them identify transactions which may be suspicious.

If a bank reasonably believes a transaction is suspicious, it must report it to the New Zealand Police.

If a bank is unable to comply with the Act in its dealings with a customer, it must not do business with that person. This means that:

- it may not process certain transactions

- it can withdraw the banking products and services it offers
- if someone wants to join the bank, it can choose not to have that person as a customer.

What does the Act mean for me?

You may have to provide more evidence of your identity and personal details than before, for all types of accounts, including personal, business and trust accounts.

If you want to transfer money over a certain threshold overseas, your bank may ask you for more information than it previously required from you.

What information may I need to provide?

- your full name and date of birth
- your address
- your relationship to the customer (if you are not the customer)
- your company's identifier or registration number
- the source of your funds
- the names and dates of birth for beneficiaries of a trust
- the details of someone you are sending money to if you are making an international payment
- the nature and purpose of your business with the bank
- any other information prescribed by regulations.

What are some examples of what my bank might accept as verification of my information?

For verification of identity you may be asked to provide:

- your passport, or
- your birth certificate and 18+ card, or
- your driver's license and EFTPOS card.

For verification of address you may be asked to provide a:

- recent utility bill, bank statement or insurance policy, or
- recent letter from the Electoral Office, a government agency, your employer, or
- recent tenancy agreement.

Please note these are examples only. Your bank may require different information from that stated above. You may wish to ask your bank how recent the address verification needs to be.

Who should I talk to if I have concerns about how the Act affects me?

While the Banking Ombudsman Scheme can provide general information about how the Act affects your banking, each bank has its own individual Act compliance policies. If you have concerns about how the Act affects you, you should discuss this with your banking service provider in the first instance.

Can the Banking Ombudsman Scheme help me if I have a complaint with my bank relating to the Act?

Banks are legally required to have policies and practices compliant with the Act. The Banking Ombudsman Scheme does not have power to review legislation, nor can we compel banks to alter their practices or policies. However, we may be able to consider a complaint about a practice or policy which has breached an obligation or duty that the bank owes to the customer.

You can also complain to the Banking Ombudsman Scheme if you believe your bank has breached its statutory obligations.

Case note 1

Mrs O wanted to transfer funds from her overseas account to her New Zealand bank account. She asked her New Zealand bank for its SWIFT code, the bank's unique identification code needed for international transfers. The bank provided the code, and also told her what information she would need to make the payment. Two days later the Anti-Money Laundering and Countering the Financing of Terrorism Act ('the Act') came into effect, which introduced additional requirements for making transfers. Unfortunately the bank did not tell Mrs O about the pending change in requirements.

Mrs O transferred funds from an overseas account to her New Zealand bank. When the funds did not appear in her New Zealand account she contacted the bank.

After a short delay the bank advised the payment was delayed because it did not meet verification requirements for New Zealand banks under the new Act. It specifically noted she had not provided her physical address overseas. It advised Mrs O that the PO Box address she provided was insufficient, and that it was taking further steps to verify the transfer to ensure it complied with the Act. It offered Mrs O a temporary overdraft while it did so and the funds were released a week after she initiated the transfer.

Mrs O complained to the bank that it had been excessive in applying the Act and requiring her physical address given that she was already known to it. She also complained she had received poor service.

She felt the bank should have advised the legislation was about to change soon when she initially contacted it, and was unhappy with the delay in the bank's response to her queries after she had made the transfer. The bank responded to her concerns and offered her $500 to settle the complaint. However, she did not accept this and asked us to investigate.

The purpose of the Act is to detect and deter money laundering and the financing of terrorism. We considered that if a physical address was not provided it was reasonable for a bank to take further steps to verify the transfer, even if the customer was already known to the bank. We found while the bank may have taken a risk-averse approach, it had acted reasonably and in compliance with the Act.

However, partly due to the introduction of the Act, the bank had taken longer than usual to respond to her queries. We acknowledged this was inconvenient but concluded the bank's correspondence was ultimately constructive and not unreasonably delayed.

We did note when Mrs O first contacted the bank about making the transfer it could have warned her requirements were about to change. However, the bank's failure to do so did not reach the threshold for recommending compensation. Following discussions with the bank, it acknowledged the lapse in service and agreed to reinstate its offer to Mrs O of $500 in compensation. We considered that Mrs O should accept the bank's offer, which she did.

Case note 2

Mr H operated a funds remittance business, ABC Ltd. His bank decided to close ABC Ltd's bank account because it had concerns the account was being used in breach of the Anti-Money Laundering and Countering the Financing of Terrorism Act ("the Act"). The bank sent Mr H a letter explaining his accounts would be closed in 14 days due to its concerns. Mr H believed the bank could not close his accounts unless it could prove its claims. He complained to the bank which maintained its decision. Mr H brought his complaint to our office.

Our office is unable to consider a complaint about a bank's decision to close an account, but we can consider whether the correct process has been followed. We determined the bank had closed the account in accordance with the Code of Banking Practice, which requires a bank to give 14 days notice of closure. We were unable to consider the complaint further.

Case note 3

Mr C was the director of a foreign exchange and international remittance agency, XYZ Ltd. Mr C received a letter from his bank advising it would close XYZ Ltd's accounts in one month because XYZ Ltd no longer met the bank's risk profile, which had changed following the introduction of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.
Mr C complained to the bank about its decision. He said the accounts had always operated lawfully and closing them was unfair. He wanted the bank to keep the accounts open, but it only allowed XYZ a further two months to make alternate banking arrangements. Mr C was not satisfied and complained to our office.

We explained that under the Code of Banking Practice banks can decide to close a customer's account even if it is operated satisfactorily. A bank will usually give a customer at least 14 days notice of the closure. The bank's terms and conditions supported the bank's ability to withdraw the products or services it offers in accordance with the code.

We told Mr C that under our Terms of Reference we do not have the power to recommend a bank provides banking services to someone. We advised Mr C it was unlikely we would be able to assist him because the bank is allowed to close XYZ Ltd's accounts and we cannot make it change this decision. Mr C accepted our explanation and withdrew his complaint.