

# Telegraphic transfers

**28 October 2016**

Telegraphic transfers are a convenient and safe way you can pay money to people overseas. Before using this form of payment, it is important you know what is involved and potential costs.

## How does a telegraphic transfer work?

The normal way a telegraphic transfer works is as follows.

- The sender (“the remitter”) instructs their bank to send the funds to someone (“the beneficiary”). This can be done in-branch, but most banks now also allow telegraphic transfers through their internet banking.
- The remitting bank will then send the funds to a bank it deals with in the destination country (“the correspondent bank”). If the beneficiary has an account with that bank, the funds are credited to their account and the transaction is complete.
- If the beneficiary’s account is with another bank in the same country, the funds will be transferred again to that bank, at which point the transaction is complete. It is possible the funds will pass through two or more correspondent banks to get to the beneficiary’s bank.

## How long will it take for the money to arrive?

The time it takes a telegraphic transfer to reach its destination depends on where it is being sent. You can ask your bank how long a particular transfer should take. Under the Code of Banking Practice your bank must provide an indication of when a transfer would normally be available to the recipient.

If the banking system in the country of destination is inefficient, payment processing can take longer than expected.

## How to contact us

## How much does it cost?

Telegraphic transfers can have several fees. The remitting bank in New Zealand will generally charge around \$25, which will be charged even if you use internet banking. Most correspondent and beneficiary banks will also charge fees for their services, which they are entitled to do. Banks in New Zealand should warn remitters these additional fees may be charged. The remitter can choose to pay the fees charged by the remitting and correspondent banks, or have them deducted from the amount paid to the beneficiary. If no instructions are given, the charges are borne by the beneficiary. The beneficiary's bank may also charge additional fees the beneficiary will have to pay.

## What happens if something goes wrong?

When you send a telegraphic transfer you have to agree to a set of terms and conditions. You should refer to these for information about your responsibilities and the bank's.

If you have sent a telegraphic transfer and it is not received within the expected timeframe you can ask your bank to find out why. There may be some cost involved with this. The terms and conditions for telegraphic transfers will generally disclaim any responsibility for delays, but banks still need to exercise due care and skill when providing the service.

New Zealand banks have only limited responsibility for a transfer once it has left New Zealand, and are not responsible at all once the payment has left the correspondent bank.

The best thing to do if you think something has gone wrong with a telegraphic transfer is to contact your bank for help. If you are not satisfied with its response you can contact us about making a complaint, but you should be aware we can only investigate complaints about New Zealand banks and their agents.

We receive complaints about telegraphic transfers when the complainant is the victim of fraud. Our [Quick Guide on Common scams targeting bank customers](#) has more information.

Bank customers sending money overseas via telegraphic transfer may also be required to provide more information due to 2013 anti-money laundering legislation. See our [Quick Guide on Anti-money laundering legislation – changes to banking](#) for more information.

## Case note 1

Ms P lived in Australia and wanted to take advantage of the favourable exchange rate at the time and transfer funds from a New Zealand bank account to an Australian one. She phoned the bank to action the transfer and was told a transfer could only be done in-branch or through internet banking (either through a telegraphic transfer or by sending a secure message to the bank's email team which would action the request).

Ms P then tried to complete the transaction using internet banking, but was unsuccessful because the transfer amount exceeded the limit. After sending a secure message, the bank contacted her to confirm whether she wanted the funds sent in Australian or New Zealand dollars.

## How to contact us

Ms P said since her initial call the exchange rate had dropped, and asked what the exchange rate would be if the funds were sent in Australian dollars. She was told the bank would have to get a special exchange rate from its Treasury department because of the amount involved. The bank called Ms P back with its Treasury's indicative rate. Ms P confirmed that she would like to exchange the funds at that rate, and was warned the rate could be different when processed.

In fact the rate did drop further when the transfer was ultimately processed. Ms P felt disadvantaged because the bank had not completed the transfer during her first call and wanted to be reimbursed for the difference. The bank wouldn't do that but offered to reimburse the difference between its Treasury rate and the actual transfer rate.

When Ms P complained to us, we looked at the bank's telegraphic transfers policy which confirmed Ms P had received accurate information about the transfer requirements. This meant she would never have been able to complete the transfer during her initial call.

We could also not hold the bank responsible for the difference in the exchange rate between its Treasury quote and point of transfer. This was because the bank's terms and conditions

made it clear the exchange rate used in a telegraphic transfer was the rate at the time of processing, not the rate at the time the transfer was requested. The bank staff member had also informed Ms P it could change. After explaining this to Ms P, she decided to accept the bank's offer.

## Case note 2

Overseas visitors, Mr and Mrs F, placed over \$100,000 on term deposit for three years with a New Zealand bank. Soon afterwards, the bank received an emailed request from Mrs F's email address asking how to withdraw funds. The bank replied by email with a telegraphic transfer form for her to complete. Two forms were subsequently returned with Mrs F's signature, requesting the bulk of the term deposit funds be paid to two separate bank accounts (one here and the other overseas).

The bank carried out the instructions. It then received two further telegraphic transfer requests from Mrs F's email. Only one was processed as, combined, they exceeded the remaining balance.

Mr and Mrs F subsequently disputed the withdrawals on the basis they hadn't authorised them and complained to our office when the bank declined to compensate them. The bank did not accept it was at fault for acting on email instructions as they came from an email address Mr and Mrs F had provided when they opened their accounts. The bank noted two staff members had verified that the signature on the requests matched the signature held on file.

When we investigated we discovered the emails to the bank had most likely been sent using a programme that hides true IP addresses. We found Mrs F's email account (Gmail) had most likely been intercepted while she was using a US airport's Wi-Fi to send emails. With access to her Gmail account, the hacker found old emails containing the term deposit and bank contact details. It then became evident the hacker had also found a signed employment agreement attached to an email and copied the signature onto the telegraphic transfer forms. However, while the signature appeared authentic, it did not match either of the two signatures the bank held on file. We considered the bank ought to have noted this and not verified the signature as matching the mandate.

## How to contact us

When we consider a bank's actions, we must weigh them up against the applicable law, the Code of Banking Practice and what is reasonable in the circumstances. We must also consider prevailing industry practice.

Even if the signature had matched the mandate, we still had concerns about the transactions. We wanted to understand industry practice in relation to emailed requests, so we surveyed the practice of other New Zealand banks.

We found the particular bank's practice when accepting instructions by email was out of step with the rest of the industry. Some banks simply do not accept email instructions, acknowledging the risk of email addresses being hacked. Other banks accept emailed instructions, but only after taking additional steps to verify the requests were from their customer. For example, they call the customer back at a number held on file and ask a series of security questions.

We did not accept the complainants contributed to the fraud by accessing their Gmail via public Wi-Fi. This is common practice, and different to accessing online banking through public Wi-Fi. While we accepted there is a risk with email communication, our view is the fraud would have been prevented if the bank had taken additional steps to verify the instructions.

We recommended the bank reimburse Mr and Mrs F for the full amount of the funds that had been fraudulently withdrawn plus interest and place their total funds back on term deposit.

The case raises lessons for both customers and banks.

Customers need to be up-to-date with how criminal activity and techniques can affect them personally. They especially need to know the risks associated with storing documents on email accounts. In addition, it's a useful reminder that security questions (including those due to the new [anti-money laundering requirements](#) which were not in place when the events occurred) really do help to protect customers from fraud.

For the banking sector, it is crucial best practice prevails to maintain customers' confidence. We are satisfied this was an unusual case and we note the bank has taken further steps to enhance its processes, practices and raise team awareness regarding high risk transactions such as telegraphic transactions.

On the other hand, we are also aware of the constant challenge of keeping up with fraudsters, and have liaised with the New Zealand Bankers' Association and our participants about this case.

## How to contact us