



NEWSLETTER



May 2005

INTERNET BANKING

The Code of Banking Practice is due for review this year, and the New Zealand Bankers' Association will shortly be calling for public submissions to assist in the review.

At the last review, it was decided to change the review period from five-yearly to three-yearly, in part because of the speed of change in banking technology. The wisdom of this decision has been amply borne out by the growth of internet banking services and the consequent need to establish standards of good practice in the provision of those services.

One of the governing principles under the current Code is that banks will use their best endeavours to make sure that banking systems and technology are secure (clause 1.2(b)(iii)). This provision applies as much to internet banking as to any other aspect of banking services, and it applies to the processes used in conjunction with internet banking as well as to the actual banking service. In a previous newsletter, for example, I commented on the process used to identify a customer before acting on a request to set up internet access to an account.

The existing Code provision is a good basis on which to build, but particularly in view of public concern about the security of internet banking, the review is an opportunity to develop some more specific standards.

Similarly, there is nothing in the current Code to indicate which party should carry the risk of unauthorised internet transactions in the absence of negligence or any other fault on the part of either the bank or its customer. The two cases reported below are an indication of the problems that are beginning to arise.

While it is reasonable for customers to expect banks to provide protection against unauthorised access to internet banking facilities to much the same degree as they provide protection against unauthorised access to more traditional facilities, it is not always possible to apply the same rules or to reason by analogy.

In Case 1, for example, the customer chose an existing internet access password as a password for internet **banking** access. The current Code requires banks to warn customers about unsuitable PINs and passwords, and permits them to refuse reimbursement of unauthorised card transactions that were successful because the customer had chosen one of the prohibited class of PINs or passwords and it had become known to the offender. Passwords used for access to other services do not

fall into the prohibited classes, and in most circumstances it is not reasonable that they should. Limiting the number of different PINs and passwords that have to be memorised is a convenience to customers and lessens the risk that the customer will be unable to remember them without writing them down. However, it may be reasonable to prohibit (or at least to warn against) the use of other internet access passwords for internet banking purposes.

In this case the terms on which the bank supplied internet banking services were similar to those for card services – with the result that the bank was potentially liable for the unauthorised transactions.

Case 2 is an indication of the complexity of problems that can arise when there are several parties involved in the effects of fraudulent activity.

Liz Brown
Banking Ombudsman

Case 1

Mr L owned a business. His business associate, Mr D, shared business premises and office facilities including an internet connection with him. Both had full security access for the internet facility. Mr D supplied various business services to Mr L. Mr L gave Mr D the access code and password to his internet bank account, and authorised him to carry out bill payments on the account to pay both himself and other suppliers.

Mr L and Mr D had a disagreement. As a result Mr L wanted to prevent Mr D accessing his internet bank account, and visited his bank to ask for advice about changing his password. Mr L also said he told the bank officer about the disagreement with Mr D. The bank officer said that he was only told that Mr L had forgotten his password.

The bank officer changed the password again at the branch, and Mr L changed the password when he got home. He selected as his password for internet banking the same password as he used for access to the internet.

Several days later Mr D attempted to access Mr L's internet bank account, but was unsuccessful as the password was incorrect. Mr D contacted the internet service provider and, as he had full

security access for the internet facility, the internet service provider told him Mr L's internet password. Mr D then used the internet password to access Mr L's internet bank account. He made two transfers of funds from the account, one to himself and one to a tradesman.

On discovering the transfers, Mr L complained to the bank. At this stage Mr L did not know how Mr D had been able to effect the transfers and thought that Mr D had somehow hacked into the bank's systems or used key-logging technology to discover his access code and password. On finding out how Mr D obtained his password, Mr L complained that the bank should have given him better advice about protecting his account. He considered he should have been advised to change his customer access code as well as his password.

I found that the bank officer had given appropriate advice when Mr L had visited the branch to arrange to change the password. A change of password would normally be sufficient to prevent unwarranted access, and in this case Mr D was only able to use the account because Mr L had chosen a password that was accessible to him.

I then considered the question of liability for the unauthorised transactions under the terms and conditions of the account. The bank had through its terms and conditions agreed to reimburse customers for losses suffered as a result of unauthorised access to their internet bank accounts unless the customer had acted fraudulently, or had caused or contributed to the loss by, for example, failing to comply with the terms and conditions. The terms and conditions stated that a customer must not select as a password for their internet bank account, a password that is used for other services. I found that in choosing the same password for his internet bank account as he did for access to the internet, Mr L breached his contract with the bank.

Notwithstanding the breach of contract, the terms and conditions also provided that a customer's liability for loss arising from unauthorised access to an internet bank account was limited to \$50 unless the customer had carried out one or more actions from a list of prohibited acts. Selecting as a password for an internet bank account a password used for other services was not one of the prohibited acts.

As there was an inconsistency in the bank's terms and conditions, I interpreted them in the way most favourable to the customer. Mr L had not done one or more of the listed actions (or anything similar to one of the listed actions), and on the face of it he was entitled to the protection of the \$50 limit on liability.

I was not able to establish whether Mr L had suffered a loss as a direct result of the unauthorised transactions. There was a dispute between Mr L and Mr D about whether the funds were owed to Mr D and the tradesman and there were claims and counter-claims between the parties. This was a matter that needed to be resolved between the parties themselves or a court. It is not my function to resolve disputes other than those involving banks.

Accordingly I concluded that if Mr L and Mr D agreed, or if a court ordered, that Mr D should reimburse the transactions and Mr L was not able to obtain reimbursement, then Mr L could be entitled to payment by the bank, but that I could not recommend reimbursement until the dispute between Mr L and Mr D was resolved.

Case 2

Mr Z could only work part-time because he cared for his elderly and disabled mother. He applied for a job advertised by email. The job required him to accept payment by way of credit to his account for goods purchased from an overseas organisation and to forward the funds to the vendor, deducting a commission. He was told that the organisation needed representatives in New Zealand because most of its customers did not trust or could not use e-currency or money transfers. This seemed reasonable to Mr Z, so he applied for the job and was very pleased to have his application accepted.

Some days later a payment of several thousand dollars was made by direct credit to Mr Z's account from a Mr and Mrs K. He withdrew most of the funds, purchased

an international money order and sent it off to his "employer".

Shortly afterwards, Mr Z became worried about the transaction after reading about a scam. He telephoned the police and his bank, but neither was able to say whether there was any criminal activity. He then searched the telephone directory, found Mr and Mrs K's telephone number and contacted Mrs K. She knew nothing of the transaction and had not even realised that funds were missing from her account.

Mr Z tried to cancel the money order, but it was too late. Two days later the payment to his account was reversed by his bank, leaving him with an overdraft that he could not possibly repay. The bank told him that it would pass the debt to a

collection agency and his credit rating would be affected. It also cancelled his credit card.

Mr Z could not understand why he +was being held entirely responsible for the debt. He understood that Mr and Mrs K had been tricked into disclosing their internet banking password and this enabled the fraudsters to transfer the funds to his account. He felt they were at least partly responsible. He also questioned the security of both banks' systems.

When Mr Z complained to his bank, he was told that he was fortunate not to be charged with a criminal offence. However it did agree to allow him to make repayments by instalments, in which case it would not pass the debt to a collection agency and his credit rating would not be affected. Mr Z was willing to repay the debt if there was no alternative, but still

felt that he had been shabbily treated and contacted my office for advice.

After discussing matters with my investigator, Mr Z accepted that neither bank had had a lapse of security or had otherwise facilitated the fraud. There was a question as to whether Mr and Mrs K's bank was entitled to reverse the credit it had made to his account, but even if I had found it ought not to have done so and should recredit the funds, it was most likely that Mr and Mrs K would then make a claim on the money and Mr Z's bank would freeze his account, leaving Mr Z to try and reach agreement with Mr and Mrs K about ownership of the money.

By this time Mr Z was ready to put the matter to rest. He decided to accept his bank's offer to allow him to repay the debt by instalments and an affordable programme was worked out.

CREDIT CARD DEBT SECURED BY MORTGAGE?

Many customers are not aware that if a bank holds a standard "*all obligations*" mortgage to secure their home loan, it may use its powers under the mortgage to recover all debt owed to it, including credit card debt.

We recently received a complaint from a woman who was selling an investment property she owned jointly with other members of her family. She was in some financial difficulty after separation from her partner and needed to realise her share of the property. Her bank refused to discharge the mortgage over the property unless she repaid a debt due on a credit card that she had taken out jointly with her former partner, even though the partner had accepted responsibility for the debt and was making regular repayments.

The bank almost certainly had a legal right to require the card debt to be repaid, but few customers would think of their credit card debt as a secured debt, especially in view of the interest rates payable on credit cards. This complaint was quickly resolved after discussion with the bank's complaints handling staff but is a reminder that credit card debt cannot necessarily be isolated from other indebtedness.

FUNDING THE BANKING OMBUDSMAN SCHEME

From 1 July 2005 there will be some changes to the way banks are charged to pay for the Banking Ombudsman scheme and consequently to the way we classify complaints for statistical and funding purposes.

At present each bank is required to pay an annual levy which is calculated by reference to the number of dispute investigations involving that bank completed during the preceding year.

A dispute is a complaint which has not been resolved through the relevant bank's internal complaints process and has come to the Banking Ombudsman for investigation. No charge is made for complaints made to the Banking Ombudsman but referred to banks for consideration through their internal complaints process and resolved there even though the Banking Ombudsman or her staff may have assisted in that process.

Under the new system one third of the levy will be calculated on a basis that relates to the size of the bank. This recognises that the Banking Ombudsman does a good deal of work that is of benefit to banks but does not directly involve dispute investigation and resolution, such as educational, promotional and complaint prevention work and the referral service for complainants.

The remaining two thirds of the levy will continue to be charged in proportion to complaints resolved by the Banking Ombudsman, taking into account those complaints that are resolved without a full investigation but with some assistance by the Banking Ombudsman as well as complaints that are investigated.

We will continue to use the terms "complaint" and "dispute", but there will be a third category termed a "facilitation". These are cases where the Banking Ombudsman has done more than simply refer the complaint to the bank for consideration through its internal complaints process but has not conducted a full investigation.

It is to be hoped that the new system will encourage banks to seek the assistance of the Banking Ombudsman at an early stage in those cases where the intervention of a neutral third party may increase the chances of a speedy resolution to a complaint.