Proposed Amendments: Code of Banking Practice

InternetNZ suggests the following amendments:

Amendment 1

Clause 8 (b) (iii) second bullet point – amend to read:

Not recording your Password or other security information including keeping your Password on a file or on your computer or other device (including in any password saving facility ***which is not secure*****). A secure Password facility is one where the information in it is securely encrypted and which can only be accessed with a password or other security device that complies with the Password guidelines set out below. We will provide you with updated information on the appropriate levels of security for secure Password facilities***;**

Rationale: It is unrealistic to expect customers to remember all passwords and access codes that they are now faced with for banks and other secure subscription services. Secure password facilities (e.g. with 128 bit encryption installed) give sufficient protection.

Intuitively, it is obvious that disallowing the use of such facilities will simply lead to customers choosing less-strong passwords for banking services than they would be able to use in conjunction with a secure password facility. The use of such facilities should be promoted, not prohibited.

Amendment 2

Clause 8 (c) (ii) – amend to read:

If you advise us as promptly as is reasonably possible that your customer ID, Password or any other security information is or may be known to another person or there has been unauthorised access to your Internet Banking information or accounts, you will not be held responsible for any loss incurred ***~~after that time~~****, unless you have acted fraudulently or negligently or have contributed to such discloser or unauthorised access* ***by not following the guidelines set out in this Code.***

Rationale: The general principle is that a customer should only be held liable for any losses if they have done something or omitted to do something as specified in the Code (and in the Bank's terms and conditions) and act or omission has caused or contributed to the loss. This clause currently seems to imply that they **will** be liable for a loss before the notification, which is inconsistent with the general principle and with the practice for other forms of banking, particularly card-based transactions.

Amendment 3

Clause 8 (c) (iii) third bullet point – amend to read:

you have kept a written or electronic record of the PIN, Password or other means of access ***other than in a secure Password facility****;*

Rationale: See rationale above for Amendment 1.

Amendment 4

Clause 8 (c) (iii) fourth bullet point – amend to read:

you have used a computer or device that does not have appropriate protective software and operating system installed and up to date ***with any recent, major security upgrades or releases.***

Rationale: With computer and security patches being issued almost daily it is unreasonable to expect customers to be up to date with every release. It is appropriate that customers be required to implement major upgrades or run the risk of loss, but they should not be penalised for delaying or missing minor upgrades. We would expect this to cause the subsequent bullet point (which refers to specific types of software) to be read consistently with the amendment proposed.

As an aside it would be useful for the Banks to give some guidance to consumers as to what they expect or would use in interpreting this clause. Such guidance could be available on the NZBA website and on the banks' individual sites.

Amendment 5

Clause 8 (c) (v) – amend to read:

We reserve the right to request access to your computer or device in order to verify that you have taken all reasonable steps to protect your computer or device and safeguard your secure information in accordance with this Code. If you ***unreasonably*** *refuse our request for access* ***or cannot provide us with reasonable evidence that you have taken those reasonable steps*** *then we may refuse* ***to process*** *your claim.* ***If we are granted access to your computer we will, at our cost, observe proper forensic and legal evidential procedures and ensure that confidential and/or privileged material on your computer is protected.***

Rationale: A customer should be able to satisfy the bank that their computer and processes are compliant without the bank making an unreasonable search.

If a search is made, a proper forensic process should be used and confidentiality and privilege must not be affected.

Failure to grant access does not extinguish a claim altogether since that is a matter of law – but it is reasonable that the bank take no further steps **to process** the claim.