

# CODE *of* Banking Practice

**REVISED SECTION 8: INTERNET BANKING  
EFFECTIVE 1 JULY 2008**

## 8 internet banking

- (a) Our Systems
- (i) We will take appropriate measures to ensure that our Internet Banking systems and technology are secure and are regularly reviewed and updated for this purpose.
  - (ii) If you incur a direct loss that is due to a security breach of our Internet Banking system as a result of our failure to take reasonable care and is not caused or contributed to by you, we will reimburse you for that loss.
  - (iii) We will exercise reasonable care and skill in providing you with Internet Banking services. However, subject to our obligations under the Consumer Guarantees Act 1993 we will not be responsible if you incur a loss, which is caused through circumstances beyond our reasonable control. In particular, we cannot be responsible for a loss caused through circumstances beyond our reasonable control because of:-
    - your inability to access Internet Banking, or any other application associated or reliant on Internet Banking, at any time, or any failure or delay in providing a service via the Internet; or
    - a malfunction of any equipment (including telecommunications equipment) which supports our Internet Banking service.
  - (iv) Your computer or device is not part of our system therefore we cannot control, and are not responsible for, its security. However, we will inform you, primarily through our website, how to best safeguard your online information and the steps you should take to protect yourself and your own computer from fraud, scams or unauthorised banking transactions.
- In addition to non technical advice (such as not leaving your

computer/device unattended when you are logged on to Internet Banking or not using shared computers like those in Internet cafés to access Internet Banking), we will also have on our website available information and advice on the benefits of installing and maintaining protection, in respect of, for example:-

- anti-virus software;
  - firewalls;
  - anti-spyware; and
  - operating system security updates.
- (v) We will inform you of what procedures you must use to report unauthorised access to your information, accounts or disputed transactions using your Internet Banking service and make available to you contact information so you can report this activity as soon as you are aware of it.
- (vi) When we first give you access to our Internet Banking services we will tell you where to find the information you need to safeguard your online information and to protect yourself and your own computer from fraud, scams or unauthorised banking transactions. This information will be updated from time to time.
- (vii) We will never send you an email asking you to confirm your security information or asking you to disclose your Password or security information by email.
- (viii) We may also warn you against using an account aggregation system or software which is not provided by us that lets you see all your online accounts from different websites on the one website and requires you to input or disclose your customer ID, Password or any other security information.
- (ix) When you access Internet Banking services we will also inform

you of the applicable terms and conditions relating to the use of Internet Banking services.

- (x) We will advise you of the current transaction limits that apply to our Internet Banking services. These limits may change from time to time and are available upon request.
- (b) Your ID and Passwords and other Authentication/Security Information

We will provide you with regularly updated information on:-

- (i) How to access Internet Banking services, including details about your customer ID, selection of appropriate Passwords and the availability of additional authentication or security options.
- (ii) Maintaining the security of your customer ID, Passwords and any other security information (which, where applicable, includes any second factor authentication security device).
- (iii) Your responsibilities for protecting your Password and any other security information, including (but not limited to):-
- never disclosing your Password and any other security information to anyone else, including bank staff, police or family members;
  - not recording your Password or other security information including keeping your Password on a file or on your computer or other device (including any Password saving facility that is not acceptable to your bank);
  - not creating or using a Password and any other security information that can be:-
    - a) easily found out; or
    - b) relates to personal information about yourself (e.g. your birthday, family, street or pet names) or includes any obvious or sequential numbers such as 54321 or related numbers such as 22222;

- creating or using a Password and any other security information that is unique and/or is not the same as or similar to Passwords and any other security information used for other services you use;
- changing your Password and any other security information immediately if anyone else does or may know it;
- regularly changing your Password for increased security, and how to do this;
- taking reasonable care when accessing your Internet Banking service to ensure that your Password or other security information is not seen by or disclosed to anyone else;
- not opening attachments or running software from untrusted or unknown sources; and
- not responding to any requests for your Password or security information.

(c) Your Liability (Responsibility)

*As a guiding principle of this section, we will continue the practice of reimbursing all customers that are genuine victims of Internet Banking fraud.*

- (i) You will not be liable for losses caused by Unauthorised Transactions before you are able to access Internet Banking for the first time or during any period we prevent you from accessing Internet Banking, including, if applicable, before you receive your customer ID, Password or any other security information provided you have notified us of your current address. In any dispute about receipt of customer IDs, Passwords or security information that are not issued to you in person, we will not rely on proof of despatch to your correct address as proof that the customer ID, Password or other security information or additional authentication were received.

- (ii) 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 an unauthorised access to your Internet Banking information or accounts you will not be held responsible for any loss, unless you have acted fraudulently or negligently or have contributed to such disclosure or unauthorised access by not following the security information and advice in this Code and as provided by us on our websites and our terms and conditions.
- (iii) You may be liable if an Unauthorised Transaction occurs after you have received the means to access Internet Banking, if for example, (but not limited to) you have breached our terms and conditions by doing the following:-
- you have a PIN or Password of a type you have been warned not to choose;
  - you have voluntarily or negligently disclosed your PIN, Password or other security information to anyone else;
  - you have kept a written or electronic record of the PIN, Password or other means of access or failed to store same in a secure facility acceptable to your bank;
  - you have used a computer or device that you know or believe does not have protective software and operating system installed and reasonably up to date;
  - you have not taken reasonable steps to ensure that the protective systems installed on your computer or device such as virus scanning, firewall, anti-spyware, operating system and anti-spam software are continued to be updated within a reasonable period of time;
  - you have not taken reasonable care to safeguard any other device that is used to access your Internet Banking service;

- you have not advised us as promptly as is reasonably possible that you are aware that someone other than you has accessed your Internet Banking service or an Unauthorised Transaction has occurred;
- you have left your computer unattended when logged on to the Internet Banking service; and
- you have not followed our reasonable security warnings about the processes and safeguards to follow when using Internet Banking.

If any of these apply your maximum liability will be the lesser of:-

- the actual loss at the time of notification to us; or
- the balance that would have been available for withdrawal from your account(s), including any Credit Facility, between the time any unauthorised access was made and the time you notified us.

- (iv) If you have used or allowed your account to be used to process fraudulent or Unauthorised Transactions you may be liable for some or all of the loss suffered by the party who has been defrauded, regardless of the balance available in your account.