AUSTRALIAN BANKERS' ASSOCIATION INC.

<AHTCC>

ASIC
Australian Securities & Investments Commission

Protecting Yourself Online

Criminals may use your online account or credit card details to make fraudulent transactions or fully take over your identity. They can use this information to apply for credit, buy goods or open accounts in your name. Online fraud, like any form of identity fraud, can have serious financial consequences, including damage to your ability to get credit.

AVOID BEING CAUGHT BY FRAUDULENT E-MAILS

Phishing e-mails are those sent to your e-mail address by criminals who want to steal your personal information. These authentic-looking messages appear to come from banks, other financial institutions and legitimate businesses, but are designed to lure recipients into divulging personal data such as bank account numbers and passwords when you attempt to logon. Often, the phishing email will use tricks to get you to lower your guard, for example, by falsely claiming that you need to provide your personal data for security upgrades, false charges, late payments or phoney investigations.

Links within these fraudulent e-mails may also take you to fake or 'ghost' websites, which are designed to fool consumers. They may look like an authentic website, with logos and a homepage, but it is, in fact, another way criminals try to steal your personal information.

Tips:

- Never provide personal details including customer ID or passwords, in response to any e-mail. A bank will never ask you for your private password and this important information should never be shared with anyone.
- Never click on a link or attachment in an e-mail which purportedly sends you to a bank's website. Only access your bank's Internet banking logon page by typing the address into your browser.
- Be wary of any e-mail from someone you do not know or trust – delete without opening any e-mails that you think are suspicious.
- Be wary about clicking on links in any e-mail that you receive that is not from a person or organisation you know. Some e-mails sent by criminals ask the recipient to click on a link for more information. If you click on the link, you may be installing a file or be taken to a website that tries to download malicious software such as a keylogger that attempts to capture your user IDs and passwords.
- Always check your statements for any transactions that look suspicious. If you see any transactions that you did not undertake, immediately report this to your bank.

- Most phishing e-mails do not address you by your proper name because they are sent out to thousands of recipients. They sometimes contain typing errors and grammatical mistakes, even if they include the banks' registered logos.
- Install software that will filter spam e-mail or use an Internet Service Provider (ISP) that will filter spam prior to delivery at your Inbox. Spam filters are often included in anti-virus software.
- Avoid using Internet cafes, or other public computer terminals, to complete Internet banking. In some places, criminals have loaded software that records your keystrokes.

If you have responded to a phishing e-mail or if you have inadvertently entered your personal information on a 'ghost' website, it is always best to seek guidance from your bank. Do not delay in contacting your bank as staff can assist with advice on your next steps. Keep the bank's customer helpline handy at home. In addition, you should report the crime to your local police.

The bank will need to do an investigation if there is any suspicion that a fraud has been committed. If the investigation proves you are an innocent victim, have not contributed to the loss, and followed the banks terms and conditions, the bank will usually refund the loss.

Read more about how phishing scams work and how to protect yourself by checking the Australian Securities and Investments Commission (ASIC) consumer website, FIDO, at www.fido.gov.au.

TIPS FOR PROTECTING YOUR COMPUTER

It is important that you take positive steps to protect your computer if you are using e-mail, browsing websites and conducting e-commerce transactions. Criminals try to defraud customers by use of Trojans that monitor keystrokes, enabling the criminal to record confidential information such as online banking passwords and logon identification, as well as other material, which is stored on your personal computer.

It is important to use only a trusted and secure computer to access your Internet banking account. Using publicly shared computers, such as those at Internet cafes, is strongly discouraged. If you use your home computer to access your Internet banking account, we recommend that you:

- Install reputable anti-virus and firewall protection on your computer. This provides additional layers of protection that help to reduce your risk of exposure from viruses that can rob your computer of valuable personal information.
- Remember that after you install virus protection you will need to regularly update the software, usually by installing patches (used to update software against evolving threats, or fix a vulnerability in a computers operating system), so the protection remains current.
- Install any security patches for your operating system and other software installed on your computer and keep these up-to-date.
- Read your bank's Internet banking security guide which can be found on the bank's website.
- Before disposing of your computer, it's a good idea to remove all traces of your personal data, such as temporary Internet files, your Internet history, cookies, passwords and

recently opened documents list. Special *wiping* software can be downloaded or purchased to help you wipe clean your entire hard drive, ensuring all files are unrecoverable.

- Before purchasing online, ensure that you are dealing with a secure website. This can be done in several ways:
  - First if you look at the top of your screen where the web address is displayed, you should see https://. The "s" that is displayed after the "http" indicates that the website is secure. Often you do not see the "s" until you actually move to the order page on the website.
  - Check a Secure Socket Layer (SSL) protects your data. An easy way to tell if you are using a genuine SSL site is to check for a padlock symbol on your computer screen.
  - Another symbol that can indicate that you are on a secure site is an unbroken key.

USING INTERNET BANKING

When banking on the Internet follow these steps:

- Always access your bank's website by typing the address into the browser.
- Keep your computer up-to-date with anti-virus, firewall software and the latest patches.
- Avoid using passwords or PINs (Personal Identification Numbers) that are relevant to your personal situation. Passwords with telephone numbers, postcodes, your name, or the name of a close relative and dates of birth are simple for criminals to trace. Create passwords with letters and numbers that cannot be easily attributable to you.
- Always memorise your password or PIN and do not write it down or store it on your computer. You are responsible for keeping this information confidential.
- Change your password regularly and don't use the same password for other services such as your video store.
- Confirm that your data is encrypted between your computer and the bank by looking for the padlock symbol on the bottom right hand corner of the browser window.
- Always log out from the Internet banking menu when you finish all your banking.
- Close your Internet browser after logging out at the end of each Internet banking session.
- Beware of any windows that 'pop up' during an Internet banking session and be very suspicious if it directs you to another website which then requests your customer identification or password.

The Electronic Funds Transfer Code (EFT Code) protects consumers who use electronic banking at ATMs, EFTPOS terminals, via telephone or the Internet. The Australian Securities and Investments Commission's (ASIC) consumer website, FIDO, at www.fido.gov.au, has ten tips for safer electronic banking and protecting yourself under the EFT Code.

What is anti-virus software?

Anti-virus software is used to detect and eliminate computer viruses and other malicious software such as worms and Trojans. Any computer connected to the Internet faces the risk of virus infection, so it makes sense to secure your computer adequately with antivirus software.

Keeping your software updated

New viruses appear every day, so in order for your antivirus software to be effective, these definitions need to be updated regularly. Most antivirus software comes with 12 months of free updates, but you'll usually have to purchase additional annual subscriptions after that. You will also need to keep your operating system up to date e.g. Microsoft Windows, Unix or Macintosh, this can usually be done via their official website.

No software can guarantee 100 percent protection — viruses are constantly evolving and can spread between PC's rapidly. Antivirus software is only effective if it's up-to-date, so it's vital that you subscribe to regular updates and ensure that it is continuously updated. Some anti virus and other software providers do supply updates online, these are called security patches.

Choosing anti-virus software that's right for you

The software you choose will depend on your operating system. Before you select a product, make sure you choose the version suitable for your platform, for example, if you use Windows XP, look for a package that is recommended for Windows XP.

December 2006

Web: www.protectfinancialid.org.au Phone: 02 8298 0417 Fax: 02 8298 0402