AUSTRALIAN BANKERS' ASSOCIATION INC.

<AHTCC>

ASIC
Australian Securities & Investments Commission

Protecting Your Business Information

WAYS TO PROTECT YOUR BUSINESS INFORMATION

Some simple steps you can take to minimise your risk of becoming a victim of identity theft include:

- Keep all sensitive business information, such as tax records and other financial information, in a secure place. Shred all unwanted sensitive documentation (both your own and that of your customers) and ensure secure disposal.
- Install and update anti-virus protection software on your computer system.
- Password-protect files that contain sensitive personal data, such as customer records or financial account information. Create passwords that combine 6-8 numbers and letters, upper and lower case. In addition, encrypt sensitive files and only provide passwords to relevant staff.
- Delete without opening any suspicious e-mails.
- Download software only from reputable sources.
- Before disposing of individual PC's, remove data from the hard drive by using a strong "wipe" utility program. Do not rely on the "delete" function or emptying a recycle bin or trash folder to remove files containing sensitive information. These methods do not remove the data; they simply remove the pointers to the file. The data remains on the hard disk. A disk wiping utility program will greatly improve the chances that your data cannot be recovered. Some programs erase the entire disk, while others allow you to select which files or folders to erase. It is important that the utility or program provide an option to erase free space (temporary files) as well.
- Keep a back up of your critical data offsite and regularly test that you can recover the data.
- Train your staff to deal appropriately with your customers' personal information and never divulge this information inappropriately to external parties.
- Ensure staff have access only to information relevant to their role.
- Ensure that when cheques are received that the company name on the cheque has not been changed in a simple way. For example, Company ABC appears as Company ABCD.

HOW DOES A BUSINESS KNOW IF IT HAS BEEN HACKED?

The following is a useful list of potential indicators that your small business has been hacked and can be used to monitor your exposure:

- Your website has been changed to whatever the hacker wants.
- You may notice that your computer system performance is exceptionally slow.
- Some secrets of your business have been exposed to the general public or to competitors.
- Transactions have been changed, for example, an account had a balance of $1000, now it's $950 without your authorisation.
- There is odd activity in a log and the more it's investigated the more the business becomes convinced that something is wrong. The business processes are not being followed and it may be that someone is operating outside of your control and is using your business.
- You are no longer receiving e-mails and no one receives e-mails you have sent.
- The entire system shuts down.
- There is a new program on your computer you didn't install.

To enable a business to assess its risk to hacking, you may want to engage the services of an external independent Internet security organisation, specialising in 'ethical hacking'. These organisations can help assess and mitigate the risks for Internet security, independent of any vendor or supplier. By doing this you take a positive step to understand your risks and install programs to test for their effectiveness.

DOES IDENTITY TAKEOVER HAPPEN TO BUSINESSES?

Identity takeover is not only limited to individuals, it could also happen to a business – even your business.

In Australia there have been some extremely large losses where new business names have been registered in similar names to existing companies. Cheques intended for the existing company have been intercepted prior to receipt and deposited into accounts conducted in the name of the fraudulent business.

(Fact Sheet continues on next page)….

How do banks protect my personal information?

Banks use a combination of safeguards to protect your information such as employee training, privacy policies, and rigorous security and encryption systems. They have systems in place to constantly monitor online transactions and if a transaction is identified as suspicious, it will be investigated to ensure there is no breach of security. Occasionally, this may involve a bank staff member contacting you to verify a transaction. In such cases bank Staff will not ask for your passwords or PINs.

Bank customers are protected from loss in genuine fraud cases. Account holders are not liable for losses resulting from unauthorised transactions where it is clear that user has not contributed to the loss. There is usually an investigation by the bank to determine how the fraud has occurred.

Banks are continuing to seek out security enhancements especially for online banking such as an on-screen keypad which is designed to prevent the incidence of keystroke logging fraud by removing the need for a keyboard to enter in passwords.

Others banks are offering what's called two-factor authentication. An example of one factor authentication is the use of a password to enable access to Internet banking.

Two-factor authentication requires two independent authentication steps for a customer to access Internet banking. Customers will authenticate their identity and access to the system twice, first with something they know and then with something they have.

There are several ways that two factor authentication can be offered to the customer. It can be completed through a SMS payment security service, which sends a unique code via SMS to a customer's mobile phone to authorise online payments. Customers have already logged on to Internet banking using a password and then need to enter the SMS code before they can finalise the online payment.

Two factor authentication can be completed through a device known as a security token which looks like a pager. It is a device issued as a credential. A token is likely to include security features which render it difficult to forge, and tying it in some manner with the particular entity – in this case the bank which issues it. To log on to Internet banking the customer uses their password and then the number generated by the token, which is then keyed in at the desktop to enable access to an Internet banking session.

Fighting cyber crime

The Australian Bankers' Association (ABA), its member banks, State and Federal police are working closely to tackle the problem of cyber crime. Bank staff have been seconded to the Australian High Tech Crime Centre (AHTCC) as part of a new team to continue the fight against fraud that occurs online. They are providing analytical assistance to police who will use this information to identify and prosecute criminals.

Banks work closely with State, Territory and Federal police to prosecute criminals who misuse customers' personal information or commit cyber crime. Each State and Territory jurisdiction has a range of offences, which cover identity crime, including the unlawful possession of documents, operating accounts in false names and obtaining monies by deception. The penalties vary across each State and Territory but include large fines and incarceration, in some circumstances for up to ten years. Banks also work closely with other organisations such as the Australian Crime Commission and the anti-money laundering regulator, AUSTRAC.

Staying informed

Banks publish information about scams on their websites. The Australian Securities and Investment Commission's (ASIC) consumer website, FIDO, at www.fido.gov.au, has lots more information about how to identify and avoid different scams and swindles.

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