

Macquarie Bank Lecture Series

The "Plain English" Dos and Don'ts - Individuals

(prepared in conjunction with the Fraud Squad of New South Wales Police)



For individuals...

- DON'T carry your identification documents such as your birth certificate or passport unless you need them
- DO keep your tax records and other financial documents in a secure place

Destroy or delete your tax file number (TFN) from any documents before throwing them away and never give your TFN to anyone unless they have a good reason for needing it.

- DON'T leave documents such as registration papers, expired drivers' licences, invoices, utility bills or traffic infringement notices in the glove box of your car
- DON'T dispose of receipts and other personal information casually

Identity thieves go through bins for your personal information. Always ensure that documents disclosing your credit card number and other personal information are shredded or torn up.

- DO install appropriate security measures on your computer

Be mindful when accessing your account information using a public or shared computer.

- DO ask for more identification if you are suspicious of a person that you are selling to by private sale

Consider accompanying the purchaser to the bank branch to ensure that the funds are correctly deposited to your account.

- DO cancel all unused accounts and reduce the number of credit cards you actively use to a bare minimum
- DON'T use the same password on your bank account that you use for borrowing videos at your video store, for connecting to your internet service provider or accessing your mobile telephone service
- DO use a locked mailbox to send and receive all mail

Don't post items containing your personal information in your local on-street post office box. Instead, take your mail to the local post office. It is easier for identity thieves to raid the local on-street post office box than the box at the post office.

- DO have a mailbox that is capable of accepting and holding mail in the quantity and size that you normally receive it

If you receive a lot of mail then you should have a deep mailbox. Similarly, if you regularly receive A4 sized envelopes or magazines then you should have a mailbox with a wider slot.

- DO collect your card in person from the issuer in order to prevent identity thieves from intercepting your credit card

If this isn't possible, be aware of your account cycles and the expiry dates and contact your financial institution if mailed new or re-issued cards are late. You should also contact your post office to confirm that your mail has not been redirected to another address.

- DO be careful of the personal information you convey in public

Identity thieves can obtain a lot of information about you by listening to your conversations and telephone calls.

- DON'T provide your personal or account information over the telephone unless you are certain of the source and you initiated the phone call

Identity thieves sometimes trick you into providing your credit card number by claiming that you have won a competition.

- DO request your details to be deleted from marketing lists

Be mindful of bogus offers and websites requesting you to provide or validate your personal or financial information.

- DON'T sign up to internet "wallet" services

Wallet services store your credit card, shipping and billing information so that you do not have to re-enter it each time you purchase on the internet. Think of how appealing such a database is to computer hackers!

- DO carefully check each bank account statement to ensure that it does not include any transactions that have not been initiated by you
- DO check your credit reports once a year

This alerts you to all credit applications made in your name including those you may not be aware of. You can also sign up to an ongoing credit reporting agency.

- DO question the information gathering and handling practices of the institutions that you deal with

Larger businesses owe obligations to you under national privacy legislation. These include protecting your personal information, collecting only what is necessary and not using the information for purposes other than for the purposes initially disclosed to you. Request to see the privacy policy of the businesses you deal with.

- DO photocopy and keep records of your account and identification documents

Keep these records in a safe place, together with a list of the customer service contact numbers for each institution that you deal with. If you become a victim of identity fraud you can contact the financial institutions swiftly with complete information.

- DO immediately report to the police and your financial institutions any instances of misuse of your personal information

Macquarie Bank Lecture Series

The "Plain English" Dos and Don'ts - Business

(prepared in conjunction with the Fraud Squad of New South Wales Police)



If you run a business and want to protect your business and its customers from identity fraud...

- DO keep all sensitive business information, such as tax records and other financial information, in a secure place
- DO install appropriate security measures on your computer system

Use password-protected facilities to store sensitive information about your business, your customers and your employees. Similarly, ensure that paper information is stored in locked security cabinets. Restrict access.

- DO use a locked mail box to send and receive all mail
- DO have a mailbox that is capable of accepting and holding mail in the quantity and size that you normally receive it

If you receive a lot of mail then you should have a deep mailbox. Similarly, if you regularly receive A4 sized envelopes or magazines then you should have a mailbox with a wider slot.

- DO have your accounts department monitor and validate each account statement
- DO check the credit reports of your business at least once a year

This alerts you to all credit applications made in your business name including those you may not be aware of. You can also sign up to an ongoing credit reporting agency.

- DO request complete details and take extra precautions when receiving orders from your customers

Mobile telephone numbers or post office box addresses may indicate that your customer does not want to be traced.

- DO ask for more identification from your customers if you are suspicious of an identity fraud

Don't be rushed or intimidated by suspected fraudsters, take your time to follow proper security procedures. Request to see a driver's licence or other identification document to confirm the identity of your customer.

- DO put up a sign in your business informing your customers that purchases over a certain dollar amount will require photo identification
- DON'T accept identification on face value

Check the identification documents carefully and question the legitimacy of the person presenting the identification documents. Don't accept faxed proof of identity.

- DO request the credit card security number (this is usually a four digit number printed above the card number or on the signature strip) if you provide telephone or internet ordering

This ensures that the card is present at the time the order is made.

- DO know your merchant agreement with your Bank or institution

You should follow the conditions in the merchant agreement relating to the fraudulent purchase of goods or services. It may require you to conduct your business a certain way or to put in place certain verification procedures.

- DO provide facilities to enable the secure disposal of sensitive information

Use shredding bins to dispose of or destroy your customers' credit card slips, unwanted applications or documents, prescription forms, or other sensitive data.

- DO train your staff to deal appropriately with your customers' personal information

Put procedures in writing and monitor all staff, both temporary and permanent. Don't allow opportunities for the misuse of information.

- DON'T divulge customer information to anyone

You may breach privacy legislation if you divulge customer details to anyone other than for legitimate transactional reasons. There is no reason your Bank, the customer's Bank, or any other agency should approach you for customer details unless it is for a law enforcement purpose.

- DO appoint external auditors

Independent review of your business' accounts may reveal incidents of internal fraud that should be investigated immediately.

- DO consider pre-employment screening of your staff
- DO report all suspected frauds to the police and your merchant processor immediately