

How to Protect Your Organisation, Customers and Yourself from Identity Fraud

This addition to our Fraud Awareness Tips and Tools library is designed to provide some easy to follow guidelines on how to safeguard against Identity fraud and identity theft. The document has been designed with a three-fold focus:

- To assist your organisation with self help tips on how to recognise common identity fraud indicators
- To assist your institution to educate and protect customers against the risk of Identity theft and associated identity fraud
- To assist to safeguard yourself with easy to follow tips and guidelines

Common Identity Fraud Indicators (or Fraud “Red Flags”)

Identity Fraud can take many forms, it can be perpetrated in a number of ways including

- Take-over of a valid identity of a customer using valid channels such as Internet banking, IVR (Telephone banking), bill payments, account opening, lending applications via remote sources and changing customer contact details. Theft of a valid identity and attempt to open an account with your institution using the stolen and sometimes altered documentation
- Production of counterfeit or fabricated documents to create an entirely new identity coupled with approaches to open accounts and create borrowings etc

Common Red Flags and indicators include:

- Documents that don't appear to be consistent with the persons age, appearance or other details such as borrowing history. For instance a middle aged person who has never borrowed before, alternately a newly created listing of credit checks appearing on an existing credit profile (for same or similar amounts of credit but with many lenders)
- Requests to change address without substantially verifying proof of identity
- New borrowings on substantially paid mortgages including internet transfers and requests for unsecured borrowings using existing assets
- Broker introduced lending and account applications where original documents have not been sighted by the individual institution
- Requests for issue of electronic card or internet access where the historical transactional profile of the customer is not through these means
- Repeat requests for issue of access cards and change of address that may have not been subjected to thorough validation checks

Education Tips for Customers to prevent identity theft and fraud

Educating customers to be alert to the risks of identity fraud is integral to safeguarding your own financial institution against risk. Customers should be not only be educated to remain alert to the risk of identity fraud theft and take-overs but should be encouraged to report any suspicious activity on their accounts as soon as possible. An example of this would be reminding them to reconcile statements regularly especially for cheque and home loan accounts and checking balances online.

Educating customers to keep ALL personal information confidential and not to disclose in such channels as email prompts (Phishing¹) and to phone callers, even if the person claims to be from the financial institution. The following tips are designed to be used in general customer education documentation such as statement mailers and regular newsletters.

Customer tips for safeguarding against identity theft and fraud

- Never carry your identification documents such as your birth certificate or passport in a wallet, case or handbag unless you need them
- Ensure you retain personal tax records and other financial documents such as statements and receipts in a secure place
- Destroy or delete your tax file number (TFN) from any documents before throwing them away never quote or give out your TFN unless there is a good reason- completing a government tax form or opening an account
- Never leave documents such as registration papers, expired drivers' licences, utility bills or spare house keys in the glove box of your car (even locked) as these are all items a would be thief can use to steal your identity
- Receipts and other personal information should never be disposed of unless shredded or destroyed
- Identity thieves will search through bins for your personal information. Always ensure that documents disclosing your credit card number are destroyed
- Install appropriate anti-virus and anti-spy ware controls on your home computer and in addition run live updates to ensure use of latest version
- Public computers or sharing a friend's can be dangerous as PINs and passwords can be captured by criminals and be used to steal funds
- Try to select passwords you can remember but that will be hard for a thief to guess if your details are stolen, having separate passwords spreads the risk whereas one password for all means all may be compromised
- Always have a locked mailbox to send and receive mail or use a post office box.
- Ensure your mailbox is big enough to take large articles so that they can't fall out or easily be taken
- Be alert to when your account statements should arrive and card expiry dates and always advise your financial institution immediately if an expected new or reissue credit or debit card or PIN mailer has not arrived
- If you suspect mail theft, contact the post office to confirm that your mail has not been redirected to another address
- Never reveal personal or account information over the telephone unless you are absolutely certain the person is genuine 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 or a holiday- don't let this fool you
- Photocopy and keep details of accounts and proof of identity and keep them in a safe place.
- If you suspect you may be a victim of identity fraud, contact all financial institutions you do business with immediately. Keep records of persons you have spoken to, lodge a report with police and advise your credit reporting agency as soon as possible
- Check all your statements and account details regularly following any suspected incident and immediately report to the police and your financial institutions any instances of misuse of your personal information

Protecting your organization from identity theft and fraud

Safeguarding your Business Against Identity Theft and Fraud

- Staff training in detection and prevention of identity fraud is crucial both to assist them to recognise potential signs and understand what to do. Coverage of situational learning scenarios on Identity Fraud is one major component of the external Computer based fraud training available from Industry Association (see below)
- Practice a clean desk policy, ensuring that all customer records and similar are locked away each evening
- Ensure that all information on laptops, disk drives and portable storage devices is either encrypted or password protected
- Use a locked bag or post office mailbox, identity thieves can steal and alter incoming cheques from customers
- Account department validation of all accounts including any online services should be performed daily and regular audits performed on access controls
- Ensure you have facilities for secure destruction of sensitive information and never throw customer details or intercepted cards into the rubbish
- Never divulge customer information to anyone and ensure staff are well trained in privacy legislation and requirements
- Law enforcement and government agencies may approach you to request records of customer accounts are produced. Always ensure you check on the legitimacy of the document and if necessary call the issuing department
- Tasking your external and internal auditors to regularly review items such as accounts, debtors and customer details can assist to reveal incidents of internal fraud. Ensure early action on any triggers or red flags especially with items such as dormant accounts, statement cycle manipulations or similar
- Always practice robust pre-employment screening of your staff – permanent, temporary and contractors
- Practice a zero tolerance to fraud by reporting all suspected frauds to the police

Need Help with Fraud Training?

Industry Association's Computer Based Training Module titled Effective Fraud Prevention- External Fraud has a detailed section on identity fraud covering all aspects, situational case studies and quizzes. The module also covers lending fraud, handling evidence, cheque fraud and card fraud. Full Details on how to purchase the Fraud Training Module are able at [CBT Fraud Prevention](#).