Identity Theft Checklist

Concerned that you might have had your identity stolen? Here are some of the warning signs:

- *Missing or stolen wallet or purse* – Even if it has been returned to you and seems to be intact, there is still a possibility your personal details may have been compromised
- *Unfamiliar charges or withdrawals* – Regularly check your bank and credit card statements and contact your Bank if you detect charges and withdrawals you do not recall making
- *Unfamiliar bills* – If you receive bills for goods or services that you did not order/purchase, this could indicate that somebody has used your information fraudulently
- *Missing mail* – If you suspect mail may have been stolen from your letter box or redirected to a new address without your authorisation, check with your post office
- *Calls from creditors* – If you are being contacted by creditors for an application, transaction or enquiry you did not make, you need to take immediate action to find out who has been dealing with them. Make it clear to the creditor that you have not engaged in those transactions
- *New credit cards* – If you receive new credit cards that you did not apply for, contact the issuer immediately to have them cancelled
- *Denial of credit* – If you are unexpectedly denied credit, you should investigate this immediately by accessing your credit report.

What to do if your identity has been stolen

There are certain steps you can take to minimise financial loss and damage. However, it is important to remember that even if you do follow all these steps, it may not prevent unauthorised or fraudulent use of your documents.

1 *Immediately inform the police*

- ❑ All incidents of identity theft should be reported to your local police, even if only small sums of money are involved
- ❑ Request a copy of the police report/number as most banks or other financial institutions will ask you for this.

2 *Speak to St.George or your Bank*

- ❑ Report your personal details as potentially compromised
- ❑ Cancel your impacted credit/debit cards and order new cards as required
- ❑ Review and report any suspicious or unusual transactions immediately
- ❑ Request Security Keywords to be added to your account, along with any additional security measures your Bank may offer
- ❑ Change the password on your Internet Banking and enable Two Factor Authentication (2FA)
- ❑ Review and update any alternate sign-in options you may use
- ❑ Use your Digital Card (a digital version of the physical card), accessible in the St.George app, while you wait for the physical card to arrive
- ❑ The Digital Card is also a safer way to shop online or over the phone – The Dynamic CVC changes every 24 hours, so if your card details are ever compromised, the details will be invalid once the CVC changes.
- ❑ Change the PIN on your cards once your physical card/s arrive – you can do this in the St.george app (search 'change card PIN')
- ❑ Perform the Security Wellbeing Check in the St.George App
- ❑ Report any suspicious emails or SMS you may have received to your Bank.

Identity Theft Checklist

Enhance your personal security

- ❑ Contact IDCARE - Australia and New Zealand's national identity & cyber support service. IDCARE provides free, confidential support and guidance to people who have been targeted by fraud, scams, identity theft or compromise. Visit idcare.org or call 1800 595 160
- ❑ Change your passwords on all other online accounts straight away, including social media, apps, emails etc. and keep your passwords unique
- ❑ If you think someone may have accessed your online accounts, report it to the relevant company
- ❑ Alert your family and friends if someone has taken over your social media accounts, your email account or is impersonating you in any way. Tell them to report the account and block any further contact.

If Government ID documents have been compromised

- ❑ Contact the relevant authority who has issued your driver licence to report this as lost/stolen/potentially compromised
- ❑ Contact Medicare via medicare.gov.au to report your details or cards as lost/stolen/compromised
- ❑ Refer to the Office of the Australian Information Commissioner (OAIC) for further data breach information oaic.gov.au

Get a copy of your credit report

- ❑ Inform the credit reporting agencies that your personal information has been compromised
- ❑ You can request a copy of your credit report from these credit reporting bodies:
  - Equifax, phone 138 332
  - Experian, phone 1300 783 684
  - illion, phone 1300 734 806
- ❑ Ask for an alert to be placed on your file (this should help prevent additional fraudulent accounts being opened in your name)
- ❑ Carefully review and ensure you authenticate all 'enquiries' made to your credit history. Contact all organisations that have made enquiries under your name that you did not authorise.

Close all unauthorised accounts

- ❑ Contact any credit providers and businesses with whom any unauthorised accounts have been opened in your name. Inform them you have been a victim of identity them and ask for any the fraudulent accounts to be closed.
- ❑ This can include:
  - Phone and internet providers
  - Utility Providers e.g. Gas, electricity, water companies etc.
  - Department stores
  - Banks and Financial institutions
  - Social Media accounts
  - Online and Mobile Apps e.g. messaging apps, dating sites etc.

Keep a copy of your conversations

- ❑ Take notes that include dates, names, contact details and what was discussed during your contact with those agencies
- ❑ Follow up all conversations and requests in writing and send these by certified mail if you need to post them
- ❑ Keep copies of all forms and correspondence.

For more helpful information, visit:
stgeorge.com.au/security