What to do when identity theft strikes

Intended purpose:

Use this checklist if you suspect or have discovered that you have been the victim of identity theft. The first part of the checklist deals with flags or indicators of identity theft to investigate, the second part is all about what you should do in response.

Part one: Flags & indicators of identity theft

- [ ] **Charges to your account/s** which you don't recognise, be very wary as bad actors will sometimes try a few cents to see if the charges will go through before processing bigger ones.

- [ ] **Emails in your inbox** that you don't recognise (these aren't typically spam but usually from reputable companies but ones which you're not doing business with). This may also be in the form of **physical mail** correspondence.

- [ ] Following the above you may also receive **calls regarding products or services** which you don't use or buy.

- [ ] **Bills which are due to arrive by physical mail are missing** or you're receiving bills for products or services you don't use.

- [ ] You receive a **call or letter from a credit reporting agency or debt collector** regarding an unpaid account which you're not familiar with. A credit reporting agency may also notify you when a **credit score check is done** on your file, if you haven't applied for anything new that may require this check, it would be worth querying it.

- [ ] You receive an email that **your information was exposed in a data breach**.

- [ ] Some websites **keep track of your login history** – check this periodically and see if there are any unknown locations listed. If you use a VPN look for date and time of login instead, if there are odd entries which you recall not logging in it's a sign someone else has access to that account

- [ ] **Tampered bins** or 'dumpster diving' can indicate someone has been going through your rubbish looking for bills or other documents with valuable or identity information

- [ ] Some big flags also include a **warrant of your arrest**, a **tax return lodged** in your name, **denial of insurance claims or credit applications**, or the **inability to access online accounts**

- [ ] **Gut feeling or instinct** is the last flag though quite ambiguous we know. It's easy for us to assume a strange or unrelated letter or email was sent in error thanks to the modern automation of mass mailing. Trust your gut and investigate and confirm that something has come to you in error with a simple phone call.

Part two: How to respond to identity theft

This checklist is written in order of **typical importance** (though dependent on personal circumstances and extent of damage already done). As you go through each step **make notes or keep a log** of your actions including **who you've called, who you spoke to there, and any case ID or reference number of the conversation**. This will be helpful as you will be having many conversations and may need to recall what actions you've taken (particularly when reporting to authorities).

☐ Contact your bank/s and **put a freeze on all of your accounts** as a temporary measure. It's likely you will need to close your accounts and open new ones; however, the freeze is typically quicker to instigate saving you time to finish this checklist before returning to officially opening new accounts, transferring funds, and closing the compromised account/s which takes time.

☐ **Change your passwords** in order of importance and risk:

1. *Online banking accounts* including accounts which have access to funds or wealth (such as a share trading account)
2. *Email accounts* are next as they can be used for password reset procedures to your other accounts
3. *Online shopping accounts* as they may have stored card information
4. *Social media accounts*
5. *All other accounts* – ensure you check all other accounts irrespective of when you last used them.

Most password managers will have a function to do this en masse and change numerous passwords at once.

☐ **Alert family and friends** as they may be targeted for a scam posing as you. Send a mass SMS message which is short and to the point. We have one you can use at the bottom of this checklist.

☐ **Report it to the police** and take note of the reference / report number they provide you.

☐ **Alert any company** who you can no longer log in to when changing your passwords. Some may have long phone ques and it may be easier to visit the 'Help' section of their website to report fraudulent activity (some companies may not have this option, but many do).

- [ ] **Report it to your credit reporting agencies** and ask them to put an alert on your file to stop additional accounts being opened in your name.

- [ ] **Report it to your relevant identity theft taskforce** as listed at the end of this checklist. We can't list them all as our readers come from all around the world but most countries in the developed world will have a taskforce or agency devoted to this. Your report could help in their tracking and identification of bad actors involved in identity theft.

- [ ] **Report the loss of sensitive identification documents** (such as passports, driver's licences, social security cards, government issued identity cards) to the relevant government agency.

It is also a good idea to **request a credit report in 3-6 months** to confirm the credit agencies rectified your file correctly and removed the fraudulent accounts whilst seeing if there is any suspicious activity still going on.

We've also listed some precautions you can take to reduce the risks of identity theft in the future in our Identity theft 101 article.

Once you're on top of the issue look after your mental health and consider speaking to a counsellor if the damage has been severe or really taken a toll on you.

Appendix A: Example text message

Hi everyone, I think I have had my identity stolen so please be wary of any unusual requests from me and ignore them while I work through this. I will provide an update later today once I'm sure what's going on.

Appendix B: Who to contact

Here is a list of government agencies or support services to report to if you have been a victim of identity theft. They are current at the time of writing but can be replaced or amalgamated in the future. We have listed links to their websites below, if you prefer to contact them by phone or email first, those details are listed on the websites.

Australia:

Report to the Australian Cyber Security Centre:
https://www.cyber.gov.au/acsc/report

Report a scam to the Australian Competition & Consumer Commission:
https://www.scamwatch.gov.au/report-a-scam

United States of America:

Report to the Federal Trade Commission:
https://www.identitytheft.gov/

Report to the Federal Bureau of Investigation's Internet Crime Complaint Centre if the identity theft occurred online:
https://www.ic3.gov/

United Kingdom:

Report to the Action Fraud the National Fraud & Cyber Crime Reporting Centre (for England, Wales and Northern Ireland):
https://www.actionfraud.police.uk/

Report to Police Scotland if you live in Scotland:
https://www.scotland.police.uk/

Canada:

Report to the Canadian Anti-Fraud Centre:
https://antifraudcentre-centreantifraude.ca/