WHAT IS **IDENTITY THEFT?**

Identity theft is when someone steals your personal information or possessions so they can use your identity.

Identity fraud is when they use your identity for their own financial gain – usually at a great cost to you.

You might not even realise that your information has been stolen until after the fraud has happened and only find out when a bill arrives for something you didn't buy, or when you have trouble taking out a credit card or a mobile phone contract.

According to research from Experian's Victims of Fraud team, it takes an average of 292 days for people to discover their information has been used for fraudulent purposes.

5 common ways **fraudsters can steal your identity**

Common theft
You could be burgled and have your personal possessions taken, for example your purse containing your ID.

Cold-calling
Fraudsters call you pretending to be a genuine business and mislead you into giving away personal and financial information.

Hacking
Software is deployed to hack into your computer or information is taken from your smartphone.

Phishing
Fraudsters send an email that appears to be from a trusted company to get you to click a link and enter your personal information, such as your banking details.

Data breach
Customer information could be stolen from a service provider. There have been a number of high-profile data breaches in recent years.

How identity theft **could affect you**

Having your identity stolen and used fraudulently can hit your finances hard. Fraudsters could take money from your bank account or they could take out credit in your name. Their actions can hurt your credit score and affect your chances of getting credit in the future.

Thankfully in most situations the effects of fraud can be reversed. But this process can take an emotional toll on you and the impact can go on for much longer than the actual fraud itself – research by Experian's Victims of Fraud team shows that it can take a staggering 300 hours to set the record straight.

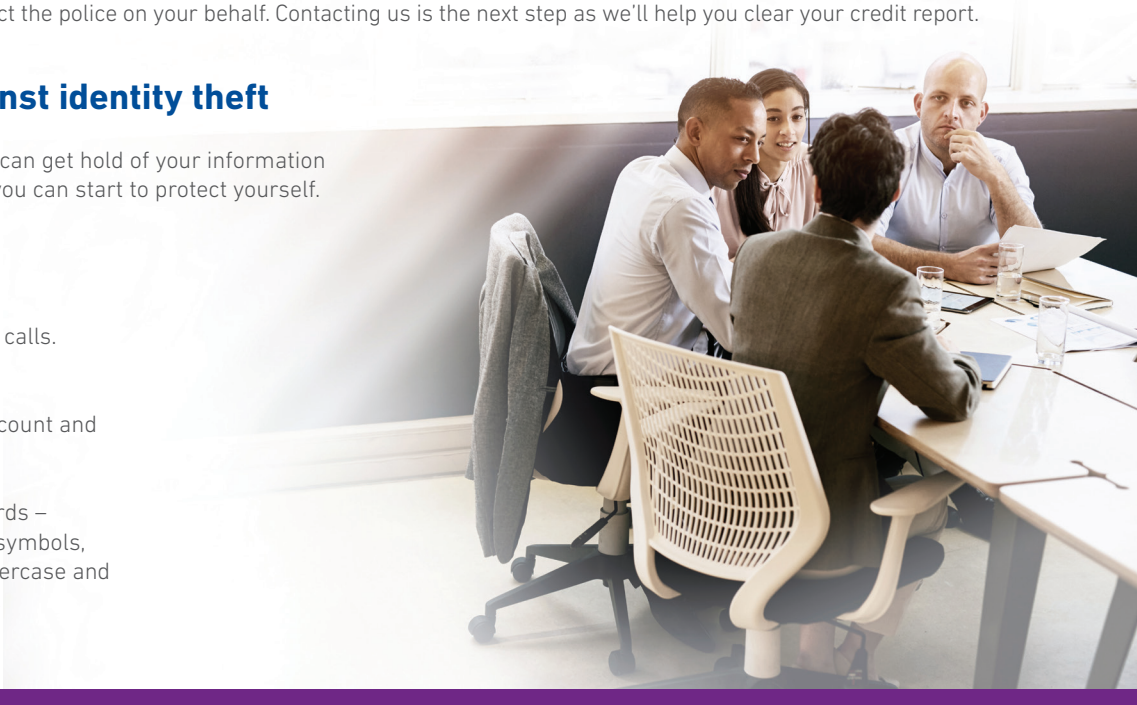
That's why it's important to act quickly. Your first step is to get in touch with your banks and lenders – they'll work with you to resolve the issues and if necessary will contact the police on your behalf. Contacting us is the next step as we'll help you clear your credit report.

Protect yourself **against identity theft**

There are many ways fraudsters can get hold of your information so there are a lot of good habits you can start to protect yourself.

These are our top three tips:

1. Never respond to unsolicited emails and phone calls.
2. Use different passwords for different accounts – particularly for your email account and online banking.
3. Use strong passwords made up of three random words – you can add in numbers and symbols, and use a combination of lowercase and uppercase letters if you want.



HOW TO PROTECT YOURSELF **AGAINST IDENTITY FRAUD**

Protecting yourself from identity fraud starts with keeping your personal information safe with a few simple habits.

There's a lot of advice out there, and that's because there are several ways criminals can steal and use your personal details to commit identity fraud.

Experian fraud experts bring you the dos and don'ts of protecting yourself against identity fraud.

If there are just three changes you make to your everyday habits, we'd recommend:

1. Don't respond to unsolicited emails and phone calls.
2. Use different passwords for different accounts – particularly for your email account and online banking.
3. Use strong passwords made up of three random words – you can add in numbers and symbols, and use a combination of lowercase and uppercase letters if you want.

Safe banking **and shopping**

- Never disclose your personal security details such as your PIN or full password.
- Never let your credit or debit card out of your sight.
- When entering your PIN, always shield the keypad and make sure no one is watching.
- Don't keep a written record of your PINs anywhere.
- Take extra care with contactless payment cards to avoid unauthorised payments
- Check your credit report for any signs of fraud.

Staying **safe online**

- Use strong passwords made up of three random words – you can add in numbers and symbols, and use a combination of lowercase and uppercase letters if you want.
- Use different passwords for different accounts - particularly for your email account and online banking.
- Keep the software on your computer and smartphone up to date.
- Check websites are secure by looking for the padlock symbol or 'https' at the start of the website address.
- Only enter your personal information or credit card details onto secure websites that belong to organisations you know and trust.
- If you're using public Wi-Fi, don't log in to any sites that need a password (eg your bank, social media or email) or enter personal information such as your card details.
- Look out for spelling and grammar mistakes. Genuine organisations won't send emails full of errors.
- Don't open attachments or click links on emails from un known sources.
- Don't enter your personal details when asked to do so via an email. For example, your bank would never email you asking you to confirm your internet banking username and password.
- Mark suspicious emails as junk mail and delete straight away.
- Don't use illegal streaming and downloading sites, as these often host malicious software or phishing scams.

Protecting **your devices**

- Secure your mobile phone or tablet with a screen lock. For added security, you can set it to lock automatically.
- Only download apps from reputable stores.
- Don't 'jailbreak' or 'root' your device as this makes it vulnerable to malicious software.

Handling **calls from strangers**

- Be cautious of unexpected phone calls.
- Be sure you know who you are talking to – it's a good idea to hang up and call the organisation back on its official number.
- Don't give away personal information to someone who has cold-called you.
- Don't be rushed into making a decision or sharing information – a genuine organisation won't mind waiting.
- If something doesn't feel right, listen to your instincts

Managing your social media profile

- Don't share personal details such as your date of birth or home address.
- Think twice about using location features that automatically make your whereabouts known.
- Only accept friends who you actually know.
- Set your privacy settings so that only your friends see what you post.

Managing **your mail**

- Always shred or destroy documents that contain personal information, like your name, address or financial details, before throwing them away.
- If you're expecting a bank or credit card statement that doesn't arrive, let your bank know.

HOW TO SPOT THE **WARNING SIGNS OF IDENTITY FRAUD**

Identity fraud can be damaging both financially and emotionally. Thankfully there are steps you can take to prepare and protect yourself and limit the chance of it happening.

If you are at risk of identity fraud, there are likely to be warning signs. Knowing what these are can help you spot the fraud early, keeping the damage to a minimum.

Actively look for **signs of fraud**

- **Check for unusual transactions**
  Always check your credit card and bank statements when you receive them, and make a habit of checking them online on a regular basis. Look for purchases you didn't make and charges you don't recognise.

- **Keep track of your mail**
  Not receiving regular bank or credit card statements could be a sign that they've been re-routed to a fraudster. The same goes for important personal documents you're expecting which fail to come through the post.

- **Check your credit report**
  You should check your credit report regularly as many of your financial accounts are detailed in it. According to our research, it takes an average of 292 days for people to discover their information has been used for fraudulent purposes. Checking your credit report lets you spot fraud early. Look out for:

- Searches on your report made by lenders as a result of a credit application.
- Home addresses that aren't yours.
- Loans and accounts that you didn't apply for.

Other warning **signs of fraud**

- Email confirmations for purchases you didn't make or emails demanding payment for an account you didn't set up.
- Credit cards arriving in the post which you didn't apply for.
- Bills from companies that you've had no dealings with.
- Debt collection agencies contacting you about bills you don't recognise.
- Being told that you've been approved or denied credit for accounts that you know nothing about.
- Being refused when you apply for a loan or credit card even though you know you have a healthy credit score.

It can be easy to overlook emails in your already jam-packed inbox or to monitor everything coming through the post. But being vigilant and creating a monitoring routine can highlight suspicious activity and protect you from identity fraud.

WHAT TO DO IF YOU'RE A **VICTIM OF IDENTITY FRAUD**

Becoming a victim of identity fraud can be emotionally upsetting.

You are probably feeling very overwhelmed but it's important to take action quickly when you realise your identity has been stolen.

Contact **your bank**

- Immediately report any lost or stolen credit or debit cards to the organisations that issued them.
- Contact the relevant bank, credit card provider or other lenders (as well as any others you have accounts with) to inform them that you've been the victim of identity fraud. They will investigate the issue and, in some instances, they will contact the police on your behalf. Be prepared to provide proof of your identity and statements showing your home address if requested.
- If a bank or lender contacts you about credit that you don't know anything about, tell them this right away.

Contact **Experian**

- Get a copy of your Experian Credit Report and check it for fraudulent information.

Stay in **control**

- Keep a record of all your calls, letters and emails about the fraud.
- Report all lost or stolen documents such as passports or driving licences to the issuing organisations.

Report suspected fraud to the **Southern African Fraud Prevention Service (SAFPS**)

- Report suspected fraud to the SAFPS helpline: 0860 101 248 or visit www.safps.org.za