SECURITY GUIDE

The McAfee Safety Series

Identity Protection Guide

Table of Contents

There's no one else like you. Let's help keep it that way.. 3

Section One—Get to know your identity 5

What is identity fraud and identity theft? 5

How does identity fraud and theft happen? 6

How do thieves get ahold of personal information? 7

What are some of the signs your identity is being used by someone else? 8

Section Two—Identity protection checklist 9

Steps for prevention 10

Steps for security 12

Steps for monitoring 14

Section Three—What to do if you're a victim 16

Five steps for recovering from identity fraud or theft 17

Why identity protection matters for ***everyone***—including the kids. . . . 19

About McAfee 20

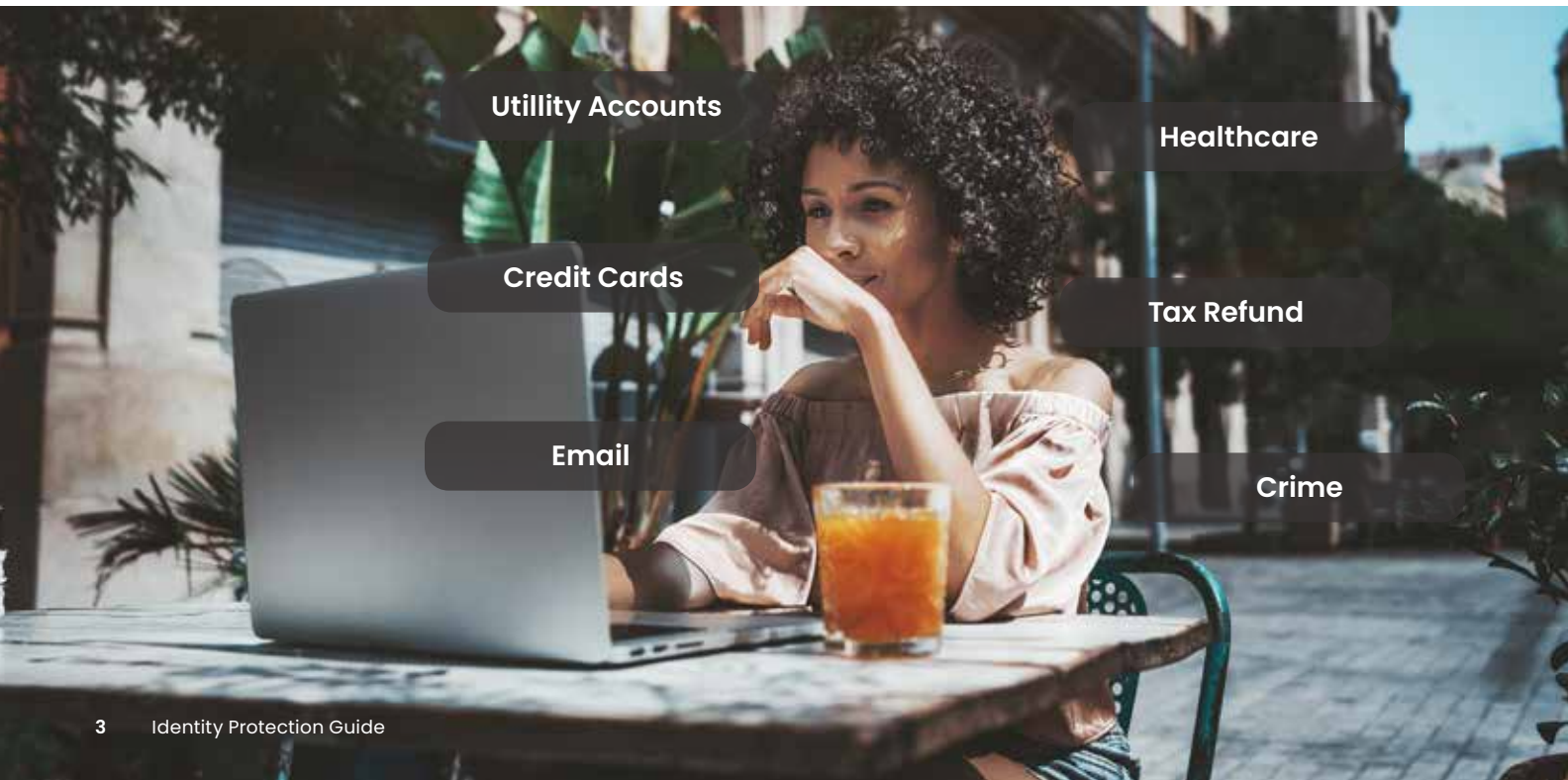
There's no one else like you. Let's help keep it that way.

It's been like this from the start—wherever people shop, do business, or simply gather together, you'll find thieves in the mix, ready to take advantage. And that's truer today when it comes to life online.

Online crime has continued its steady climb over recent years, with identity crime a major contributor. Data breaches flood marketplaces on the dark web with personal information, malware and phishing stealing millions of login credentials, while other hacks force their way into accounts with weak or compromised passwords. In a time where the internet has so much to offer us in terms of convenience, connection, and enjoyment, thieves find a way to turn it to their advantage.

What's at risk with identity theft? Depending on the type and amount of information an identity thief gets their hands on, they can cause harm to your finances and reputation in several ways, including:

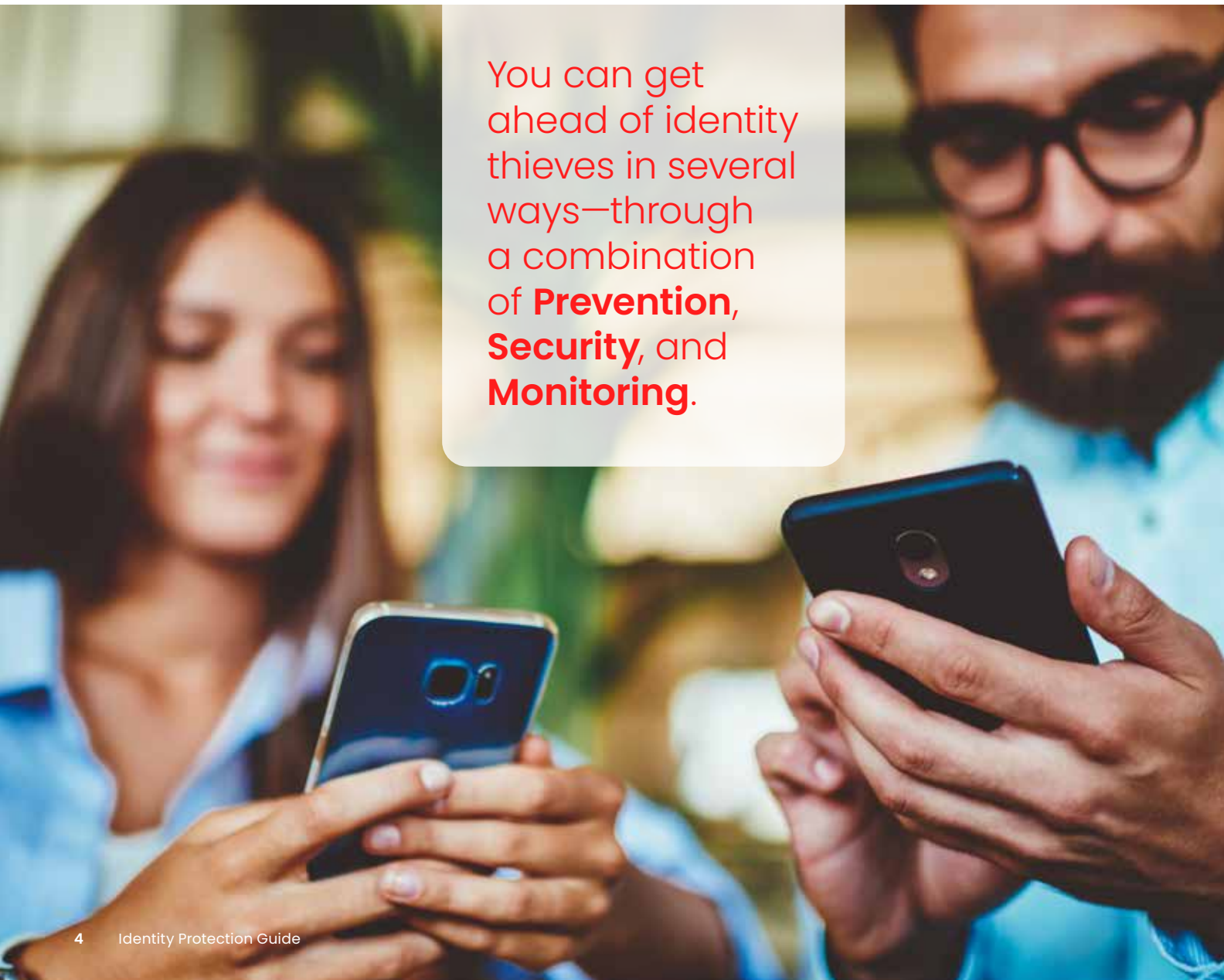
- Opening utility accounts in your name.
- Using your credit cards for unauthorized purchases.
- Hijacking your email.
- Claiming healthcare expenses under your insurance.
- Stealing your tax refund.
- Assuming your identity when they're arrested for a crime.



With so much of our information and data "out there" online, the idea of protecting your identity can feel daunting. *Where to start? What to do? Isn't some of this simply out of my hands?* The truth is that you have far more control over your identity than you might think, ways you can shore it up and make it far more difficult for thieves to steal.

You can get ahead of identity thieves in several ways—through a combination of **Prevention**, **Security**, and **Monitoring**. We'll look at all three in this guide, along with a quick primer on how identity thieves pull off fraud and theft, so you know what you're up against.

Once we're through, you'll see that with the right techniques and tools you can stay far safer than before.



Section One—Get to know your identity

Let's get into the basics of your personal identity, which will set the groundwork for the protections we'll talk about next. A set of four questions will guide the way:

- What is identity fraud and theft?
- How does identity fraud and theft happen?
- How do thieves get ahold of personal information?
- What are some of the signs your identity is being used by someone else?

What is identity fraud and identity theft?

For starters, there are two primary types of identity crime: identity fraud and identity theft. What's the difference between the two? Well, it's subtle, so much so that it's easy to use them nearly interchangeably. While both can take a bite out of your wallet, they are different—and knowing the differences can help you know understand what's at stake.

Let's start with some definitions and a few examples of each.

Identity fraud is ...

- When someone steals or misuses your personal information to exploit an account or accounts you already have.
- Examples:
  - A criminal gets ahold of your debit card information from a data breach and makes purchases with it against your bank account.
  - A criminal gains access to one of your social media accounts via a phishing attack and then starts posting messages under your name.

Identity theft is ...

- When someone uses your personal information to open and abuse new accounts or services in your name—or possibly to impersonate you in other ways.
- Examples:
  - A criminal uses your personal information to open a new line of credit at a retailer under your name and then makes purchases against the line of credit.
  - A criminal uses your Social Security Number to create a driver's license with their likeness but with your name and personal information.

So, there's that subtle difference we mentioned. Identity fraud involves misuse of an existing account. Identity theft involves stealing your personal information, which is then used to impersonate you in some way, such as opening new accounts in your name.

How does identity fraud and theft happen?

It starts with your **Personally Identifiable Information (PII)**. One way to think about your identity is like a jigsaw puzzle. Hundreds, if not thousands, of pieces make up your identity. Collectively, they're known as Personally Identifiable Information, or PII for short. PII is information about you that others can use to identify you, whether directly or indirectly.

A prime example of direct PII is your **tax ID number** because it's unique and directly associated with your name. Further instances include your **facial image** to unlock your smartphone, your **medical records**, your **finances**, and your **phone number** because each of these can be directly linked back to you.

Then there are indirect pieces of PII that act as helpers. While they may not clearly identify you on their own, a few of them can when they're added together. These helpers include things like **internet protocol (IP) addresses**, the unique **device ID** of your smartphone, or other identifiers associated with your browsing or device usage.

Thus, PII could identify you on its own, or it could identify you when it's linked to other identifiers, like the ones associated with the devices, apps, tools, and protocols you use. In other words, if an identity thief patches together a few pieces of your PII or gets ahold of a key piece of PII like a tax ID number, that completes just enough of the jigsaw puzzle picture needed to steal your identity.

One way to think about your identity is like a jigsaw puzzle. Hundreds, if not thousands, of pieces make up your identity.

How do thieves get ahold of personal information?

Physical Theft

One of the readiest examples involves losing your wallet or debit card—or having them stolen outright. There are also instances where thieves will go through trash for bills and statements to gather personal information from them. Mailbox theft is in the mix too. Thieves will simply **grab sensitive pieces of mail before you can get to them**. And in more extreme cases, thieves will register a change of address with a bank, credit card, or utility to have your mail routed to them, where they can harvest your PII and put it to their own illegal use.

Digital Theft

Life online opens a multitude of avenues for the theft of PII. Data breaches at retailers, healthcare providers, insurance companies, financial institutions, and so forth can pump millions of people's PII into the hands of bad actors—whether directly or when crooks post it for resale on dark web marketplaces. Digital theft can also involve a dedicated crook piecing together various bits of personal information that have been gathered from **social media**, **phishing attacks**, or **malware** designed to harvest information.

Additionally, thieves may eavesdrop on public Wi-Fi and **steal information from people who're shopping or banking online** without the security of a VPN. Also through public Wi-Fi, hackers may compromise point-of-sale terminals and ATMs so that they can "skim" credit or debit card information during the transaction.

What are some of the signs your identity is being used by someone else?

Identity thieves leave a trail. With your identity in hand, they can charge things to one or more of your existing accounts (**identity fraud**)—and if they have enough information about you, they can even create entirely new accounts in your name (**identity theft**). Either way, once an identity thief strikes, you're probably going to notice that something is wrong.

Possible signs include:

- You start getting mail for accounts that you never opened.
- Statements or bills stop showing up from your legitimate accounts.
- You receive authentication messages for accounts you don't recognize via email, text, or phone.
- Debt collectors contact you about an account you have no knowledge of.
- Unauthorized transactions, however large or small, show up in your bank or credit card statements.
- You apply for credit and get unexpectedly denied.
- And in extreme cases, you discover that someone else has filed a tax return in your name.

As you can see, the signs of possible identity compromise run a wide range, going anywhere from the curious to the outright alarming. Additionally, they crop up as a surprise. They can appear long after the actual fraud or theft has occurred, like when you check your credit report and see a year-old balance on an account you never opened.

We'll cover what to do if you suspect that your identity has been compromised—but first, let's look at ways you can prevent it from happening in the first place, through Prevention, Security, and Monitoring.

Section Two—Identity protection checklist

You can keep identity fraud and theft at bay by taking steps that fall into three groups—**Prevention**, **Security**, and **Monitoring**.

Below is a checklist that highlights the steps, each of which we'll cover in detail. While the list is certainly comprehensive (yet by no means exhaustive), the good news is that plenty of steps are rather straightforward, and many more are handled for you with online protection software.

Steps for Prevention

- Invest in a paper shredder.
- "Shred" your digital documents too.
- Protect your tax ID number.
- Lock your devices with a passcode.
- Learn how to remotely lock and wipe your devices.
- Clean up your personal data online.

Steps for Security

- Use online protection software.
- Create strong, unique passwords for every account with a password manager.
- Spot and avoid phishing attacks.
- Consider a credit lock.
- Look into a security freeze.

Steps for Monitoring

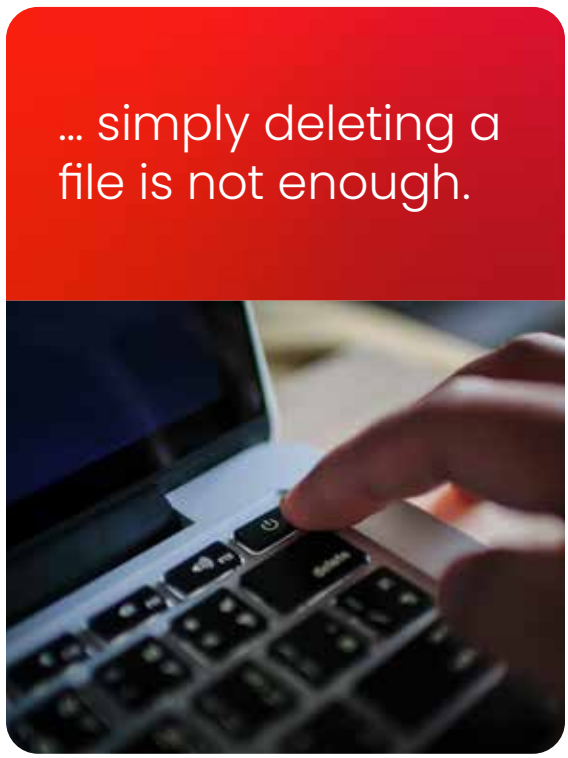
- Check your bills and statements.
- Find out your Protection Score.
- Monitor your credit.
- Monitor your identity.
- Take advantage of identity protection.

Steps for prevention

Limiting your exposure to threats

Invest in a paper shredder. Sensitive documents come in all forms. Top-of-the-line examples include things like tax returns, bank statements, and financial records. Yet there are also things like your phone and utility bills, statements from your doctor's office, and offers that come to you via mail. Together, these things can contain personal information such as account numbers, your full Social Security Number, the last four digits of your Social Security Number (which can still be useful to thieves), and other information that may uniquely identify you.

You'll want to dispose of sensitive documents like these so that they can't be harvested by hackers. For physical documents, consider the low-cost investment of a paper shredder to help ensure they don't fall into the wrong hands when you are done with them. (And let's face it, they're fun to use!)



"Shred" your digital documents too. For things like electronic tax forms, financial records, and other sensitive data on your computer, simply deleting a file is not enough. That data remains on the drive until it is written over or otherwise removed permanently. One way to go about that is with a digital document shredder that renders the data practically unusable when you're ready to trash the file. Comprehensive online protection software will often include such a feature, such as our own file shredder.

Protect your tax number. This is one of the most prized possessions a thief can run away with because it is so closely associated with you and things like your tax returns, employment, and so on. Keep it stored in a safe location rather than on your person or in your wallet. Likewise, be careful about giving it out. For example, in the U.S., many organizations may ask for a Social Security Number as a form of identification. (Doctor's offices are a prime example.) However, only organizations like the IRS, your bank, and employer require it. If you get such a request from someone other than those organizations, ask them what they intend to use it for and then ask if another form of identification will work instead.

Lock your devices with a passcode. Our recent worldwide study found that only 58% of adults protect their computers with a passcode and only 56% do the same on their smartphones. When you consider all the personal and financial information we keep on these devices, a lost or stolen device becomes an open book for an identity thief. Using a passcode, facial ID, PIN, or other form of locking your devices can make life tough on a thief in the unfortunate event of loss or theft.

Learn how to remotely lock and wipe your devices. Many laptops and mobile devices have location tracking services to help find a lost device—in addition to features that let you remotely lock or even wipe the contents of the device if you fear it's lost for good or fallen into the wrong hands.

- Apple provides iOS users with a step-by-step guide for remotely wiping devices.
- Google offers up a guide for Android users as well.
- For laptops, Microsoft and Apple users can enable the following settings:
  - Windows: Enable in Settings > Update & Security > Find my device
  - macOS: Enable via Settings > Your Name > iCloud > Find My Mac

Clean up your personal data online. Earlier we likened your PII like to the pieces of a puzzle. With enough pieces in place, a thief can attempt to steal your identity. However, they don't always need to go to a dark marketplace online to get useful pieces. Another place they can get it is from websites that gather personal information from public records, social media, and other online sources. Known as data broker sites, they build profiles of individuals that identity thieves, hackers, and spammers can use to wage their attacks.

While getting your info removed from these sites can seem like a daunting task (Where do I start, and just how many of these sites are out there?), we're rolling out our **Personal Data Cleanup**[1] to help. It regularly scans these high-risk data broker sites for info like your home address, date of birth, and names of relatives. It identifies which sites are selling your data, and also depending on your plan, automatically requests removal.

1. Personal Data Cleanup is not available in all plans or locations.

Steps for security

Putting safeguards in place

Use online protection software. Given all the banking and shopping we do on our computers and phones, let alone all the other activities that leave a trail of PII in their wake, installing and using comprehensive online protection software is a must these days. It puts several layers of security in place, such as creating complex passwords automatically, antivirus, protecting your privacy and data online like connecting with a VPN, and a host of other features for keeping you safe. In short, online protection software acts as a solid first line of defense.

Create strong, unique passwords for *every* account. Comprehensive online protection software often includes a password manager that can generate strong, unique passwords for each of your accounts and remember them for you. It's extra protection that makes life a lot easier for you by managing all the accounts you're juggling. Also, use MFA (multi-factor authentication) on the accounts that give you the option, which makes it harder for a thief to crack your accounts with a password alone.

Spot and avoid phishing attacks. Phishing attacks are one of the primary ways identity thieves steal personal information. Whether they come via a direct message, social media, email, text, or phone calls, thieves use them to harvest your personal info by posing as a legitimate organization—such as in this recent IRS phishing scam in the U.S.

Phishing attacks often prompt you to click a link or download an attachment or software. The best advice is don't click. If you get a notification that appears to be from one of your accounts, go directly to their website and log in from there to follow up. Also, be wary that many phishing attacks play on emotions and sense of urgency. That's another sign the message could be bogus. Comprehensive online protection software like ours will also provide you with safe browsing features that can help you steer clear of malicious links and downloads.

Phishing attacks are one of the primary ways identity thieves steal personal information.

Consider a credit lock. As mentioned above, identity thieves can open accounts in your name and damage your credit along the way. A credit lock can help keep that from happening. The protection offered will vary depending on where you live and the credit reporting agencies involved, yet it restricts access to your credit reports. This keeps companies from accessing your credit report, which can prevent thieves from opening accounts in your name. A credit lock will also prevent you from opening new accounts when it's in place, so using a lock takes some careful planning if you're about to rent an apartment, take out a car loan, apply for a new credit card, and so on.

For more information, check with the credit bureaus in your country—in the U.S., the major three being Equifax, TransUnion, and Experian. Likewise, depending on your location and plan,[2] you can establish a credit lock from your McAfee online protection software (and lift it as needed), which prevents unauthorized people from opening accounts in your name.

Note that when using McAfee's credit lock feature, remember to freeze the other two Bureaus in conjunction with the Credit Lock to ensure all Bureaus are covered.

Look into a security freeze. Another feature offered by McAfee depending on your location and plan[3] is a security freeze. It provides you with guidance on initiating a security freeze, including three varieties:

- **Credit freeze:** Stops creditors from accessing your info to open new loans or credit cards.
- **Bank freeze:** Prevents fraudsters from opening a bank account in your name.
- **Utility freeze:** Prevent someone from opening a telecom, electric, water or other utility in your name.

Note that a credit freeze differs from a credit lock, so you'll need to check with your credit bureau for full details before establishing one.

What's the difference between a credit lock and a credit freeze?

- Both can prevent unauthorized access to your credit info on the three main credit bureaus.
- In the U.S., a credit freeze is free and requires additional information and a PIN to establish and use.
- Offers, features, and terms may vary between the bureaus. Check with each for details.

—Source, *Nerdwallet*

2. Credit lock is not available in all plans or locations.
3. Security freeze is not available in all plans or locations.

Steps for monitoring

Keeping tabs on your identity

Check your bills and statements. Whether they come in the mail, email, or if you simply look them up online when it comes time to pay them, give your bills and statements a close review. Not every case of identity theft comes with a big-ticket purchase or outlandish charge. Even the smallest of suspicious charges could indicate a larger problem. If you spot an unknown charge, follow up with the company or institution in question and file a fraud report with them as needed.

In the case of credit and debit cards, the institution may go ahead and issue you a new physical card and account number along with it. Go ahead and update your passwords associated with that account as well. A password manager can help, and now would be a good time to start using one if you haven't already.

Find out your Protection Score. One of the trickiest parts of staying safe online is knowing exactly how safe you are. *Do I have the right protection in place? Is there more I could be doing?* Those are good questions to ask, and now you can get the answers to them with your Protection Score. As part of your McAfee subscription,[4] the Protection Score gives you a clear and easy-to-read overview of your online protection and how healthy it is. Next, it identifies and helps you fix security weak spots with simple instructions and then offers personalized feedback that helps you maintain healthy online protection.

For example, one way your Protection Score can help keep your identity secure is in the case of data breach. If your information is found in a data breach, your Protection Score goes down and your app sends you an alert. It then assists you in resolving the breach, your Protection Score goes back up, and monitoring continues, maintaining a lookout for future breaches and issues.

4. Protection Score is not available in all plans or locations. For more information on what factors affect your Protection Score and how it is calculated, see our Protection Score page and FAQs. An excellent score does not guarantee total safety. No connected life can be totally secure, but an excellent score does show you're doing a good job of preventing and handling risks.

Monitor your credit. In addition to keeping an eye on your bills and statements as they come in, a credit monitoring service keeps daily tabs on your credit report. While you can do this manually, there are limitations. First, it involves logging into each bureau and doing some digging of your own. Second, there are limitations as to how many free credit reports you can pull each year. A service does that for you and without impacting your credit score.

Depending on your location and plan,[5] McAfee's credit monitoring allows you to look after your credit score and accounts to see fluctuations and help you identify unusual activity, all in one place, checking daily for signs of identity theft.

Monitor your identity. When we mentioned Personal Data Cleanup earlier, we brought up the dark web where PII is bought and sold, stored, and exchanged. The problem is that it's particularly difficult for you to determine what, if any, of your PII is on the dark web where hackers and thieves can get their hands on it. Identity monitoring can help.

McAfee's identity monitoring helps you keep your personal info safe by alerting you if your data is found on the dark web, an average of 10 months before our competitors. Monitored info can range anywhere from bank account and credit card numbers to your email addresses and government ID number, depending on your location.[6] If your information gets spotted, you'll get an alert, along with steps you can take to minimize or even prevent the damage if the information hasn't already been put to illegal use.

Take advantage of identity protection. Identity protection through McAfee takes identity monitoring a step further by offering, depending on your location and plan, identity theft coverage for financial losses and expenses due to identity theft, in addition to hands-on help from a recovery professional to help restore your identity—all in addition to the identity monitoring called out above, again depending on your location and plan.

5. Credit monitoring may not be available in all plans or locations.
6. Not all identity monitoring elements are available in all countries.

Section Three—What to do if you're a victim

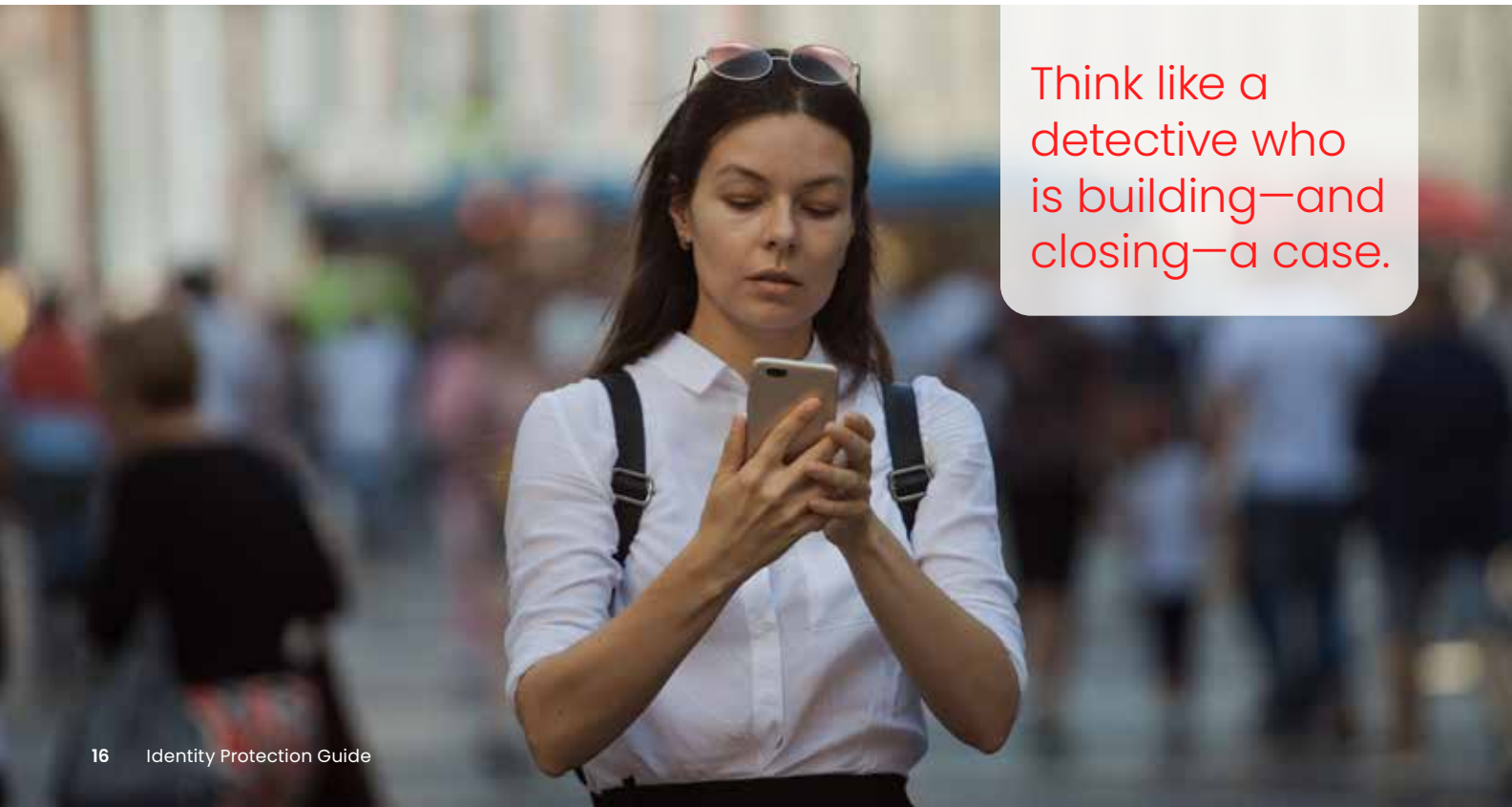
Another hard and fast truth about identity fraud and theft is that there's no sure-fire way of keeping them from happening entirely—even with Prevention, Security, and Monitoring precautions in place.

Whether you spot one of the warning signs we detailed earlier, or if you receive an alert from your monitoring service, there are several steps you can take if you think you've fallen victim to identity fraud or theft:

- Notify the companies involved.
- File a police report.
- Contact your governmental anti-fraud or trade organization.
- Put on a credit freeze or lock.
- Continue to monitor.

Realizing that you've become a victim carries plenty of emotion with it, which is understandable—the thief has stolen a part of you to get at your money, information, or even reputation. Once that initial rush of anger and surprise has passed, it's time to get clinical and get busy.

Think like a detective who is building—and closing—a case. That's exactly what you're doing. Follow the steps, document each one, and build up your case file as you need. Staying cool, organized, and ready with an answer for any questions you'll face in the process of restoring your identity will help you see things through.



Five steps for recovering from identity fraud or theft

1. Notify the companies involved.

Whether you spot a curious charge on your bank statement, discover potentially a fraudulent account when you check credit report, or when you get an alert from your monitoring service, let the bank or organization involved know you suspect fraud or theft. With a visit to their website, you can track down the appropriate number to call and get the investigation process started.

2. File a police report.

Some businesses will require you to file a local police report to acquire a case number to complete your claim. Beyond that, filing a report is a good idea in itself. Identity theft is still theft and reporting it provides an official record of the incident. Should your case of identity theft lead to someone impersonating you or committing a crime in your name, filing a police report right away can help clear your name down the road. Be sure to save any evidence you have, like statements or documents that are associated with the theft. They can help clean up your record as well.

3. Contact your governmental anti-fraud or trade organization.

In the U.S., the identity theft website from the Federal Trade Commission (FTC) is a fantastic resource should you find yourself in need. In addition to keeping records of the theft, the FTC can provide you with a step-by-step recovery plan—and even walk you through the process if you create an account with them. Additionally, reporting theft to the FTC can prove helpful if debtors come knocking to collect on any bogus charges in your name. With a copy of your report, you can ask debtors to stop.

Likewise, other nations have similar resources available as well:

- In the UK; https://www.actionfraud.police.uk/
- In Ireland: https://www.garda.ie/en/crime/fraud/
- In Canada, https://www.antifraudcentre-centreantifraude.ca/
- In Australia, https://www.counterfraud.gov.au/find-where-report-fraud
- In New Zealand, https://sfo.govt.nz/

Also contact your national tax or revenue agency as well if you believe your tax ID number was involved in identity fraud or theft. They will have their own reporting mechanisms and processes to assist you with the recovery process.

4. Put on a credit freeze or lock.

An instance of identity fraud or theft, suspected or otherwise, is a good time to review your options for a credit freeze or lock. As mentioned earlier, see what the credit bureaus in your region offer, along with the terms and conditions of each. With the right decision, a freeze or lock can help minimize and prevent further harm.

5. Continue to monitor.

Strongly consider using a monitoring service like the one we described earlier to help you continue to keep tabs on your identity. The unfortunate fact of identity theft and fraud is that it can mark the start of a long, drawn-out affair. One instance of theft can possibly lead to another, so even what may appear to be an isolated bad charge on your credit card calls for keeping an eye on your identity all around. Many of the tools you would use up to this point still apply, such as checking up on your credit reports, maintaining fraud alerts as needed, and reviewing your accounts closely—along with utilizing an identity monitoring service.

6. Work with a recovery pro.

A recovery service can help you clean up your credit in the wake of fraud or theft, all by working on your behalf. Given the time, money, and stress that can come along with setting your financial record straight, leaning on the expertise of a professional can provide you with much-needed relief on several counts.

Why identity protection matters for *everyone*—including the kids.

Protecting your identity is a family affair.

Identity fraud and theft isn't limited to adults—or even older teenagers who're opening their first accounts with banks, online shopping sites, and online games. It can affect even the youngest of children.

In fact, little ones are high-value targets for cybercriminals because we typically don't run credit reports on children. In this way, an identity thief who holds the Social Security Number of a child in the U.S. can potentially open all manner of credit and accounts and go undetected for years until that child attempts to rent an apartment or apply for their first credit card.

So, while we've outlined how you can protect your identity through Prevention, Security, and Monitoring, you can take the same steps for your children as well. Everyone in the family can benefit from identity protection.

Identity Protection = Confidence

While setting yourself up with strong identity protection calls for some up-front effort, many of the protections take care of the work for you once you have them in place. Considering the continued rise of identity theft, the effort is worthwhile, particularly compared to the potential financial and reputational costs that can follow in the wake of an attack.

The ultimate benefit, though, is confidence. With identity protection working on your behalf, it frees you to enjoy your time online knowing that what's personal and private can stay that way.

For more on protecting your identity and online protection overall, our blog offers you and your family a terrific resource across a wide range of topics from online banking, gaming, and shopping to tough-yet-important topics like cyberbullying and which apps are safe for kids.

Our aim is to help you think about what's best for your family and the steps you can take so that you can make everyone's time online safer and more enjoyable.

Visit us any time!

https://www.mcafee.com/blogs/

About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

www.mcafee.com

For more information about online protection, visit us at mcafee.com/blogs

McAfee™

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com