Identity Theft Remediation Guide

Derrell Crimm
AC Financial Partners
1800 International Park Drive | Suite 10 | Birmingham, AL 35243
205.235.3500 | 205.235.5170 fax | www.acfinancialpartners.com | derrell.crimm @acfinancialpartners.com

Table of Contents

Derrell Crimm

AC Financial Partners
1800 International Park Drive | Suite 10 | Birmingham, AL 35243
205.235.3500 | 205.235.5170 fax | www.acfinancialpartners.com | derrell.crimm @acfinancialpartners.com

Identity Theft

Identity theft is when someone uses your personal information without your permission. Typically, criminals attempt to use this information for their own financial gain. For example, a criminal may fraudulently open a credit card or withdraw funds from a victim's bank account. In the worst-case scenario, a thief may take over a victim's identity altogether.

Unfortunately, identity theft has become a major phenomenon that victimizes millions of people each year. The number of crimes has increased at an alarming rate over the past few years, especially as criminals have become more adept at obtaining personal identifying information, such as passwords, over the internet.

If you believe you've become a victim of identity theft or fraud, act immediately to mitigate damages to your finances, credit, and reputation. At first, this may seem to be an overwhelming task, but with fast action and the proper steps, you'll be well prepared to remedy the identity crimes perpetrated against you.

Derrell Crimm, CFP®

AC Financial Partners
1800 International Park Drive | Suite 10 | Birmingham, AL 35243
205.235.3500 | 205.235.5170 fax | www.acfinancialpartners.com | derrell.crimm @acfinancialpartners.com

Basic Steps to Take in the Event of Identity Theft

If you fall victim to identity theft, be sure to take the following steps right away, no matter the specifics of the crime:

- Visit identitytheft.gov to select your identity theft scenario and develop a recovery plan. This process will also generate an identity theft report for the Federal Trade Commission (FTC).
- Contact the three major credit bureaus (Equifax, Experian, and TransUnion) to put an initial or extended free fraud alert on your credit file to make it harder for identity thieves to open accounts in your name. It also requires businesses to verify your identity before issuing credit.
- Place a free credit freeze to prevent anyone from opening a new line of credit in your name. A credit freeze will not affect your credit score.
- Order a free credit report from Annual Credit Report or call 877.322.8228. Your credit report is a summary of your credit history. It lists your name, address, social security number, credit cards, loans, how much money you owe, and information on whether you pay your bills on time or late.
  - One way to protect your personal information is to learn what information is in your credit report. Take a look at the *Inquiries* section—that's where you'll see who else checked your credit, and it can be an early warning sign of a problem.
  - When you get the report, make sure all the information is about you. If you don't recognize something, it could mean someone stole your identity. You'll need to contact any of your accounts that may be affected by identity theft.
- Employ identity theft protection services, which offer valuable tools to help protect your identity, such as real-time credit monitoring, customized account alerts, and 24/7 live support. They generally have a subscription fee.
- Think about where this information could have possibly leaked from and secure it. Frequently, these types of incidents trace back to a weak password on an online account that you may not have updated in a while. Next, ensure that all your accounts have unique, strong passwords, and update them frequently. A strong password includes 12 or more characters, as well as a mixture of uppercase and lowercase letters, numbers, and symbols.
- If your email account was hacked, review the mail forwarding rules in your account and delete any that you don't recognize. Attackers often add these rules so that when your account sends or receives certain emails, those emails are forwarded to the attacker, even after you've regained access and changed your password.

Derrell Crimm, CFP®

AC Financial Partners
1800 International Park Drive | Suite 10 | Birmingham, AL 35243
205.235.3500 | 205.235.5170 fax | www.acfinancialpartners.com | derrell.crimm @acfinancialpartners.com

- Ensure that multifactor authentication is enabled on your important online accounts, where applicable. This safeguard reduces the risk of an attacker compromising your account by requiring more than one form of identification, such as something the user should know (e.g., password, PIN) combined with something the user has (e.g., a smartphone, a hardware token).
- Keep a close eye on your online financial accounts. Report any suspicious charges to your financial institutions immediately.
- Contact any financial institutions with which you hold accounts and let them know about the theft. They will inform you of any additional security procedures or safeguards to help you secure your accounts and information from future fraud.
- File a police report with your local jurisdiction. While your city or county may not be able to investigate this crime, having a police report can be an essential document to help you to recover from identity theft.
- Consider identity theft insurance to help you recover from the costs related to identity theft. For example, you can be reimbursed (up to your policy limit) for expenses you had in order to restore your identity. Keep in mind, identity theft insurance typically only covers the expenses that happen after the identity theft occurs (like legal fees, lost wages, and application fees). It won't cover direct financial losses you incurred as a result of the identity theft, like fraudulent charges on your credit card statement.
- Visit the FTC's website for more information and resources about identity theft. This site has some great tips to help you secure your personal information.

Additional Steps If You Fall Victim to a Specific Type of Identity Theft

Not all identity crimes are the same. Be sure to take targeted actions to address the theft depending on how exactly your information was stolen or compromised.

Tax Fraud

Tax-related identity theft occurs when someone uses your stolen social security number to file a tax return claiming a fraudulent refund. If you fall victim to tax fraud, be sure to take the following steps:

- If you suspect or have knowledge of the fraudulent use of your social security number, notify the IRS immediately with a completed identity theft affidavit or Form 14039.
- If you receive a letter from the IRS indicating that you are a victim of identity theft, respond immediately and follow the steps provided.
- Close any financial or credit accounts opened by identity thieves.
- Report the fraudulent use of your social security number to the Social Security Administration (SSA), and review your social security statement. The SSA identity theft guide has additional information about applying for a new number, if necessary.
- Place a fraud alert on your credit with the three major credit bureaus to warn you of any suspicious activity. Request a freeze on your credit as well.
- File your tax return as soon as possible in the future. You can prevent future risk of falling victim to tax fraud again, to a certain extent, by filing early.
- Read the IRS's taxpayer identity theft guide for additional information.

Derrell Crimm, CFP®

AC Financial Partners
1800 International Park Drive | Suite 10 | Birmingham, AL 35243
205.235.3500 | 205.235.5170 fax | www.acfinancialpartners.com | derrell.crimm @acfinancialpartners.com

Car or Home Break-In

Many criminals opt for low-tech methods for stealing personal information, including breaking into homes and cars. If your property has been broken into, here are some steps to help you secure any potentially stolen information:

- Sort through your belongings to look for any missing papers or devices that may contain personal information.
- If you notice your credit or debit cards were taken during the break-in, immediately alert your bank to the theft. A bank representative can help you identify any fraudulent charges, cancel the stolen cards, and request new cards.
- Contact your local authorities and file a police report about the incident. Provide them with information about the incident's location and the stolen items.
- Consider filing an insurance claim. The decision of whether to file an insurance claim will likely depend on what was stolen during the break-in. If the dollar amount significantly exceeds your deductible, then you may want to file an insurance claim. Stolen personal information will need to be addressed through a homeowner's or renter's claim.
- Contact your insurance agent, give them the police report number, and then send them the information about the break-in. If your insurance company needs any more details, they will request them from you as you are navigating the claim process.

Stolen Social Security Number

If your social security number has been compromised, be sure to immediately take the following actions to address this theft:

- Report the fraudulent use of your social security number to the SSA, and review your social security statement. Read the SSA identity theft guide for additional information about applying for a new number, if necessary.
- Visit identitytheft.gov to select your identity theft scenario and develop a recovery plan. This process will also generate an identity theft report for the FTC.
- File a police report.
- Place a fraud alert on your credit with the three major credit bureaus.
- Request a freeze on your credit.

Credit Card Fraud

If your credit or debit card is lost or stolen—or the number has been used to make fraudulent charges—federal law limits your liability. You must act quickly to rectify unauthorized purchases and prevent future fraud. Be sure to take the following steps:

- Contact your bank or credit card company. Inform them of the date and time that you realized that your card was lost or stolen. If the card was used to make unauthorized purchases, report these as soon as possible. By acting quickly, you'll have a much better chance to prevent future unauthorized purchases, rectify the fraud, and, if necessary, receive reimbursement for purchases that you did not make.
- Review statements for any additional fraudulent charges and keep detailed records of any transactions that you did not make.
- Check if your homeowner's or renter's insurance covers any of your liability.
- Change your online passwords and PINs to prevent fraudsters from doing any further damage.
- Place a fraud alert on your credit with the three major credit bureaus to warn you of any suspicious activity.
- Request a freeze on your credit.
- Obtain a copy of your credit report. Often, signs of fraud—such as new accounts you don't recognize—will show up on credit card statements first, then on your credit reports. When you request a fraud alert, you will also get a copy of your credit report.

Missing or Stolen License

If your driver's license is lost or stolen, an identity thief has direct access to your full name, driver's license number, birth date, and other personal information. Follow these steps to help protect yourself from future fraudulent actions taken under your name:

- Report your license as lost or stolen to the Department of Motor Vehicles (DMV) and replace it. Read the DMV's guide to learn the specific steps you need to take for your state of residence.
- Read the DMV's list of five important steps when your license is lost or stolen.

Missing or Stolen Account Numbers

If your account numbers have been involved in a case of identity theft, take these steps to safeguard against fraud:

- Check with your financial institution or advisor regarding levels of restriction and other safeguards that are available for your accounts.
- In some situations, you may be able to change your account numbers altogether.

Identity Theft of a Deceased Person

Identity thieves can get personal information about deceased individuals by reading obituaries, stealing death certificates, or searching genealogy websites that sometimes provide death records from the Social Security Death Index. If the identity of a deceased relative or spouse is compromised, take the following actions to stop and prevent fraudulent activity:

- Send a copy of the death certificate to the IRS using the address where the deceased would have normally filed their paper tax return. You can also send a copy of the death certificate with the person's final tax return. Refer to the IRS's instructions on how survivors can file the final tax return on behalf of a deceased person.
- Send copies of the death certificate to each of the three major credit bureaus. They will guide you through the immediate steps to take and will most likely place a freeze on the deceased person's credit.
- Call the SSA at 800.772.1213 to inform them when someone dies. If a social security recipient has passed away, the SSA can lock their social security number to help prevent a thief from changing the address and bank account number where benefits are received.
- Notify all banks and financial institutions with which the deceased person held accounts about the identity theft. Ask these organizations about specific safeguards they can put in place.
- If you are a surviving spouse or the executor of the estate, you can request a copy of the deceased's credit report from all three major credit bureaus using a form provided by the Identity Theft Resource Center (ITRC). The reports can help alert you to fraud, and also inform you about active accounts that still need to be closed or pending collection accounts.

Identity Theft of a Minor

Some identity thieves target minors' identities because of their lack of credit history. If your child's identity is compromised in any way, take the following actions immediately:

- Inform the company's fraud department that someone opened a fraudulent account using your child's identity. Ask them to close the account and send you a letter confirming your child isn't liable. If needed, send a letter explaining your child is a minor who can't enter into contracts. Attach a copy of your child's birth certificate.
- Contact the three major credit bureaus to have them remove any fraudulent accounts from your child's credit report.
- Consider placing a credit freeze on your child's credit until the child is old enough to use it.
- Read the FTC's guide for more information about child identity theft.