CHECKLIST | IDENTITY THEFT RESPONSE

Presented by Highpoint Insurance Group

As criminals become increasingly sophisticated, it's crucial to be prepared for an identity theft incident. Such an incident takes place when someone utilizes your personal or financial information to receive benefits, file taxes, make purchases or commit other forms of fraud. In the event that you are the victim of an identity theft incident, you can help bolster your response efforts and mitigate potential damages by following the steps on this checklist.

Immediate Response Steps	COMPLETED
If possible, contact the companies where you know fraud took place and explain that someone has stolen your identity. Ask the companies to close or freeze your account(s) to prevent anyone from adding new charges without your permission.	☐
Change all login information, passwords and PINs for your accounts. Make sure this information is difficult to guess and isn't too similar to your old logins, passwords and PINs.	☐
Place a fraud alert by contacting one of the following three credit bureaus: • Experian • TransUnion • Equifax This practice will make it more difficult for someone to open new accounts in your name. Placing an alert is a free service—you will not be charged by any of the credit bureaus. Regardless of which credit bureau you use, each one will send you a letter to confirm that a fraud alert has been placed on your file.	☐
Be sure to secure your free credit report from any of the three bureaus. Once you receive your credit report, review it closely and take note of any fraudulent accounts or transactions.	☐
Report the incident to the Federal Trade Commission (FTC). Try to provide as many details as possible. Based on the information you provide, the FTC will help you create your identity theft report and recovery plan. Make sure you print and save this document immediately. Having this document is crucial because it guarantees you specific rights.	☐
Consider filing a report with your local police department. Be sure to provide the following information: • A copy of your identity theft report and recovery plan • A government-issued photo ID • Any documents that provide proof of your address (e.g., utility bills) • Any proof that you've gathered regarding the incident Don't forget to ask for a copy of the report.	☐

Mitigation Steps	COMPLETED
After reviewing your identity theft report and recovery plan, contact the fraud department of each company where a fraudulent account was opened or fraudulent transactions took place. When speaking with each company: • Inform them that someone stole your identity and created the fraudulent account or made the charges. Keep in mind that the company may request a copy of your identity theft report and recovery plan as evidence. • Have the company close the account and remove any fraudulent charges. Ask them to send you a letter to confirm that the account and charges aren't yours, you aren't liable for them and they've been removed from your credit report. Save this letter for use in case the account or charges appear on your credit report. • Keep note of which companies you contacted and when.	☐
Correct your credit report by writing a letter to each of the three credit bureaus. Be sure to include a copy of your identity theft report and recovery plan, as well as proof of your identity (e.g., a copy of your driver's license). Explain which information in your credit report is fraudulent and request that this information be removed. This practice—also known as blocking—will ensure that the information won't show up on your credit report and will prevent companies from collecting any fraudulent debt from you. If you have an identity theft report and recovery plan, the credit bureaus must honor your blocking request. Without this document, you can still have fraudulent information removed from your credit report—but it can take longer and the credit bureaus could deny your request.	☐
To prevent further misuse of your personal information, consider contacting one of the three credit bureaus for assistance in carrying out either of these precautions: • Using an extended fraud alert—This practice calls for companies to verify your identity before granting access to your credit report or issuing any new credit. Under federal law, this precaution is free for identity theft victims. An extended fraud alert lasts for seven years. • Implementing a credit freeze—This practice halts all access to your credit report until you lift or remove the freeze. The cost and availability of this precaution depend on applicable state laws.	☐
Apart from utilizing an extended fraud alert or credit freeze, consider reaching out to these additional organizations to be sure that the identity thief hasn't infiltrated your other accounts: • Consult the Internal Revenue Service to remedy any tax-related identity theft concerns. • Contact your health insurance company and medical care providers to ensure the identity thief hasn't used your information to receive health care services. • Consult the companies, programs, agencies or providers associated with any of your other accounts (e.g., utilities, government benefits, checking accounts, investment accounts, apartment or house rentals, and student loans) to detect and remedy any identity theft concerns. Keep note of which organizations you contacted and when.	☐

Additional Steps for Certain Situations	COMPLETED
If you think someone might be using your Social Security number for work purposes, be sure to contact your local Social Security Administration office. If your Social Security card is lost or stolen, click here to apply for a free replacement card.	☐
If your driver's license is lost or stolen, click here to locate your nearest motor vehicles office. From there, the state your license is from can flag your license number in case someone else tries to use it, and help you apply for a replacement license.	☐
If your passport is lost or stolen, contact the State Department. To replace your passport: • Schedule an appointment to apply in person at a Passport Agency or Center (only if you are traveling within the next two weeks). • Fill out Form DS-11 and DS-64 in person at an authorized Passport Acceptance Facility (if you are not traveling within the next two weeks).	☐
If a criminal uses your name or personal information when they are arrested, contact the law enforcement agency that arrested the criminal and file a report regarding the impersonation. Provide copies of your identifying documents to allow the law enforcement agency to compare your information to the criminal's. Have the law enforcement agency change all records from your name to the criminal's name and provide you with a "clearance letter" to document your innocence. Keep this letter with you at all times.	☐
If a court prosecutes a criminal using your name or personal information, contact the court where the arrest or conviction took place. Provide proof of your identity and ask the district attorney to help you clear your name in court records. Ask the court to provide you with a clearance letter to document your innocence. Keep this letter with you at all times.	☐
In any circumstance where a criminal uses your name or personal information, be sure to ask the law enforcement agency which information brokers buy their records. Contact these brokers to have any false information or convictions removed from your file.	☐
If a debt collector is trying to collect debts that you don't owe due to an identity theft incident, make sure you contact the debt collector within 30 days of receiving the collection letter. Tell the debt collector that someone stole your identity and the debt is not yours. Provide a copy of your identity theft report and recovery plan as evidence. Do the same for any companies with which the fraudulent account was opened, and ask the companies to stop reporting this debt to the credit bureaus. Ask the credit bureaus to block information about this debt from your credit report.	☐

Keep in mind that certain forms of identity theft may require additional response steps and considerations. For further guidance from the FTC on how to respond in these circumstances, click here.

Without adequate response measures in place, the consequences of an identity theft incident can be devastating—placing excess stress on you and your family, as well as wreaking havoc on your financial well-being. Taking these steps can make all the difference in limiting the impact of an incident. For more personal risk management guidance, contact us today.