

Combating Identity Theft — Client Checklist*

Organization	What to Do
Credit Agencies	<input type="checkbox"/> Report the identity theft to the fraud department of one of the following reporting agencies as soon as possible. They must notify the other two agencies. <ul style="list-style-type: none"> • Equifax: equifax.com • Experian: experian.com • TransUnion: transunion.com
	<input type="checkbox"/> Request a copy of your credit report and request that only the last four digits of your Social Security number be placed on the report.
	<input type="checkbox"/> Close accounts that you think have been compromised or opened fraudulently.
	<input type="checkbox"/> Inform the credit bureaus and the credit issuers (in writing) of any fraudulent accounts and incorrect information.
	<input type="checkbox"/> Obtain replacement credit cards with new, secure account numbers and destroy any old cards.
	<input type="checkbox"/> Notify those who have received your credit report in the last six months to alert them to any disputed, fraudulent or incorrect information.
	<input type="checkbox"/> Confirm that an extended fraud alert (seven years) is placed on your credit report.
Federal Trade Commission (FTC)	<input type="checkbox"/> Report the crime to the FTC to establish an Identity Theft Affidavit. Identity Theft Victim's Complaint and Affidavit .
Local Police	<input type="checkbox"/> Report the crime to your local police or sheriff's department. Make sure to prompt as much documented evidence as possible.
	<input type="checkbox"/> Verify that the report lists the fraudulent accounts and keep a copy of the report.
Internal Revenue Service (IRS)	<input type="checkbox"/> Contact the IRS to report the theft. This will alert them to any claim for refund or other activity on your account. File IRS Form 14039, Identify Theft Affidavit . <ul style="list-style-type: none"> • IRS Identity Protection Specialized Unit (IPSU): 800.908.4490 • Form 14039, Identity Theft Affidavit Contact your CPA with any questions.
State Tax Agency	<input type="checkbox"/> Contact your state tax agency to report the theft. Some agencies may require a police report and/or the IRS affidavit.
Other Agencies and Organizations	<input type="checkbox"/> U.S. mail fraud: Contact your local postal inspector. <ul style="list-style-type: none"> • Online: postalinspectors.uspis.gov • Phone: 800.275.8777
	<input type="checkbox"/> Social Security number misuse — non-IRS issues: <p>Check your earnings record to make sure no one is using your SSN to obtain work. Call your local Social Security Administration (SSA) office if something looks inaccurate.</p> <p>Contact the SSA Inspector General to report Social Security benefit fraud, employment fraud, or welfare fraud.</p> <ul style="list-style-type: none"> • Online reporting resources: <ul style="list-style-type: none"> - socialsecurity.gov/oig - Fraud Reporting Form • SSA fraud hotline: 800.269.0271



Health Insurance Provider

- Contact your health insurance company if your insurance card was accessed or stolen to help prevent the thief from using your insurance. Similarly, notify Medicare if your Medicare card was accessed or stolen.

Utilities and Brokers

- Contact your local utility providers (gas, electric, cable, Internet, cellular carrier, etc.) to ensure no new accounts are opened in your name. Similarly, let your investment or retirement account company know your identity documents were stolen so they will be alert to any suspicious activity on your account.

Debt Collectors

- Tell collectors that you are a victim of fraud and, therefore, not responsible for the account.
- Ask for the name of the collection company/the name of the person contacting you, the phone number and the address.
- Ask for the name and contact information for the referring credit issuer, the amount of the debt, account number and dates of the charges.
- Ask if the debt collector needs you to complete a specific fraud affidavit form or whether the FTC affidavit may be used.
- Follow up, in writing, with the debt collector and ensure that they confirm, in writing, that you do not owe the debt and that the account has been closed.

What Else Can You Do?

- Create an identity theft file (keep copies of everything).
- Change all your account passwords. As an extra step, consider changing your username.
- In all communications with the credit bureaus, refer to the unique number assigned to your credit report. When mailing information, use certified, return receipt. Be sure to save all credit reports as part of your fraud documentation file.
- Review your credit report periodically. An extended fraud alert allows you to obtain two free credit reports from each of the credit reporting agencies within 12 months.
- Consider requesting a security freeze. By [freezing your credit reports \(bit.ly/freezefile\)](https://www.fraud.ftc.gov/identity-theft/identity-theft101/protect-yourself/protect-yourself3.html), you can prevent issuers from accessing your credit files unless you give them permission. This prevents thieves from opening up new credit card and loan accounts.
- Consider requesting a criminal background check to ensure your identity is not being used in connection with criminal activities.

*This checklist provides you (our valued client) a structured plan to resolve identity theft issues. Use it to contact the applicable agency (or agencies) and report the fraud. Should you need assistance, please contact any of our Bank branch locations.

