Client identity theft checklist

Action steps for recovery

Identity theft is a complex and evolving threat, and one that costs U.S. citizens billions of dollars annually.

Without question, it is one of the most pressing challenges our country faces. Unfortunately, the problem is growing and fraudsters are always looking for new ways to steal confidential information to commit crimes. As your trusted adviser, we understand your concerns with identity theft and take every precaution to keep your personal information safe.

There are numerous types of identity theft. For example, a thief could steal a wallet and use credit cards to make illegal purchases or obtain information to file a tax return on behalf of a taxpayer to claim an illegal refund.

Should you ever find yourself a victim of any type of identity theft, the checklist on the next two pages will be your guide. It outlines specific steps you should take to help mitigate the damage of identity theft: closing credit cards, filing a police report, filing a complaint with the Federal Trade Commission, addressing matters with the IRS and more.

For tax-related identity theft matters, we are here to help. Assistance may involve contacting the IRS to make sure your payments are properly credited to your account, helping to retrieve a refund issued to the wrong person or responding to IRS notices. Feel free to call our office to discuss your situation and see how we can be of service.

Combating identity theft — client checklist*

Organization	What to do
Companies where you know fraud occurred	☐ Contact the fraud department of each company where the fraud occurred and explain that your identity was stolen. Ask them to freeze or close the account and not add any new charges unless you agree. ☐ Change your logins and passwords. *Note that you might have to contact these companies again after you have received your Identity Theft Report.
Credit agencies	☐ 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. • Equifax: equifax.com • Experian: experian.com • TransUnion: transunion.com ☐ Request a copy of your credit report and that only the last four digits of your Social Security number be placed on the report. ☐ Inform the credit bureaus and the credit issuers (in writing) of any fraudulent accounts and incorrect information. ☐ Obtain replacement credit cards with new, secure account numbers and destroy any old cards. ☐ Notify those who have received your credit report in the last six months to alert them to any disputed, fraudulent or incorrect information. ☐ Ask for a free, one-year fraud alert by contacting one of the three credit bureaus. That company must inform the other two. You will get a letter from each credit bureau that will confirm they placed a fraud alert on your file. ☐ Confirm that an extended fraud alert (seven years) is placed on your credit report.
Federal Trade Commission (FTC)	☐ Report the crime to the FTC. • Note that the FTC has overhauled the process for helping victims of identity theft. Go to identitytheft.gov to report identity theft. ☐ Based on the information you provide, identitytheft.gov will create your Identity Theft Report and recovery plan. ☐ Verify that the report lists the fraudulent accounts and keep a copy of the report.
Local police	☐ Report the crime to your local police or sheriff's department. Make sure to provide as much documented evidence as possible.
Internal Revenue Service (IRS)	☐ Contact the IRS to report tax-related identity theft. This will alert them to any claim for refund or other activity on your account. File IRS Form 14039, *Identify Theft Affidavit*. • IRS Identity Protection Specialized Unit (IPSU) can be reached at 800.908.4490. Contact your CPA with any questions. * Note: You should only file a Form 14039 after a data breach if your Social Security number was compromised and your e-file return was rejected as a duplicate OR if the IRS has informed you that you may be a victim of tax-related identity theft.

Combating identity theft — client checklist* (continued)

Organization	What to do
State tax agency	☐ 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	☐ U.S. mail fraud: contact your local postal inspector. • Online: postalinspectors.uspis.gov • Phone: 877.876.2455 ☐ Social Security number misuse — non-IRS issues: Check your earnings record to make sure no one is using your identification number to obtain work. Call your local Social Security Administration (SSA) office if something looks inaccurate. Contact the SSA Inspector General to report Social Security benefit fraud, employment fraud or welfare fraud. • Online reporting resources: – oig.ssa.gov – Fraud Reporting Form • SSA fraud hotline: 800.269.0271 • Apply for a replacement Social Security card if your card was lost or stolen. • If your driver's license was lost or stolen, contact the nearest DMV branch to report it. • If your passport was lost or stolen, call the State Department at 877.487.2778.
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 make sure no new accounts have been 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/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. ☐ Within 30 days of getting a collection letter, follow up, in writing with the debt collector and send them a copy of your Identity Theft Report. Make sure that they confirm, in writing, that you do not owe the debt and that the account has been closed.
Companies where you know fraud occurred	☐ Recontact the fraud department of each business where identity theft occurred. The business may request a copy of the Identity Theft Report. ☐ Close accounts that you think have been compromised or opened fraudulently. ☐ Ask the company to send you a letter confirming that the fraudulent account isn't yours and you are not liable for the charges. Keep a copy of this letter.

Combating identity theft — client checklist* (continued)

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 a 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, you can prevent issuers from accessing your credit files unless you give them permission. This prevents thieves from opening new credit card and loan accounts.
- Consider requesting a criminal background check to confirm your identity is not being used in connection with criminal activities.

* This checklist provides you (our valued client) with 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 our office. Our trained staff is available to help you resolve identity theft matters (including problems with the IRS) and proactively make sure your information is secure.

Contact information

Address	PAYAN & PAYAN CPAs
Phone number	7936 W Sahara Ave
Website	Las Vegas, NV 89117
	702-233-9526
	www.p2cpa.com

Identity Protection PIN Opt-In Program for Taxpayers

About the IP PIN

The Identity Protection Personal Identification Number (IP PIN) is a 6-digit number assigned to eligible taxpayers. It helps prevent identity thieves from filing fraudulent tax returns with stolen Social Security numbers (SSNs). An IP PIN helps the IRS verify taxpayers' identities and accept their electronic or paper tax returns for processing. The IRS issues IP PINs to confirmed identity theft victims once their cases are resolved. This process is unchanged. What is new for 2020 is the expanded number of taxpayers who are not IDT victims but who are eligible to opt into the IP PIN program. These taxpayers can opt-in by using the Get an IP PIN tool on IRS.gov.

Who is eligible for the IP PIN Opt-In Program?

IP PIN eligibility for taxpayers who want to opt into the program is expanding in phases. At the start of the 2020 filing season, you may opt into the program if you filed a federal return last year from Arizona, California, Colorado, Connecticut, Delaware, District of Columbia, Georgia, Florida, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, New York, North Carolina, Pennsylvania, Rhode Island, Texas and Washington. Additional locations will be eligible later in 2020.

About the IP PIN Opt-in Program

The IP PIN is a valuable tool against tax-related identity theft. Here's what you need to know before applying:

- You must pass a rigorous identity verification process.
- Only the online process is available. We are working on alternatives.
- Spouses and dependents are eligible for an IP PIN if they can pass the identity proofing process.
- An IP PIN is valid for a calendar year.
- You must obtain a new IP PIN each year.
- The IP PIN tool is unavailable mid-November through mid-January each year.
- Correct IP PINs must be entered on electronic and paper tax returns to avoid rejections and delays.

How to Get an IP PIN

Eligible taxpayers who want an IP PIN can go to www.irs.gov/ippin to access the Get an IP PIN tool. Taxpayers who do not already have an account, must register with the IRS.

Make sure you have all the necessary identity verification items:

- Email address
- Social Security Number (SSN) or Individual Tax Identification Number (ITIN)
- Tax filing status and mailing address
- One financial account number linked to your name:
  - Credit card – last 8 digits (no American Express, debit or corporate cards) or
  - Student loan or
  - Mortgage or home equity loan or
  - Home equity line of credit (HELOC) or
  - Auto loan
- Mobile phone linked to your name (for faster registration) or ability to receive an activation code by mail

See www.irs.gov/secureaccess for tips on how to successfully authenticate your identity. Once you are registered and able to access the Get an IP PIN tool, your six-digit number will be revealed to you.

IMPORTANT: The IRS will never email, text or call you to request your IP PIN. Do not reveal your IP PIN to anyone but your trusted tax software provider or tax preparer. Neither your provider nor preparer will ask for your IP PIN except to complete your tax return. Protect your IP PIN from theft, especially scams.

Publication 5367(EN-SP) (11-2019) Catalog Number 73362D Department of the Treasury **Internal Revenue Service** www.irs.gov