
SWC's
10 Point
Identity Theft
Recovery Action Plan

SWC's 10 Point Identity Theft Recovery Action Plan



SWC (Stees, Walker & Company, LLP)
16875 W. Bernardo Drive, Ste. 290 | San Diego, CA 92127
p: (858) 487-4580 | f: (858) 487-8033 | e: admin@swc.cpa | w: SWC.cpa

©2022 SWC (Stees, Walker & Company, LLP) | All rights reserved. | No portion of this booklet may be used without the express and written permission of SWC.

TABLE OF CONTENTS

Introduction: SWC's 10 Point Identity Theft Recovery Action Plan	3
Step 1: Don't Panic	7
Step 2: Contact All Organizations That May Be Impacted	9
Step 3: Contact the Consumer Credit Reporting Agencies	11
Step 4: File a Report with the Federal Trade Commission (FTC)	13
Step 5: File a Police Report	15
Step 6: Contact Your Health Insurance Providers (if applicable)	17
Step 7: Contact the Internal Revenue Service (IRS) (if applicable)	19
Step 8: Contact Any Relevant State Tax Agencies	21
Step 9: Contact Other Agencies or Organizations That May Be Able to Help	23
Step 10: Protect Your Identity	25



intro

Introduction

Despite huge advances in cyber security, identity and digital wallet theft is on the rise, and experts cite a perfect storm of circumstances as a major reason.

For one thing, more people are working from home, and they're working without the protections of corporate networks which are more reliable at blocking phishing schemes than home networks are. In addition, there are more transactions being handled online these days, including the electronic forwarding of unemployment checks and other government benefits.

Then there are the lingering fears about COVID that make some people vulnerable to online tactics dreamed up by nefarious hackers that enable them to steal your personal information and access your online accounts. And having more of your information stored in the cloud doesn't help matters in the least.

We've all heard the expression about "shutting the barn door after the horse has bolted." It's a folksy idiom that means it's too late to try and stop something that has already happened. It's a futile effort because, of course, the horse is history.

Unfortunately, even if you are being careful and doing all the right things to prevent identity theft, you can still fall victim to it. That's why it is so important to know how to recover when the unforeseeable and unavoidable happens to you.

Which is why we're pleased to share our *10 Point Identity Theft Recovery Action Plan*.

Rest assured that, as your trusted tax planning and financial strategy adviser, we take every precaution to safeguard your personal information, and we're here to help. If you've fallen victim to identity theft, call our offices to find out how we can be of service. We'll get your wayward steed back in the stall.

step 1

Step 1: Don't Panic

Fear increases your vulnerability to identity theft. Panic makes it worse. You're not legally liable for crimes that other people commit using the personal information they stole from you. So just scratch that concern off your list.

Likewise, if someone used your personal information to steal from you, you should be able to get your money back. For example, if a con artist filed a fraudulent tax return using *your* name and *their* address to steal *your* tax refund, the Internal Revenue Service (IRS) still owes you that refund.

Pro Tip: While you shouldn't panic, you should act with a sense of urgency. The faster you do all the right things, the less damage you're likely to suffer, and the greater the chances the perpetrator of the crime(s) will be caught and brought to justice.

Keep a detailed record of all the steps you take to curtail the damage, along with all the documentation you collect along the way. A written record will smooth the path to recovering any losses and protecting you from any losses that others (for example, your bank or creditors) may suffer as a result.

step 2

Step 2: Contact All Organizations That May Be Impacted

Although identity theft involves your personal information, it also impacts companies and organizations you do transactions with, so be sure to involve them in your recovery plan:

- Change your username and password for each compromised account.
- Report the incident to the fraud department of the organization where the fraud occurred. This may be your bank, a credit card company, your internet service or email provider, the IRS, your retirement plan administrator, your state unemployment office, the Social Security Administration, a bona fide debt collector, your electric or gas company ... you get the idea.
- Cancel or freeze any credit, debit, or bank accounts that may have been compromised, so that no new charges or transactions can be processed without your consent.
- Request a letter from each organization confirming that you're not liable for any fraudulent activity on your accounts.

Keep a list of all the organizations you contacted and let them know when you receive your Identity Theft Report from the Federal Trade Commission (FTC), as explained later in this document.

Warning: Beware of “me-to-me” scams involving instant digital money transfer platforms like Zelle and Venmo and your bank. Text messages from what appears to be your bank’s fraud department may be part of a sophisticated phishing scheme. Before replying, contact your bank to confirm that the message is legitimate.

step 3

Step 3: Contact the Consumer Credit Reporting Agencies

Equifax, Experian, TransUnion, and Innovis are four of the consumer credit reporting agencies that are equipped to help companies evaluate the credit risk of prospective borrowers. They can also be valuable allies in helping you recover from identity theft and credit fraud:

- Report the identity theft incident to one of the consumer credit reporting agencies, which will notify the other three:
 - Equifax at www.equifax.com
 - TransUnion at www.transunion.com
 - Experian at www.experian.com
 - Innovis at www.innovis.com
- Request a copy of your credit report and review it for any suspicious activities, such as accounts you don't recall having opened or addresses in places you never lived.
- Inform the credit agencies and any prospective creditors (in writing) of any fraudulent accounts and incorrect information.
- Ask one of the three credit reporting agencies to place a free, one-year fraud alert on your account. (Extended fraud alerts may also be available at a minimum cost.)

4

step

Step 4: File a Report with the Federal Trade Commission (FTC)

The FTC can help you recover from identity theft while tracking down the perpetrators. Here's what you need to do:

- Report the identity theft incident to the FTC at www.identitytheft.gov. Using the information you provide, the FTC will create your identity theft report and recovery plan.
- When you receive your report, review it to ensure that the information it contains is complete and accurate.
- Keep a copy of the report.

Clues someone may have stolen your identity and it's time to file a report with the FTC include the following:

- You notice withdrawals from your bank account that you cannot explain.
- You stop receiving mail or specific bills.
- Restaurants and retailers refuse your checks.
- You find unfamiliar accounts or charges on your credit report.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you never worked for.
- You receive a notice that your personal or account information was compromised by a data breach at a company where you do business or have an account.

step 5

Step 5: File a Police Report

Don't call 911. Identity theft is not considered an emergency.

To obtain additional documented evidence of the identity theft, report the incident to your local police department or sheriff's office.

In most areas, you can file a police report in person by:

- Visiting the nearest police precinct or sheriff's office in person
- By contacting your police precinct or sheriff's office by calling their non-emergency number.
- Search the web for your city and state followed by "police," or search for your county and state followed by "sheriff" for info about your local law enforcement agency, including its address, phone number, and website address.

Once your report is filed, contact the police department or sheriff's office to verify that it has been received and that everything was properly reported. Sadly, many crime reports are never followed up on because of a procedural error.

By contacting the police department or sheriff's office within eight hours of filing your report, you'll know if your information was properly submitted and if a case number has been assigned to your report.

Pro Tip: In some metro areas, you also may be able to file a police report online. Visit your police or sheriff's department website to see if filing online is right for you and your situation.

step 6

Step 6: Contact Your Health Insurance Providers (if applicable)

If your health insurance account (private insurance or Medicare or Medicaid) was compromised or you sense you're a victim of medical identity theft, notify your healthcare provider and your health insurance company to have your card/account number cancelled and obtain a new one.

With medical identity theft, someone uses your personal information (e.g., name, Social Security number, or health insurance account number) to see a doctor, obtain prescription medications, buy medical devices, or submit claims to your insurance provider. If the perpetrator's health information gets mixed in with yours, it could impact your medical care, health insurance benefits, or even your credit score and ability to qualify for a loan, lease, or job.

Pro Tip: After reporting the medical identity theft to your health insurance provider, ask for information about recent activity on your account, so that you can identify and dispute any unauthorized activity, such as bills for medical services you didn't receive.

To prevent medical identity theft, keep all medical information in a safe place, including the following:

- Health insurance cards
- Prescriptions and prescription bottles
- Billing statements from healthcare providers
- Benefit statements from your health insurance company

step

7

Step 7:

Contact the Internal Revenue Service (IRS) (if applicable)

If you're the victim of tax-related identity theft, get the IRS involved by doing the following:

- If you're one of our clients (or want to be), [contact us](#), as we can assist with connecting with the IRS.
- File IRS [Form 14039, Identify Theft Affidavit](#).
- Call the IRS Identity Protection Specialized Unit (IPSU) at (800) 908-4490.
- [Get an IP PIN](#) from the IRS if you don't already have one. An Identity Protection Personal Identification Number (IP PIN) is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number (TIN). It helps the IRS verify your identity when you file your electronic or paper tax return.


For more information, read [How to Get an Identity Protection Personal Identification Number from the IRS](#) on the SWC blog, or download the post in the form of an SWC Singlette from [Client Resources](#) on the SWC website.


step 8


Step 8: Contact Any Relevant State Tax Agencies

If you're a victim of tax-related identity theft, also contact relevant state tax authorities to report the incident. State authorities may require a copy of your police report or an IRS Identity Theft Affidavit (IRS Form 14039).

While each state's reporting requirements differ, in California, recent or potential *personal* tax-related identity theft may be reported by mail, phone, or fax. When making a report in California, use [Identity Theft Affidavit \(FTB Form No. 3552\)](#).

 **Mail**
Filing Compliance Bureau MS F151
Franchise Tax Board
PO Box 1468
Sacramento CA 95812-1468

 **Phone**
(916) 845-7088
Weekdays, 7 AM to 5 PM

 **Fax**
(916) 843-0561

If your *business* has been breached in California, report the following by email to ftbdatabreach@ftb.ca.gov:

- Reporting individual's name and title
- Name of business
- FEIN/SEIN
- Number of employees affected
- Nature of the data breach
- Contact information

step 9

Step 9: Contact Other Agencies or Organizations That May Be Able to Help

Depending on the nature of the identity theft and the means by which it was perpetrated, other agencies or organizations may be able to help, including these:

- **U.S. Postal Inspector:** If you have reason to believe that the U.S. Postal Service was used to perpetrate the identity theft or use your identity to commit other crimes via mail, you can file a report at www.uspis.gov/report or call (877) 876-2455.
- **Social Security Administration (SSA):** If you think someone may be using your Social Security number for work purposes (for example, to claim unemployment benefits), you can check your earnings report at www.ssa.gov/myaccount and file a fraud report at oig.ssa.gov/report or by calling the SSA fraud hotline at (800) 269-0271. If your SSN has been stolen and is still being used to commit fraud, the SSA can also help you obtain a new SSN.
- **Bureau / Department of Motor Vehicles (BMV/DMV):** If your driver's license was stolen or lost, contact your state's BMV or Department of Motor Vehicles to report it and obtain a replacement.
- **U.S. State Department:** If your passport was lost or stolen, call the State Department at (877) 487-2778.

step 10

Step 10: Protect Your Identity

Depending on the nature of the identity theft and the means by which it was perpetrated, other agencies or organizations may be able to help, including these:

- Use hard-to-guess account usernames and passwords.
- Change your account passwords at least once a year, or use a password-management program like [1Password](#), [LastPass](#), or [LogmeOnce](#).
- Store your passwords securely.
- Activate two-factor authentication for every online account that offers it. With two-factor authentication, you'll receive a code via email or mobile device to verify your identity as part of the logon process.
- Review your credit report periodically. You can obtain a free credit report from each consumer credit reporting agency annually. That's four free reports per year.
- Place a security freeze on your credit report with all three consumer credit reporting agencies. This prevents anyone from opening a new credit card or loan account in your name without your permission. It's a hassle having the freezes lifted whenever you apply for a new credit card or loan, but it's worth the inconvenience.
- Order a criminal background check on yourself to confirm that your identity isn't being used in connection with any criminal activities.

In a way, we are all victims of identity theft. So long as criminals are committed to spending their time and effort stealing from good people instead of earning an honest living, we take on the added burden of protecting ourselves and recovering when our self-defenses aren't enough to block their efforts.

What's important is that we work together. Thank you for doing your part to combat identity theft and report any incidents of it. By taking the time to read this plan and implement a few common-sense precautions, you've already done a great deal to prevent fraud and help the authorities lock down or lock up the perpetrators.

If you're one of our clients (or want to be), and you've fallen victim to identity theft (or are concerned about it), let us know what we can do to help you.



Disclaimer: The information in this 10 Point Identity Theft Recovery Action Plan is provided for general informational purposes only and may not reflect current financial thinking or practices. No information contained in this plan should be construed as financial advice from the staff at SWC (Steas, Walker & Company, LLP), nor is this the information contained in this plan intended to be a substitute for financial counsel on any subject matter or intended to take the place of hiring a Certified Public Accountant in your jurisdiction. No reader of this plan should act or refrain from acting on the basis of any information included in, or accessible through, this plan without seeking the appropriate financial planning advice on the particular facts and circumstances at issue from a licensed financial professional in the recipient's state, country or other appropriate licensing jurisdiction.

SWC (Steas, Walker & Company, LLP)
16875 W. Bernardo Drive, Ste. 290 | San Diego, CA 92127
p: (858) 487-4580 | f: (858) 487-8033 | e: admin@swc.cpa | w: SWC.cpa