

Identity Theft  
Victim

# IDENTITY THEFT RECOVERY GUIDE

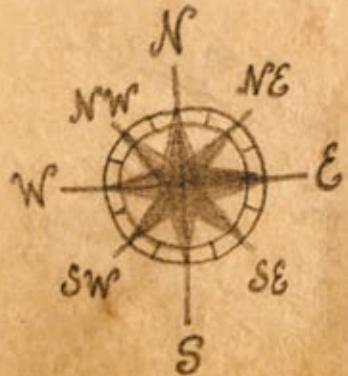
Reclaiming Your  
Treasured Data...  
AND YOUR LIFE

Secure  
Your Wealth

Stop Criminal  
Imposters

Clear  
Your Name

 Recovered  
Identity



**John Sileo**  
Identity Theft Expert

Copyright 2014 by John Sileo. All rights reserved.

Published by Da Vinci Publishing, Denver, Colorado.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, Da Vinci Publications 381 S. Broadway, Denver, Colorado 80209.

**Limit of Liability/Disclaimer of Warranty:** While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit, net worth, time or any other commercial or personal damages, including but not limited to special, incidental, consequential, or other damages.

# A Guide to “the Guide”

<b>Author’s Note: Everything Will Be Okay.....</b>	<b>5</b>
<b>Signs of Theft: How do I know I’m a victim?.....</b>	<b>6</b>
<b>Part 1: Immediate Lock-Down Steps.....</b>	<b>6</b>
1. Start an Identity Theft Recovery Log.....	8
2. Deactivate the Affected Accounts.....	8
3. Protect Your Financial Investments.....	9
4. Remotely Wipe Lost Mobile Devices.....	9
5. Change Critical Online Account Passwords.....	10
6. Place a Fraud Alert on Your Credit File.....	10
7. Contact your ATM, Bank Card and Debit Cards Issuers.....	10
8. File a Police Report Close to Home.....	12
9. File an ID Theft Victim’s Report with the FTC.....	12
10. Properly Alert Creditors about Fraud.....	13
11. Dispute Errors with Credit Reporting Companies.....	13
12. Dispute Fraudulent Charges on Your Existing Accounts.....	14
13. Monitor Credit/Debit Card, Bank, Investment & Financial Statements.....	15
14. Monitor Your Checking Accounts.....	15
15. Freeze Your Credit (or Extend Your Fraud Alerts).....	16
16. Consider Identity Theft Monitoring & Recovery Services.....	17
17. Implement Prevention Steps in Privacy Means Profit to Stop a Recurrence.....	17
<b>Part 2: Taking Recovery to the Next Level.....</b>	<b>18</b>
18. Notify the Postal Inspector.....	18
19. Contact Utility Companies.....	18
20. Contact the Social Security Administration.....	18
21. Contact the Passport Office.....	19
22. Secure your Phone Service.....	19
23. Protect your Driver’s License.....	19
24. Fight Bankruptcy Proceedings.....	19
25. Report Fraudulent Student Loans.....	19
26. Report Income Tax Fraud.....	20
27. File an Active Duty Alert (for Military Personnel).....	20
28. Report Medical Identity Theft.....	21
29. Contain Child Identity Theft.....	22
30. Fight Criminal Charges.....	23
31. Consider Hiring an Attorney.....	24

## **Part 3: Appendices & Further Resources**

Sample Letters & Forms.....	25
Appendix A: Identity Theft Recovery Log.....	27
Appendix B: Permanently Stopping Inquiries From Debt Collectors.....	29
Appendix C: Sample Dispute Letter for Existing Accounts.....	31
Appendix D: Sample Dispute Letter for New Accounts.....	33
Appendix E: Sample Dispute Letter to Credit Reporting Agency.....	35
Appendix F: Memo from FTC to Law Enforcement.....	37
Further Resources & Links.....	39

## **Author's Bio ..... 43**



## Author's Note: *Everything Will Be Okay*

**Right now, you might be experiencing a moment of panic.** Maybe your purse, wallet or smartphone is missing. Maybe there are charges on your credit card you don't recognize or money missing from your bank account. In more serious cases, you might have received a visit from law enforcement, a collection agency or the IRS. In the worst scenarios, you might be facing criminal charges (like I was), denial of medical treatment or notification of bankruptcy proceedings. You might feel lost without a map.

**The recovery task ahead isn't enjoyable or quick, but the calmer you remain, the fewer mistakes you will make** and the less collateral damage you will cause to your identity and financial health. Put your methodical, detail-oriented cap on for a few hours over each of the next few days and when it's over, you will be much safer and able to sleep again.

I know that becoming a victim of identity theft feels as violating as having an intruder in your home. It's creepy to have someone else abusing your personal space, even if it is virtual. The thought of someone financially posing as you, spending your net worth, committing crimes or having medical procedures in your name is enough to shake even the most courageous among us.

**I know because I am a two-time victim of identity theft.** The first time, a woman purchased a home in my name using my Social Security number. When she could no longer make payments (having drained my bank account in the process), she defaulted on the loan and started bankruptcy proceedings in my name. Recovery was a massive headache and took weeks away from my work and family.

In the second case, my friend and business partner used my banking login credentials to embezzle funds from our clients. In that case, I lost more than \$300,000 and two years in the recovery process, which included criminal cases, the death of my business and almost complete financial and personal destruction. If you are interested in the full story, or how to prevent it (believe me, you don't want to have to recover from this kind of ID theft) you can read about it in my second book, **Privacy Means Profit**, after you've completed your recovery.

By taking the right steps, in the right order, you will never have to experience what I did, never have to lose everything that my family lost.

It is my intention in the *Identity Theft Recovery Guide* to provide you with all possible steps you may need to take should your identity be stolen. However, there are so many possible scenarios that it is impossible to cover every recovery situation. Therefore I've broken this workbook into two sections: **Part 1: Immediate Lock-Down Steps** and **Part 2: Taking Recovery to the Next Level**. I've also provided you with helpful links where appropriate to access additional resources. There is no final word on ID theft recovery, so think of what you are about to start as an ongoing, dynamic process.

**With all my heart, I encourage you to not put off this process, but to take the steps outlined in this workbook as soon as possible.** I will be here with you along the entire journey. After all, together we are fighting for your identity, for your financial health and for everything that defines the very best of Who You Are.

John Sileo  
Identity Theft Expert & Keynote Speaker

The most important thing you can do right now is to take a deep breath,  
Slow down and proceed rationally.

*Everything will be okay.*

# SIGNS OF THEFT:

## How Do I Know I'm a Victim?

### Not sure that you are a victim?

Surprisingly, most cases of identity theft are discovered first by the victim, which reinforces the importance of monitoring your various accounts for suspicious behavior. Below are a few of the most common warning signs suggesting that you might be a victim of identity theft or data breach.

1. You receive a data breach notice in the mail from a company with which you do business explaining that your data has been compromised.
2. You've lost your purse, wallet, or mobile computing device.
3. Your bills or statements are not arriving in your mail (or email) on time.
4. You notice unauthorized charges on your credit card bill or debit card statement.
5. You lose control of your social media, email or financial accounts (you can't log in).
6. You notice new accounts or erroneous information on your credit report.
7. You are denied credit for a purchase or loan.
8. You receive credit card bills for cards you don't own.
9. You are contacted by a collection agency about an item you didn't purchase or a loan that isn't yours.
10. You receive bills for unknown purchases, rental agreements or services.

Even if you're uncertain about being a victim, taking the first few steps is wise and preventative. It's like taking an aspirin if you feel like you might be having a heart attack - no harm, no foul.

*"Most identity theft is first detected by the victim"*

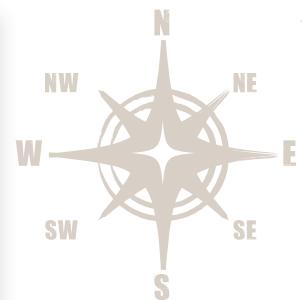
11. Businesses won't accept your check, debit or credit card.
12. You are unable to set up new banking, loan or brokerage accounts.
13. You notice withdrawals on your checking, savings or brokerage account that you didn't make.
14. The checks listed on your bank statements don't reconcile with those listed in your check register.  
Many times these checks are made out to "Cash."
15. You notice a downward trend in benefits on your annual Social Security Statement.
16. Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
17. The Internal Revenue Service (IRS) notifies you that more than one tax return was filed in your name, or that you have income from an employer for whom you don't work.
18. The police, collection agencies or district attorney's office show up at your home.
19. A subpoena to appear in court arrives on your doorstep.

Record the date, time and indicators  
that you are a victim in the space below:

DATE: \_\_\_\_\_

TIME: \_\_\_\_\_

INDICATORS:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



(This can be used to prove innocence in cases of fraud.)

# PART 1:

## Immediate Lock Down Steps

### 1. Start an Identity Theft Recovery Log

Over the next couple of weeks, tracking what you do is going to be important. As you take the following steps, you should keep a log of every step you have taken, with whom you spoke, the date and time of your conversation and the results of your call. This log of contacts will become part of your recovery dossier and will help you prove your financial, civil and criminal innocence, should they be questioned. I suggest that you take these steps mostly in order (if they are relevant to your case of ID theft), as several of the earlier steps become more difficult once you've completed the latter action items. I also recommend that you take the first seven steps within 24 hours of detection or potential theft to draw a virtual line in the sand that establishes a fraud "born on" date. This makes it easier to prove your innocence in regard to fraudulent transactions completed after that date. As you complete each step, check it off in this book or on the downloadable Master Checklist (if you purchased the complete Recovery System [www.IDRecoveryGuide.com](http://www.IDRecoveryGuide.com))

### 2. Deactivate the Affected Accounts

- The quickest way to minimize ID theft damage is to quickly deactivate any affected accounts – financial or otherwise. If there is a specific account involved that you feel has been violated, shut that account down first. For example, if your credit card has been stolen, alert that specific credit card company and deactivate the affected card. Some experts warn you not to cancel the card as it might make it more difficult to track the crime. From experience, your crime will never even be investigated, let alone solved, so protect yourself and proceed to the next step. If it is a bank or brokerage account, have them suspend all capabilities on the account until you notify them of next steps. For credit cards, under federal law, you are only responsible for a maximum of \$50 if you report the fraudulent charges immediately. Debit cards have higher liabilities and the money will be absent from your account while you prove that you didn't make the withdrawal.
- Eventually, you will want to obtain a new credit card number, account number, password on the account, etc. or potentially cancel the account all together. When you are speaking to the financial institution, explain to them that a thief has used your identity and ask them to suspend or close the account. You can also request more details about the unauthorized account or use of the account, since they will know more than you do.
- Request that they have any negative entries removed from your credit report. They may require you to send them an ID Theft Affidavit or other documentation (explained in a later step). Make sure you follow up with them and also submit this request in writing and keep a copy for your records.
- For compromised bank accounts, you will probably have to visit your local branch to cancel the old accounts and set up the new. Don't delay in getting this done as the bank only covers theft that is reported in a "reasonable" time.

To help you keep your conversations organized and make the recovery process easier, I have included a blank Identity Theft Recovery Log in Appendix A at the back of this workbook.

### 3. Protect Your Financial Investments

If an identity thief has tampered with your investments, retirement or brokerage accounts, contact your broker, account manager, and the U.S. Securities and Exchange Commission (SEC). Brokerage accounts are protected differently (and potentially more susceptible to permanent loss), so you don't want to waste time taking this step.

- Call your broker or account manager and describe the situation. Ask them to take all steps necessary to ensure the security of your account. Consider setting your account up with two-factor authentication (details in **Privacy Means Profit**).
- File an electronic complaint with the SEC in one of three ways: online at [www.sec.gov/complaint/tipscomplaint.shtml](http://www.sec.gov/complaint/tipscomplaint.shtml), a mailed complaint to: **SEC Office of Investor Education and Advocacy**, 100 F Street NE, Washington, DC 20549 or by phone: **(202) 942-8088**.

I get the fact that this recovery process is terribly inconvenient, and I know it's a strain on your time and patience. But think of it as an investment in your lifetime wealth. It won't just protect you and your family now, but also in the future.

### 4. Remotely Wipe Lost Mobile Devices

A lost or stolen smartphone, tablet or laptop is quite possibly the most dangerous repository of identity that you can lose, both in a personal and professional sense. Think about it; not only do mobile devices often contain sensitive contact information, passwords, banking logins, work materials and account numbers, they also give the thief the ability to imitate you on phone calls (with your caller ID) and emails (they can have your bank send a password reset to your email on the smartphone). Unfortunately, if you haven't already taken preventative steps to protect your mobile devices, there is very little you will be able to do to protect the data on your device. Learn more about passcodes, remote tracking and wiping and encryption in **Privacy Means Profit**.

- If you have enabled remote tracking and remote wiping capabilities on your device (see **Privacy Means Profit**), log into your remote monitoring software (Find My iPhone, Lookout, Symantec, etc.) and immediately send the wipe command so that all of your data is instantly removed from the device. If there was no passcode or password on the device, and the thief is data savvy, they will have removed all of your data within 30 minutes of stealing the phone.

#### Notes to Self:

---

---

---

---

---

There is nothing that strikes sweat-inducing panic like a missing smartphone. Don't beat yourself up, but once you've recovered, put that feeling of loss to work - let it motivate you to properly protect your replacement device so that it never happens again.

- If you are unable to remotely wipe (called bricking, because you turn the device into a useless brick), you will need to contact every financial or online account listed in your contact book (especially if they contain account numbers or passwords) and have them change your account information.
- Also, if you have no remote wiping capabilities, you should contact your phone carrier (AT&T, Verizon, T-Mobile, Sprint, Cricket, etc.) and alert them to the stolen device. Ask them if they have the capability to remotely wipe your device. Hopefully you have backed your data up or synced recently so that you can easily recover a copy of your valuable information.

## 5. Change Critical Online Account Passwords.

☐ Particularly if you have an electronic device stolen, or if you stored online accounts in the purse, wallet, travel bag or files that were taken, be sure to change passwords on all relevant online accounts. Because so much of our wealth is now accessible through the Internet, it is imperative to shut off this line of collateral damage. Even if these online credentials weren't compromised, changing your passwords regularly vastly increases your security. For tips on creating long, strong, varied and easily remembered passwords, or increasing your security using password protection software, consult the relevant chapter in **Privacy Means Profit**.

## 6. Place a Fraud Alert on Your Credit File.

A Fraud Alert requests that creditors contact you before issuing credit or opening new accounts in your name. If you file a Fraud Alert with one bureau, they are supposed to report it to the other two. However, this rarely happens, so play it safe and report it to each agency. Placing a Fraud Alert is only a temporary solution. You will likely be freezing your credit in an upcoming step, after you have cleared any errors or fraudulent accounts off of your credit report.

☐ Immediately place a Fraud Alert with all three credit-reporting bureaus.

### The 3 nationwide credit reporting companies

- > **Equifax**: 1-800-525-6285 or [www.equifax.com](http://www.equifax.com)
- > **Experian**: 1-888-397-3742 or [www.experian.com](http://www.experian.com)
- > **TransUnion**: 1-800-680-7289 or [www.transunion.com](http://www.transunion.com)



☐ Make sure to cover the following points with the credit bureau:

- o Let them know that your identity is being used by a criminal to fraudulently obtain credit in your name.
- o Ask them to place a Fraud Alert on your credit file. This is temporary and will last for 90-180 days only. Eventually, I recommend that you take the additional step of Freezing Your Credit (**see Step 15**).
- o Make sure that they include a victim's statement (if available) on your report such as "My identity has been stolen and used to fraudulently apply for credit. Please call me at [your phone number—cell phones are generally best because you carry them with you] to verify all applications."

☐ Verify with the bureau that you will be receiving a current copy of your credit report as well as instructions on how to file an extended multi-year Fraud Alert, should you want one. Review your credit file thoroughly to expose any fraudulent new accounts or existing account abuse.

☐ If the credit bureau won't forward a copy of your credit file, you have the right to get one anyway. To do this, visit [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com). By law, you can receive one free report from each of the three main credit-reporting agencies (Experian, Equifax and TransUnion), once per year. This is a primary source of detecting credit-related identity theft.

## **7. Contact your ATM and Debit Cards Issuer.**

As an identity theft victim, you have protections under federal law for ATM or debit card transactions. Federal law also limits your liability for the unauthorized electronic transfer of funds that result from identity theft.

It's best to act as soon as you discover a withdrawal or purchase you didn't make or authorize. Many card issuers have voluntarily agreed that an account holder will not owe more than \$50 for transactions made with a lost or stolen ATM or debit card. However, under the law, the amount you can lose depends on how quickly you report the loss\*.

### **Here are the steps to take:**

- Contact your ATM and debit card issuer and report the fraudulent transaction.  
Act as soon as you discover a withdrawal or purchase you didn't make.
  
- Have them issue a new ATM or debit card with an entirely new card number.
  
- Write a follow-up letter to confirm that you reported the problem.
  - Keep a copy of your letter.
  - Send it by certified mail and ask for a return receipt.
  - Request that they send a letter back acknowledging your submission.

### **\*How much you stand to lose by putting off reporting the loss or theft of your debit or ATM card:**

- If you report before any unauthorized charges are made: \$0
- If you report within 2 business days after you learn about the loss or theft: \$50
- If you report more than 2 business days after you learn about the loss or theft, but within 60 calendar days after your statement is sent to you: \$500
- If you report more than 60 calendar days after your statement is sent to you, ALL the money taken from your ATM/debit card account, and possibly more, could be lost. For example, you can be held liable for money residing in accounts linked to your debit card account, or overdraft protection loans.

In most cases, the financial institution has ten business days to investigate your report of a fraudulent transaction. They must tell you the results within three days of finishing the investigation and fix an error within one business day of finding it. In some cases, it can take 45 days to finish the investigation.

If you don't report loss on your debit card within 60 days of the day your institution sent you the account statement showing the unauthorized withdrawals, you could lose all the money the thief took from your account.

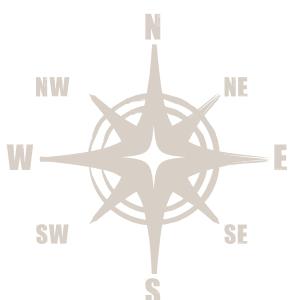
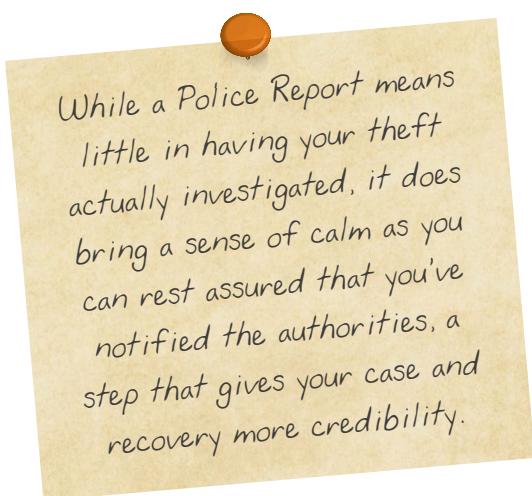
**Congratulations!** You have finished the first seven steps to recovering your identity and are much safer than you were when you began. The process isn't over, but it is quickly becoming less risky. Take a break if you need it, or power on if you love the feeling of accomplishment.

## **8. File a Police Report Close to Home.**

Immediately report the crime to your local police department. I suggest filing close to home so that you won't have to travel to a distant station should the report require follow up. The chances that they will investigate the crime are small, but you need a copy of the police report to begin proving your innocence to creditors and law enforcement agencies. Some law enforcement agencies see so much identity theft that they make filling out a report quite a chore for the victim. Stick with it until you have a legitimate report. Make sure that you bring/include the following items in your report:

- A copy of a government issued ID and proof of residency (utility bill).
- Any fraudulent account numbers that were established and any and all documented proof you have that the accounts are fraudulent.
- Any information that you have on the thief or the crime.

Get a copy of the report; you will need it repeatedly while straightening out credit and legal issues.



## **9. File an Identity Theft Victim's Report with the FTC.**

It is important that you file the proper governmental forms to prove that you have been a victim of identity theft. An FTC Identity Theft Report helps you deal with credit reporting companies, debt collectors, and businesses that opened accounts in your name. You can use the Report to:

- Get fraudulent and damaging information removed from your credit report
- Stop a company from collecting debts that result from identity theft, or from selling the debt to another company for collection
- Place an extended fraud alert on your credit report and minimize expenses
- Obtain information from companies about accounts the identity thief opened or abused

Visit [www.Consumer.gov/idtheft](http://www.Consumer.gov/idtheft) to file an FTC Identity Theft Report (commonly referred to as an Identity Theft Affidavit) and to verify that you have taken all of the steps suggested by the Federal Trade Commission. You will want to keep this Report nearby for the next several months, as you might be faxing, emailing or presenting it multiple times to help prove that you did not establish the accounts or make the charges in question.

## 10. Properly Alert Creditors about Fraud.

- You should immediately contact all creditors about accounts that have been set up fraudulently. For example, if the identity thief took out a home loan, call the loan agency and alert them to the problem. Request that they close the account or transfer it to a new account number immediately. They may ask for supporting documents such as your FTC Identity Theft Report and Police Report. If the thief set up phone or cable service, a new credit card or bank account or any type of financially-connected account, contact that provider immediately.
- If debt collectors contact you, respond immediately (within 30 days) in writing and keep a copy of your letter. Explain that you are the victim of identity theft and that you don't owe the money. You have the right to ask the debt collector for the name of the business that is owed the debt. Include your FTC Identity Theft Report and a copy of the Police Report with your letter. Find sample dispute letters for creditors in the appendices.
- Get copies of documents the identity thief used by contacting the business that has records of those transactions.
  - Ask for copies of documents the thief used to open new accounts or make purchases in your name.
  - Include details about where or when the fraudulent transactions took place.
  - When contacting the creditor, include a copy of your FTC Identity Theft Report or the proof the business requires, and proof of your identity.

The business must send you free copies of the records within 30 days of getting your request. You can get sample letters at [www.consumer.ftc.gov/articles/0281-sample-letters-and-forms-victims-identity-theft](http://www.consumer.ftc.gov/articles/0281-sample-letters-and-forms-victims-identity-theft). If you continue to have problems with debt collectors, see **Appendix B: How to Permanently Stop Calls and Letters from a Debt Collector**. Please also review **Step 12** at this time as you might be able to save yourself some time by taking two steps during a single phone call.



### WARNING

This particular step can be very frustrating, as it is difficult to reach an actual human with whom to file your complaints. However, this is a crucial phase of your recovery process, so don't give up! Your credit is what lets you buy a new home, lease a car and send your kids to college, so it's worth it!

## 11. Dispute Errors with Credit Reporting Companies.

**NOTE:** If you have difficulties contacting the credit reporting agencies or clearing up your credit profile, I strongly recommend signing up for an identity theft monitoring and recovery company that can help you with the process (more on identity theft services in a later step). Because they have direct lines of communication with Experian, Equifax and TransUnion, they will have an easier time of rectifying damage.

- In order to review your credit history, get a free copy of each of your three main credit reports (one from Equifax, Experian and TransUnion). You can do this either when filing a fraud alert (explained above) or by using the website [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com), which is run by the three bureaus.
  - Carefully review each credit report for accounts you don't recognize, amounts you don't owe or other peculiarities.

- If you find mistakes or accounts you don't understand when you review your credit reports, call, file online or send letters explaining the mistakes to:
  - **The 3 nationwide credit reporting companies**
    - > **Equifax**: 1-800-525-6285 or [www.equifax.com](http://www.equifax.com)
    - > **Experian**: 1-888-397-3742 or [www.experian.com](http://www.experian.com)
    - > **TransUnion**: 1-800-680-7289 or [www.transunion.com](http://www.transunion.com)
  - > The fraud department of each business that reported a fraudulent transaction on your existing accounts
  - > The fraud department of each business that reported a new account opened in your name by an identity thief

- Ask the credit reporting companies and affected businesses to block the disputed information from appearing on your credit reports. The credit reporting companies must block transactions and accounts if you can prove you are a victim of identity theft. Make sure you send supporting documents showing the errors, as well as your FTC Identity Theft Report and Police Report. The credit reporting company must investigate the items you send and forward that information to the business that reported the information to the credit reporting company.
- Make sure you receive a response from each credit reporting company. If your credit file changes because of the business' investigation, the credit reporting company must send you a letter with the results. If the credit reporting company puts the information back in your file, it must send you a letter explaining the actions it took.

## **12. Dispute Fraudulent Charges on Your Existing Accounts.**

It is important that you not only dispute errors on your credit report, but with all of the companies that the identity thief did business with in your name. While you are on the phone with the company (credit card provider, bank, utility provider, online account, phone company, etc.), make sure that you take these additional steps:

- Change the passwords or PINs for your account(s), as you never know what else the criminal has changed while pretending to be you.
- Ask each business if it will accept your FTC Identity Theft Report or if it uses special dispute forms. If you must use the business' forms, ask for blank forms that you can fill out.
- I recommend that you write to or email the fraud department of each business, as you then have a printed or electronic record of correspondence. This can be done through email or postal mail; just make sure you save a copy of any correspondence.
  - Use the address they specify for disputes.
  - Explain that you are an identity theft victim.
  - List the errors you found.
  - Send copies of documents that show the error.
  - Ask the business to remove fraudulent information.
  - Include a copy of your FTC Identity Theft Report (or the special dispute forms if the business requires them).
  - Include a copy of your credit report.

Make sure to black out any personal information on your forms that does not pertain to or is not necessary for your dispute.

- Ask the business to send you a letter confirming that it removed the fraudulent information.
- See **Appendix C: Sample Dispute Letter for Existing Accounts.**

### **13. Monitor Credit/Debit Card, Bank, Investment & Financial Statements Closely.**

Since you know that at least one financial account has been violated, make sure that you closely monitor all financial accounts for similar abuse. Many victims find that their identities are being used for multiple fraudulent purposes and catch the additional crimes by closely monitoring their statements.

I highly recommend setting up automatic account alerts with your banks, credit card companies and investment firms. Automatic alerts will email or text you any time a transaction is made on the account, an easy way to determine if someone else is spending your money. See **Privacy Means Profit** for details on this preventative measure.

Your newly-discovered habit of consistently monitoring accounts (especially if you monitor them electronically) will put you in the lowest risk group for future cases of severe identity theft.

### **14. Monitor Your Checking Accounts.**

An identity thief may steal your paper checks, misuse the account number from the bottom of your checks, or open a new account in your name. If this happens, contact your bank or financial institution and ask them to close the account immediately.

Federal law doesn't limit your losses if a thief forges your signature on your checks or uses your account number to buy something by phone, but most states hold banks responsible for losses from those fraudulent transactions. However, banks expect their customers to take reasonable care of their accounts.

Contact Check Verification Services:

- Contact your bank to place stop payments on all missing checks and close your account or obtain a new account number if needed.
- If your checks were stolen or new checking accounts were established in your name, call the check verification companies and report the fraudulent checks:
  - > **Certegy Check** 1-800-770-3792
  - > **ChexSystems** 1-800-428-9623
  - > **CrossCheck** 1-800-552-1900
  - > **Global Payments** 1-866-850-9061
  - > **National Check Fraud Service** 1-843-571-2143
  - > **Shared Check Authorization Network** 1-800-262-7771
  - > **TeleCheck** 1-800-366-2425

*Notes to Self:*

---

---

---

## 15. Freeze Your Credit (or Extend Your Fraud Alerts).

The best way to ensure that a thief cannot use your credit record anymore is to place a Security or Credit Freeze on your account with each of the major credit reporting agencies. A Credit Freeze places a password on your credit file, meaning that no one will have access to your information unless you share the password with him or her. Freezing your credit is free, though unfreezing it when you need to establish new credit sometimes requires a small fee (generally no more than \$10). **NOTE:** Take a moment to review **Step 16** regarding identity monitoring services right now. While it is less time-sensitive than a Credit Freeze, it is much simpler to complete **Step 16** prior to **Step 15** if you decide to invest in monitoring.

- Freeze your credit with all three credit-reporting agencies. Since all states don't allow you, by law, to freeze your credit, the three credit reporting bureaus have begun to offer credit freezes on a national basis. Use the following links, addresses or phone numbers to complete each freeze:

### Equifax Credit Freeze

[www.freeze.equifax.com/Freeze/jsp/SFF\\_PersonalIDInfo.jsp](http://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp)

P.O. Box 105788

Atlanta, Georgia 30348

Toll-Free: 1.800.685.1111

### TransUnion Credit Freeze

[www.transunion.com/personal-credit/credit-disputes/credit-freezes.page](http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page)

Fraud Victim Assistance Department

P.O. Box 6790

Fullerton, CA 92834

Toll-Free: 1.888.909.8872

### Experian Credit Freeze

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

P.O. Box 9554

Allen, TX 75013

Toll-Free: 1.888.397.3742

- If you do not wish to freeze your credit, I recommend that you extend your Fraud Alerts. After you receive your credit reports, follow the instructions from each bureau on how to extend the length of your fraud alert for a longer period of time. You will generally have to do this in writing, and may need to include supporting documentation such as your FTC Identity Theft Report or Police Report. Make sure you reference the unique ID number that the bureau assigns your case, and use Certified, Return-receipt mail when you send the requests. This is how you will know that they are processing your request and that action is being taken. Fraud alerts can be removed from your account at any time. Some of the items you should request in your written letters to each bureau are:

- Ask for the names and phone numbers of the credit grantors that were fraudulently established by the identity thief. This will save you time researching contact information.
- Request that bureaus remove inquiries on your account that are due to fraudulent activities.
- In some states, the bureaus are required to remove fraudulent accounts if you include a copy of the Police Report with your request. Ask them to do so if you live in one of these states.
- Ask the bureaus to notify any companies that have received your erroneous credit reports in the past few months to alert them to the disputed information.

Make sure that you wait until after you have resolved the identity theft issues to place a freeze on your credit because a freeze makes it more difficult for creditors to clean up the financial mess. A Credit Freeze can slow down (only by a few minutes) the process of applying for new credit in the future, but this minor inconvenience is well worth the peace of mind it will give you.

You've just taken probably the most significant step in minimizing this case of financial identity theft AND in preventing future cases of ID theft. A credit freeze is an incredibly powerful tool if used in the right manner.

- When you have been granted an extended alert, you are allowed two free copies of everything in your credit file over the first 12 months. Take advantage of the second report to make sure that you have cleared everything to your satisfaction.

Please be aware that these measures will not necessarily stop new fraudulent accounts from being established by the identity thief. Credit issuers (credit card companies, car dealers, lending companies, etc.) are not required by law to observe fraud alerts. Consequently, you should monitor your credit report from this point on with increased diligence to spot any suspicious activity. Additionally, the Credit Freeze discussed above will stop most new fraudulent accounts from being established.

## 16. Consider Identity Theft Monitoring & Recovery Services.

I highly recommend identity theft monitoring services for victims of identity theft, as it gives you an extra level of identity surveillance. Should the thief use your identity in additional ways, you have a far better chance of catching it early with monitoring services. To learn more about monitoring services, please visit [www.sileo.com/product-reviews/](http://www.sileo.com/product-reviews/). If you decide that identity monitoring is right for you, it is important to take this step. It is important that you take this step before you Freeze Your Credit, which can make the sign-up process more difficult. If you already have a reputable identity theft monitoring service, contact them immediately to help you resolve your case of identity theft. Most of the services include recovery services as part of their offering, which is one of the most valuable services they offer.

For those victims who want some additional peace of mind, I find identity theft monitoring services (the good ones) to be useful, especially in the first year after being victimized. You deserve a little extra protection and someone who has your back.

## 17. Prevent identity theft from happening to you again as outlined in *Privacy Means Profit* ([www.sileo.com/store/product/privacy-means-profit/](http://www.sileo.com/store/product/privacy-means-profit/)).

Recovery, by itself, is not enough. It is so important to protect all of the identity assets you have just recovered.

For the latest identity theft and privacy scams, visit [www.sileo.com/blog](http://www.sileo.com/blog), where we provide weekly updates on this and related topics.

You deserve a big pat on the back. You are now in the 1% of victims who take a highly proactive approach to recovering from this crime. No matter how bad you were hit, it's a fraction of what could have happened had you not made it to this point in the workbook.

At this point in your journey, you should glance through **Part 2: Taking Recovery to the Next Level**, to see if there are any additional steps you would like to (or need to) take.

## PART 2:

# Taking Recovery to the Next Level

The following action items are for victims of specific types of identity theft (e.g. medical) as well as for those victims who want to take extra steps to recover and protect their identities.

### 18. Notify the Postal Inspector.

If you feel that you are the victim of mail theft or a fraudulent change of address, contact the Postal Inspector's Office.

- Call the U.S. Post Office at 1-800-275-8777 or visit [postalinspectors.uspis.gov](#) to obtain your regional number. You should also consider getting a locking mailbox or P.O. box and drop off any sensitive outgoing mail to USPS collection boxes.

If you have made it this far in the workbook and are continuing, you deserve special recognition, as you are treating your identity and financial health with the respect they deserve. From one victim to another, thank you.

### 19. Contact Utility Companies.

An identity thief may use your personal and financial information to get telephone, cable, electric, water, or other services. Report fraudulent accounts to the service provider as soon as you discover them. Take the following steps to report fraudulent utility charges and accounts:

- Contact the utility or service provider and close the account that the identity thief opened.
- Contact your state Public Utility Commission for additional help. Search online at [www.naruc.org/Commissions/](#).
- Contact the Federal Communications Commission for help with cell phone or telephone services: 1-888-225-5322 or 1-888-835-5322 (TTY), Consumer & Governmental Affairs Bureau, 445 12th Street SW, Washington, DC 20554 or [www.fcc.gov/cgb](#)

Your retirement benefits could be worth hundreds of thousands of dollars over your retirement, so taking a few extra minutes to secure this piece of your identity is wise and worthwhile.

### 20. Contact the Social Security Administration.

- If your Social Security Number has been stolen and is being used to commit benefits or unemployment fraud, contact the SSA. You report fraud to their hotline at 1-800-772-1213 or 1-800-325-0778 (TTY) or visit their website at [www.SSA.gov](#).
- You can also visit your local Social Security Office for a replacement card if necessary. While you are there, ask them about any additional steps they would have you take in response to a stolen Social Security card. I strongly suggest that you closely monitor your Social Security benefits statements, as you would hate to have your retirement benefits drained when you begin cashing them out.

## **21. Contact the Passport Office.**

- Whether you have a passport or not, alert the passport office to warn them about fraudulent passport applications in your name. They can be reached at [www.travel.state.gov/passport/passport\\_1738.html](http://www.travel.state.gov/passport/passport_1738.html)

## **22. Secure your Phone Service.**

- Call your phone companies (landline and mobile phone) and ask them to password protect your account. It is advisable to follow this same step with every company with which you have financial transactions. By placing a call-in or phone password on the account, it makes it more difficult for a criminal to impersonate you and gain access.

## **23. Protect your Driver's License.**

- If someone is using your driver's license number to write bad checks, contact your state's Department of Motor Vehicles to see if another license has been issued in your name. Have them place a fraud alert on your license if possible. If not, ask them the procedure in your state for filing a complaint. You can find your local office at [www.OnlineDMV.com](http://www.OnlineDMV.com).

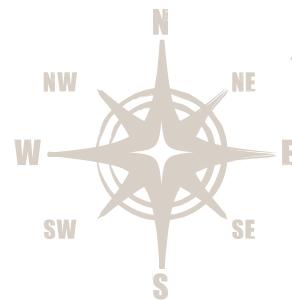
## **24. Prevent Bankruptcy Issues.**

- If you believe someone filed for bankruptcy in your name, contact the U.S. Trustee in the region where the bankruptcy was filed. The U.S. Trustee Program refers cases of suspected bankruptcy fraud to the United States. Write to the U.S. Trustee in the region where the bankruptcy was filed.
  - Find regional offices at [www.usdoj.gov/ust](http://www.usdoj.gov/ust) or in the Blue Pages of the phone book under U.S. Government Bankruptcy Administration.
  - Consider hiring an attorney who can explain to the court that the bankruptcy filing was fraudulent.

## **25. Report Fraudulent Student Loans.**

- Contact the U.S. Department of Education using one of the means below:

- 1-800-647-8733
- U.S. Department of Education, Office of the Inspector General, 1400 Maryland Avenue SW, Washington, DC 20202
- [www2.ed.gov/about/offices/list/oig/misused/index.html](http://www2.ed.gov/about/offices/list/oig/misused/index.html)



## **26. Report Income Tax Fraud.**

If someone uses your Social Security number to get a job, the employer will report the person's earnings to the Internal Revenue Service (IRS) as if they were YOUR earnings. When you file your tax return, you won't include those earnings. But, IRS records will show you failed to report all your income, and you can expect to get a letter from the IRS.

If someone uses your Social Security number and files a tax return in your name before you file, they may get your refund. When you file your own return later, IRS records will show the first filing and refund, and you'll get a letter from the IRS.

If you think someone has misused your Social Security number to get a job or tax refund – or the IRS sends you a notice indicating a problem – contact the IRS immediately. Specialists will work with you to protect your account.

- Contact the Internal Revenue Service at: IRS Identity Protection Specialized Unit 1-800-908-4490 or [www.irs.gov/identitytheft](http://www.irs.gov/identitytheft).
- Report the fraud and ask for the IRS ID Theft Affidavit Form 14039.
- Send a copy of your Police Report or an IRS Identity Theft Affidavit Form 14039 and proof of your identity, such as a copy of your Social Security card, driver's license or passport. Anytime you are sending your SSN, make sure to use Certified Mail, Return Receipt Requested.

## **27. File an Active Duty Alert (for Military Personnel).**

Military personnel have additional protections. If you're deployed, you can place an active duty alert on your credit reports to help minimize the risk of identity theft while you're away.

- Contact all three credit reporting companies as explained earlier in this workbook and:
  - Request an active duty alert.
  - Provide proof of identity, such as a government-issued identity card, driver's license, military identification, birth certificate, or passport.
  - Ask the credit reporting companies to take your name off their marketing list for pre-screened credit card offers for two years, unless you ask them to add you back onto the list.
- Mark your calendar.
  - Active duty alerts last for one year. If your deployment lasts longer, renew the alert.

*Notes to Self:*

---

---

---

---

---

---

## 28. Report Medical Identity Theft

If an identity thief gets medical treatment using your name, the thief's medical information – for example, blood type, test results, allergies, or illnesses – can get into your medical file and have adverse affects on your health. Information about the thief can be added to your medical, health insurance, and payment records. In addition, thieves can quickly drain your medical benefits, leaving you with nothing the next time you need medical attention.

- If you suspect an identity thief has used your medical information, get copies of your medical records. Under federal law, you have a right to know what's in your medical files. Contact each doctor, clinic, hospital, pharmacy, laboratory, health plan, and anywhere you believe the thief has used your information, and let them know what has happened. Contact each of your health care providers and ask for copies of your medical records.
- Visit [www.healthit.gov/bluebutton](http://www.healthit.gov/bluebutton) for details on obtaining your records.
- Complete the request form and pay any fees required to get copies of your records. If your provider refuses to give you copies of your records because it thinks that would violate the identity thief's privacy rights, you can appeal. Contact the person the provider lists in its Notice of Privacy Practices, the patient representative, or the ombudsman. Explain the situation and ask for your file. If the provider refuses to provide your records within 30 days of your written request, you may complain to the U.S. Department of Health and Human Services Office for Civil Rights at [www.hhs.gov/ocr](http://www.hhs.gov/ocr).

When obtaining your medical records, I recommend that you don't mention possible identity theft, as this can complicate the process due to HIPAA regulations. You can always notify your medical provider of fraud at a later time.

Review your medical records and report any errors to your health care provider.

- Write to your health care provider to report mistakes in your medical records.
- Include a copy of the medical record showing the mistake.
- Explain why this is a mistake and how to correct it.
- Include a copy of your Police Report or Identity Theft Report.
- Send the letter by Certified Mail and ask for a return receipt.

Your health care provider should respond to your letter within 30 days. It must fix the mistake and notify other health care providers who may have the same mistake in their records.

Notify your health insurer and all three credit-reporting companies.

- Send copies of your Police Report or FTC Identity Theft Report to your health insurer's fraud department and the three nationwide credit reporting companies.

## 29. Contain Child Identity Theft

Child identity theft happens when someone uses a child's personal information to commit fraud. A thief may steal and use a child's information to get a job, government benefits, medical care, utilities, car loans, or even a mortgage. Avoiding, discovering, and recovering from child identity theft involves some unique challenges.

Parents and guardians don't expect a minor child to have a credit file and rarely request or review their child's credit report. A thief who steals a child's information may use it for many years before the crime is discovered. The victim may learn about the theft years later, when applying for a job, loan, or apartment, or when a business reviews the credit file and finds fraudulent accounts.

By helping your child recover from or prevent identity theft, you are making a significant investment in their future.

It could make a difference worth hundreds of thousands of dollars over their lifetime. Feel good about the time you are spending on this step.

A parent or guardian can check whether a minor child has a credit report if they think the child's information is at risk, perhaps because the child's Social Security card was lost, a school or business leaked the child's personal information to the public, or bill collectors or government agencies contact the child about accounts the child didn't open. To get a minor child's credit report, a parent or guardian must contact the credit reporting companies and provide proof of identity and other documents.

### How to Find Out if a Child Has a Credit Report

Contact each of the three nationwide credit-reporting companies and ask for a manual search of the child's file.

- Email **TransUnion**: [childidtheft@transunion.com](mailto:childidtheft@transunion.com).
- Call **Experian** (1-888-397-3742)
- Call **Equifax** (1-800-525-6285)

The companies will check for files relating to the child's name and Social Security number, and for files related only to the child's Social Security number. The credit reporting companies may require copies of:

- Your child's birth certificate listing parents
- Your child's Social Security card
- The parent or guardian's government-issued identification card, like a driver's license or military identification or copies of documents proving the adult is the child's legal guardian
- Proof of address, like a utility bill, or credit card or insurance statement

### How to Help a Child Victim of Identity Theft

If you find out that someone has misused your child's personal information, follow these steps (many of which mirror the steps for adults discussed earlier in the workbook):

Contact each of the 3 nationwide credit-reporting agencies.

- Send a letter asking the companies to remove all accounts, inquiries and collection notices associated with the child's name or personal information.
- Explain that the child is a minor and include a copy of the Uniform Minor's Status Declaration. Go to [www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0095-uniform-minor-status-declaration.pdf](http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0095-uniform-minor-status-declaration.pdf)

- Place a fraud alert on their credit profile, if one exists.
- Learn about your rights. The credit reporting company will explain that you can get a free credit report, and other rights you have.
- Consider requesting a credit freeze if your child has an active credit report. The credit reporting companies may ask for proof of the child's and parent's identity.
- Order the child's credit report.
- Contact businesses where the child's information was misused.
- Create an FTC Identity Theft Report.

## 30. Fight Criminal Violations

### How to Clear Your Name of Criminal Charges

If an identity thief uses your name, date of birth, Social Security number, or other personal information during an investigation or arrest, the information will be added to your state's criminal database. The information also may be added to a national criminal database.

- If you learn who the thief is, ask the criminal records database manager(s) to change the "key name" in the database to the thief's name so that the records will show the thief's name instead of yours.
- Contact the agency that made the arrest, the court that convicted the identity thief, and your state Attorney General's office to get documents that will help you show your innocence.
  - File a report about the impersonation.
  - Give copies of your fingerprints, photograph, and identifying documents.
  - Ask the law enforcement agency to:
    - Compare your information to the imposter's
    - Change all records from your name to the imposter's name
    - Give you a "Clearance Letter" or "Certificate of Release" to declare your innocence
- Keep the "Clearance Letter" or "Certificate of Release" with you at all times.

### Important Things to Remember:

---

---

---

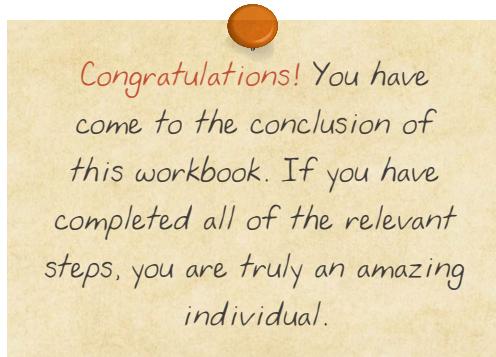
---

## What to do if a Court Prosecuted a Case Against a Thief Who Used Your Name

- Contact the court where the arrest or conviction happened.
  - Ask the District Attorney for records to help you clear your name in court records.
  - Provide proof of your identity.
  - Ask the court for a "Certificate of Clearance" that declares you are innocent.
- Keep the "Certificate of Clearance" with you at all times.
- Contact your state Attorney General.
  - Find your state Attorney General's office at [www.naag.org](http://www.naag.org).
  - Ask if your state has an "identity theft passport" or some kind of special help for identity theft victims.
- If you obtain an *Identity Theft Passport*, keep it with you at all times.
- Consider hiring a criminal defense lawyer.
  - Your state Bar Association or Legal Services provider can help you find a lawyer. See contact info at the back of the workbook.
- Contact information brokers.
  - Information brokers buy criminal records and create criminal records files to sell to employers and debt collectors.
  - Ask the law enforcement agency that arrested the thief for the names of information brokers who buy their records.
  - Write to the brokers and ask them to remove errors from your file.

### 31. Consider Hiring an Attorney.

Certain recovery situations will be beyond your control or capabilities. In these cases, I highly recommend investing in a competent attorney to aid in your recovery. I personally spent more than \$12,000 on lawyer fees (I know, it seems high!), but that investment probably saved me at least that much and quite possibly kept me out of jail. Ask your close friends or co-workers if they have lawyers that they would recommend.



Just because you've reached this advanced stage of recovery, don't get complacent about protecting your identity against a recurrence. Take every step you can find to protect the valuable data that makes up your identity. And if you discovered steps along the way that you wished were part of the workbook, or if a phone number or website has changed, please let us know. Some of our very best information comes from victims like you who contribute to the ever-changing contents of this Guide. **We would love your feedback! Visit us at [Sileo.com](http://Sileo.com).**

## PART 3:

# Appendices & Further Resources

### Sample Letters and Forms

**Appendix A:** Identity Theft Recovery Log

**Appendix B:** Permanently Stopping Inquiries From Debt Collectors

**Appendix C:** Sample Dispute Letter for Existing Accounts

**Appendix D:** Sample Dispute Letter for New Accounts

**Appendix E:** Sample Dispute Letter to Credit Reporting Agency

**Appendix F:** Memo from FTC to Law Enforcement

For more sample letters and forms, see [www.consumer.ftc.gov/articles/0281-sample-letters-and-forms-victims-identity-theft](http://www.consumer.ftc.gov/articles/0281-sample-letters-and-forms-victims-identity-theft).



## Appendix A

# Identity Theft Recovery Log

Remember that you should keep a log of every step you have taken, names of anyone with whom you have spoken, the date and time of your conversation and the results of your call. This log of contacts will become part of your dossier and will help you prove your financial, civil and criminal innocence, should they be questioned. I suggest that you take these steps in order, as several of the steps become more difficult once your credit is frozen. The first seven steps should be taken within 24 hours of the theft or potential theft.



## Appendix B

### How to Permanently Stop Calls and Letters from a Debt Collector

By law, credit-reporting agencies must block identity theft-related information from appearing on a victim's credit report. They must block unauthorized transactions, accounts, and inquiries. To get unauthorized information blocked, you must give information to the credit reporting companies.

Write a letter to the debt collector and tell them to stop contacting you about the debt. After the debt collector gets the letter, it can't contact you again, except once – to say it won't contact you again, or that it plans to take specific action. Sending this letter should stop calls and letters from the collector, but it doesn't prevent the debt collector from suing you to collect the debt.

#### To stop collection action, follow these steps:

- Write to each credit reporting company.
  - Send a copy of your FTC Identity Theft Report.
  - Include proof of your identity including your name, address, and Social Security number.
  - Explain which information on your report resulted from identity theft and that the information didn't come from a transaction you made or approved.
  - Ask the company to block the fraudulent information.

You can get sample letters at [www.consumer.ftc.gov/articles/0281-sample-letters-and-forms-victims-identity-theft](http://www.consumer.ftc.gov/articles/0281-sample-letters-and-forms-victims-identity-theft).

If the credit reporting company accepts your FTC Identity Theft Report, it must block the fraudulent information from your credit report within 4 business days after accepting your Report, and tell the business that sent the fraudulent information about the block.

If the credit reporting company rejects your FTC Identity Theft Report, it can take 5 days to ask you for more proof of the identity theft. It has 15 more days to work with you to get the information, and 5 days to review information you sent. It may reject any information you send after 15 days. It must tell you if it won't block information. You can re-submit the Report.

After a business has been notified about a block of fraudulent information, it must:

- Stop reporting that information to all the credit reporting companies.
- Not sell or transfer a debt for collection.



## Appendix C

### Sample Dispute Letter for Existing Accounts

[Date]  
[Your Name]  
[Your Address][  
[Your City, State, Zip Code]

[Name of Company]  
[Fraud Department or Billing Inquiries]  
[Address]  
[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am writing to dispute [a] fraudulent charge[s] on my account in the amount[s] of \$\_\_\_\_\_, and posted on [dates]. I am a victim of identity theft, and I did not make [this/these] charge[s]. I request that you remove the fraudulent charge[s] and any related finance charge and other charges from my account, send me an updated and accurate statement, and close the account (if applicable). I also request that you stop reporting this inaccurate information and report the correct information to all of the nationwide credit reporting companies (CRCs) to which you provided it.

Enclosed is a copy of my FTC Identity Theft Report, credit report, and account statement showing the fraudulent items related to your company that are the result of identity theft. Also enclosed is a copy of the Notice to Furnishers of Information issued by the Federal Trade Commission, which details your responsibilities under the Fair Credit Reporting Act as an information furnisher to CRCs.

Please investigate this matter and send me a written explanation of your findings and actions.

Sincerely,

[Your Name]

Enclosures:

FTC Identity Theft Report  
Proof of Identity  
FTC Notice to Furnishers of Information  
Copy of account statement showing fraudulent items



## Appendix D

### Sample Dispute Letter for New Accounts

[Date]  
[Your Name]  
[Your Address]  
[Your City, State, Zip Code]

[Name of Company]  
[Fraud Department or Billing Inquiries]  
[Address]  
[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am a victim of identity theft. I recently learned that my personal information was used to open an account at your company. I did not open or authorize this account, and I therefore request that it be closed immediately. I also request that [Company Name] absolve me of all charges on the account, and that you take all appropriate steps to remove information about this account from my credit files.

Enclosed is a copy of my FTC Identity Theft Report, and a copy of my credit report showing the fraudulent items related to your company that are the result of identity theft. Also enclosed is a copy of the Federal Trade Commission Notice to Furnishers of Information, which details your responsibilities as an information furnisher to credit reporting companies (CRCs). As a furnisher, upon receipt of a consumer's written request that encloses an FTC Identity Theft Report, you are required to cease furnishing the information resulting from identity theft to any credit reporting company.

The Notice also specifies your responsibilities when you receive notice from a CRC, under section 605B of the Fair Credit Reporting Act, that information you provided to the CRC may be the result of identity theft. Those responsibilities include ceasing to provide the inaccurate information to any CRC and ensuring that you do not attempt to sell or transfer the fraudulent debts to another party for collection.

Please investigate this matter, close the account and absolve me of all charges, take the steps required under the Fair Credit Reporting Act, and send me a letter explaining your findings and actions.

Sincerely,

[Your Name]

Enclosures:

FTC Identity Theft Report  
FTC Notice to Furnishers of Information  
Credit report of [Your Name] identifying information to be corrected



## Appendix E

### Sample Dispute Letter for Credit Reporting Company

[Date]  
[Your Name]  
[Your Address]  
[Your City, State, Zip Code]

[Credit Reporting Company Name and Address]

Write a separate letter to each of the 3 companies. See contact info on inside back cover.

Dear Sir or Madam:

I am a victim of identity theft and I write to dispute certain information in my file resulting from the crime. I have circled the items I dispute on the attached copy of my credit report. The items I am disputing do not relate to any transactions that I made or authorized. Please remove or correct this information at the earliest possible time.

I dispute the [name of source, like "Company" or "Court"] [name of item, like "account" or "judgment"] because [explain why the item is inaccurate]. As required by section 611 of the Fair Credit Reporting Act, a copy of which is enclosed, I am requesting that the item[s] be removed [or request another specific change] to correct the information.

[If possible: I have enclosed copies of documents that support my dispute.]

Please investigate and correct the disputed item[s] as soon as possible.

Sincerely,

[Your Name]

Enclosures:

FTC Identity Theft Report

Credit report of [Your Name] identifying information to be corrected

FCRA Section 611



## Appendix F

### Memo from FTC to Law Enforcement

**To:** Law Enforcement Officer

**From:** Division of Privacy and Identity Protection - The Federal Trade Commission

**Re:** Importance of Identity Theft Report

The purpose of this memorandum is to explain what an “Identity Theft Report” is, and its importance to identity theft victims in helping them to recover. A police report that contains specific details of an identity theft is considered an “Identity Theft Report” under section 605B of the Fair Credit Reporting Act (FCRA), and it entitles an identity theft victim to certain important protections that can help him or her recover more quickly from identity theft.

Specifically, under sections 605B, 615(f) and 623(a)(6) of the FCRA, an Identity Theft Report can be used to permanently block fraudulent information that results from identity theft, such as accounts or addresses, from appearing on a victim’s credit report. It will also make sure these debts do not reappear on the credit reports. Identity Theft Reports can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. An Identity Theft Report is also needed to allow an identity theft victim to place an extended fraud alert on his or her credit report.

In order for a police report to be incorporated in an Identity Theft Report, and therefore entitle an identity theft victim to the protections discussed above, the police report must contain details about the accounts and inaccurate information that resulted from the identity theft. We advise victims to bring a printed copy of their ID Theft Complaint filed with the FTC with them to the police station in order to better assist you in creating a detailed police report so that these victims can access the important protections available to them if they have an Identity Theft Report. The victim should sign the ID Theft Complaint in your presence. If possible, you should attach or incorporate the ID Theft Complaint into the police report, and sign the “Law Enforcement Report Information” section of the FTC’s ID Theft Complaint. In addition, please provide the identity theft victim with a copy of the Identity Theft Report (the police report with the victim’s ID Theft Complaint attached or incorporated) to permit the victim to dispute the fraudulent accounts and debts created by the identity thief.

For additional information on Identity Theft Reports or identity theft, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).



# Additional Resources

## **CREDIT REPORTING COMPANIES**

### **Equifax**

[www.equifax.com](http://www.equifax.com) 1-800-525-6285

### **Experian**

[www.experian.com](http://www.experian.com) 1-888-397-3742

### **TransUnion**

[www.transunion.com](http://www.transunion.com) 1-800-680-7289

## **FEDERAL GOVERNMENT**

### **Federal Communications Commission**

For help with telephone service: [www.fcc.gov/cgb](http://www.fcc.gov/cgb)  
1-888-225-5322  
1-888-835-5322 (TTY)

### **Federal Financial Institutions Examination Council**

To locate the agency that regulates a bank or credit union:  
[www.ffiec.gov/consumercenter](http://www.ffiec.gov/consumercenter)

### **Federal Trade Commission**

To report identity theft: [www.ftc.gov/complaint](http://www.ftc.gov/complaint)  
1-877-438-4338  
1-866-653-4261 (TTY)

### **Internal Revenue Service**

Identity Protection Specialized Unit  
To report identity theft: [www.irs.gov/identitytheft](http://www.irs.gov/identitytheft)  
1-800-908-4490

### **Legal Services Programs**

To locate a legal services provider: [www.lsc.gov/local-programs/program-profiles](http://www.lsc.gov/local-programs/program-profiles)

### **Social Security Administration**

To report fraud: go to [www.socialsecurity.gov](http://www.socialsecurity.gov) and type "Fraud" in the Search box.  
1-800-269-0271  
1-866-501-2101 (TTY)

### **U.S. Department of Education**

To report fraud:  
[www.ed.gov/about/offices/list/oig/hotline.html](http://www.ed.gov/about/offices/list/oig/hotline.html)

Or go to [www.ed.gov](http://www.ed.gov) and type "OIG Hotline" in the Search box.  
1-800-647-8733

### **U.S. Department of Justice**

To report suspected bankruptcy fraud:  
[www.justice.gov/ust/eo/fraud](http://www.justice.gov/ust/eo/fraud)  
Or send email to [USTP.Bankruptcy.Fraud@usdoj.gov](mailto:USTP.Bankruptcy.Fraud@usdoj.gov)

### **U.S. Postal Inspection Service**

To file a complaint: [postalinspectors.uspis.gov/contactUs/filecomplaint.aspx](http://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx)  
1-877-876-2455

### **U.S. Postal Service**

To place a hold on mail: [www.usps.com/holdmail](http://www.usps.com/holdmail)  
To locate a post office: [www.usps.com](http://www.usps.com)  
1-800-275-8777

### **U.S. Securities and Exchange Commission**

To report fraud:  
[www.sec.gov/complaint/tipscomplaint.shtml](http://www.sec.gov/complaint/tipscomplaint.shtml)  
1-800-732-0330

### **U.S. Department of State**

To report a lost or stolen passport: [www.travel.state.gov/passport/passport\\_1738.html](http://www.travel.state.gov/passport/passport_1738.html)  
1-877-487-2778  
1-888-874-7793 (TDD/TTY)

Ask each company for the email or postal mail address for sending dispute or blocking requests.



## Other

### American Bar Association

To locate state and local bar associations:

[www.americanbar.org/groups/bar\\_services/resources/state\\_local\\_bar\\_associations.html](http://www.americanbar.org/groups/bar_services/resources/state_local_bar_associations.html)

### Free Annual Credit Reports

To order a free annual credit report:

[www.annualcreditreport.com](http://www.annualcreditreport.com)

1-877-322-8228

### Certegy

To ask about a declined check:

[www.askcertegy.com](http://www.askcertegy.com)

1-800-437-5120

### ChexSystems, Inc.

To report checking accounts opened in your name:

[www.consumerdebit.com](http://www.consumerdebit.com)

1-800-428-9623

### National Association of Attorneys General

To find a State Attorney General:

[www.naag.org](http://www.naag.org)

1-202-326-6000 (Not a toll-free number)

### National Association of Regulatory Utility Commissioners

To get contact information for a state utility commission:

[www.naruc.org/commissions](http://www.naruc.org/commissions)

1-202-898-2200 (Not a toll-free number)

### Opt Out

To opt out of prescreened offers of credit or insurance:

[www.optoutprescreen.com](http://www.optoutprescreen.com)

1-888-567-8688

### TeleCheck Services, Inc.

To report check fraud:

[www.firstdata.com/telecheck](http://www.firstdata.com/telecheck)

1-800-710-9898



# John Sileo, Keynote Speaker

## Technology • Identity • Privacy • Security



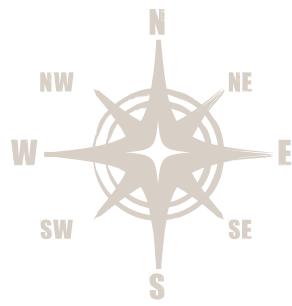
John Sileo's identity was stolen from his business and used to **embezzle \$300,000** dollars from his clients. While the thief covered his crimes using Sileo's identity, John and his business were held legally and financially responsible for the felonies committed. The **breach destroyed John's company** and consumed two years of his life as he fought to stay out of jail.

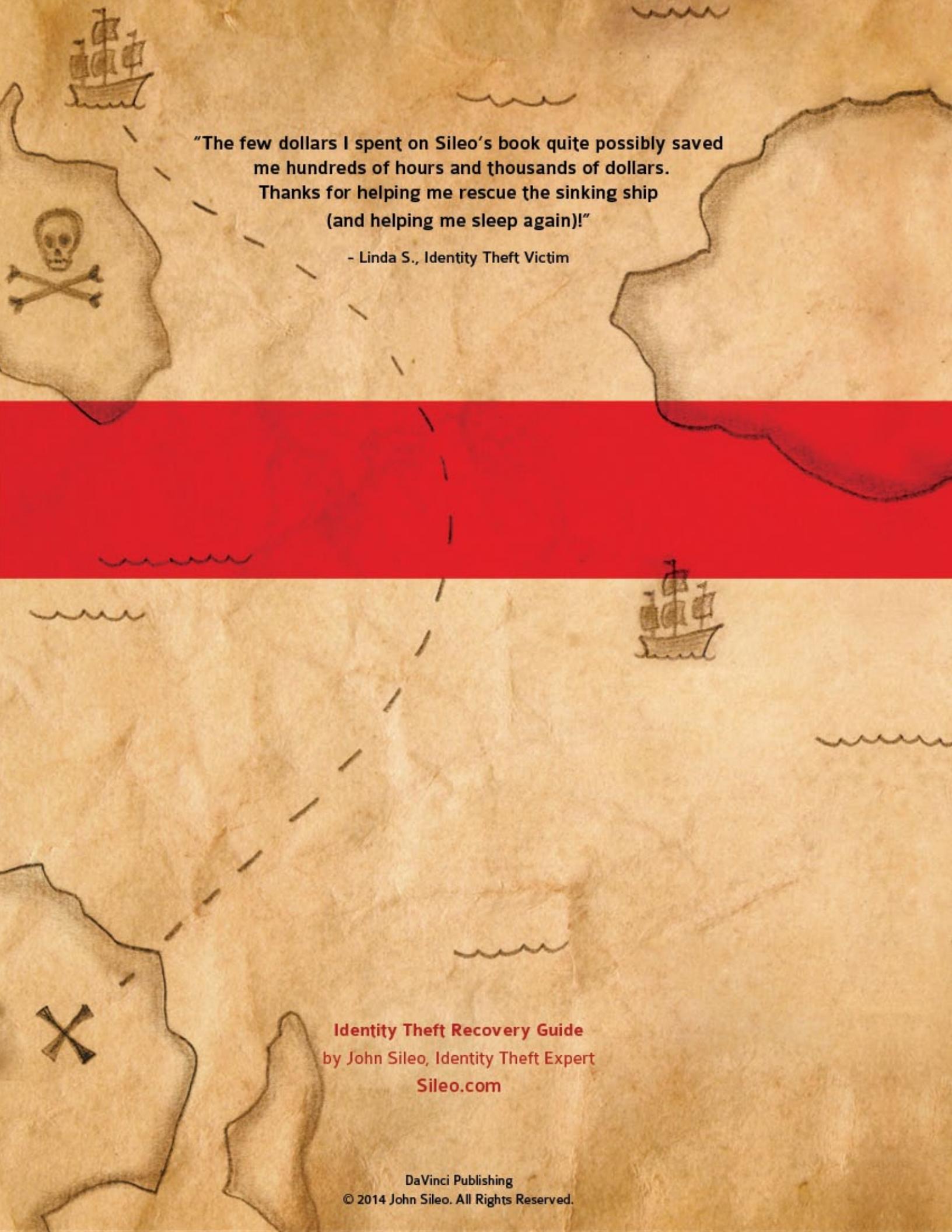
In response, John made it his mission to help others protect the private data that represents their wealth. Now America's leading keynote speaker on privacy, identity and technology protection, **John specializes in making security fun and engaging for audiences so that it works**. John's most requested topics include identity theft prevention, online privacy, social media exposure, mobile technology, social engineering and cyber security.

John is the **award-winning author** of many books including **Privacy Means Profit** (Wiley), and has recently appeared on **Rachael Ray, 60 Minutes**, Anderson Cooper and Fox Business.

John's **satisfied clients** include the Department of Defense, Visa, Blue Cross Blue Shield, Homeland Security, University of Massachusetts, the FDIC, Pfizer, NASBA, the Federal Trade Commission, Lincoln Financial, Northrop Grumman, AARP, the Federal Reserve Bank and scores of corporations, universities, and associations of all sizes.

John is **CEO of The Sileo Group**, a privacy think tank that helps organizations protect the privacy that drives their profits. He graduated from **Harvard University** with honors and spends his free time snowshoeing the Rocky Mountains with his remarkable wife and two highly-spirited daughters.





**"The few dollars I spent on Sileo's book quite possibly saved  
me hundreds of hours and thousands of dollars.  
Thanks for helping me rescue the sinking ship  
(and helping me sleep again)!"**

- Linda S., Identity Theft Victim

**Identity Theft Recovery Guide**  
by John Sileo, Identity Theft Expert  
[Sileo.com](http://Sileo.com)