7 Steps to Preventing **Identity Theft**

John Sileo

Protecting your personal identity doesn't need to be difficult. But it does take a bit of effort to minimize your digital footprint. The following action items are among the first you should take to protect yourself and your family. From there, we can go into greater detail on protecting the smartphones, laptops and Internet accounts that are increasingly being targeted.

Summary of ID Theft Protection Action Items

1. **Opt out** of financial junk mail by registering at www.OptOutPreScreen.com.
2. **Shred** any paper documents that would go in the trash with a durable and safe confetti document shredder.
3. **Freeze** your credit with Experian, Equifax, and TransUnion.
4. **Use** Identity Monitoring to track your data.
5. **Lock** your identity documents in a bolted-down, fire-resistant document safe.
6. **Protect** your computer with security software, a firewall, secure Wi-Fi, encryption and strong passwords.
7. **Track** your credit report 3 times per year for FREE at www.AnnualCreditReport.com.

For further tools, purchase a copy of Privacy Means Profit.

1 **Opt out** of financial junk mail by registering at www.OptOutPreScreen.com.

?

Your private data is bought and sold by junk-mailers without your knowledge.

!

Opt out by calling 1-888-567-8688 or visiting www.OptOutPreScreen.com.

There are complete industries built around collecting, massaging and selling your data – your name, phone number, address, spending patterns, net worth, the age of your children, the magazines you buy, etc. Companies buy bits of your privacy so that they can knowledgeably market products to you that you are likely to purchase.

To minimize the amount of your personal information bought and sold on the data market, begin "opting out". Opting out is the process of notifying organizations that collect your personal information to stop sharing it with other organizations. "Pre-Approved" credit card offers (i.e., financial junk mail) are a major source of identity theft. Those mailers give thieves an easy way to set up credit card accounts in your name without your consent. They spend money on the card and default on the balance, leaving you with the mess of proving that you didn't make the purchases. The solution is to opt out of receiving pre-approved credit, home loan and insurance offers.

Pre-approved credit offers (also called pre-screened or pre-qualified credit offers) are possible because credit reporting bureaus (Experian, Equifax and Trans Union – companies that collect and sell financial data on nearly every American) make a great deal of money selling your identity (i.e., name, address, phone number, age, credit score) to credit card, loan and insurance companies. But it is your right to stop the sale of your information. To opt out of pre-approved credit offers with the three main credit reporting bureaus, call 1-888-567-8688 or visit www.OptOutPreScreen.com. There is no cost to you for opting out.

Once you've completed this step, begin opting out of ALL information sharing on every account you have (bank, brokerage, mortgage, utilities, phone, etc.) as well as with the Direct Marketing Association.

2 **Shred** any paper documents that would go in the trash with a durable and safe confetti document shredder.

? We throw away private information every day. This is where dumpster divers begin.

! Buy a high-quality document shredder.

Assume that any document you throw out will end up in the hands of an identity thief. Get in the habit of either chopping or locking documents and disks that contain identity (name, phone number, address, social security number, account numbers, passwords, PIN numbers, phone numbers, client information, children's' information, etc.).

When buying a paper shredder, I recommend the following features:

- Cross-cut confetti shredding
- 10+ pages of simultaneous feeding capacity
- Allows shredding of stapled documents, credit cards and CDs

The shredders I like best are made by Fellowes. I like Fellowes because of their SafeSense technology, which turns the shredder off if your fingers (or your kids' fingers) get too close to the shredding device. This adds a great deal of peace-of-mind to an already effective product. They also have anti-jamming technology that makes them less frustrating than other brands and they don't seem to break down as frequently. Convenience is key! Make sure you place a confetti shredder next to ALL of the places that you handle identity (where you open your mail, your home office, your desk at work) and shred everything possible. Don't skimp here – if you don't make it convenient for yourself and your employees, it won't get done. If a document has identity of any sort on it, shred it, even if it isn't your information. Don't forget to destroy digital files as well, like those that live on a hard disk when you donate your computer. If you can't shred it, lock it up in a fire-safe (see below).

3 **Freeze** your credit with Experian, Equifax, and TransUnion.

?

If a thief gains access to your credit file, they can spend everything you're worth.

!

Freeze your credit with Experian, Equifax, and TransUnion.

Every time you establish new credit (e.g., open up a new credit card, store account or bank account, finance a car or home loan, etc.), an entry is created in your credit file, which is maintained by companies like Experian, Equifax and TransUnion. The trouble is, with your name, address and social security number, an identity thief can pretend to be you and can establish credit (i.e., spend your net worth) in your name.

A credit freeze is simply an agreement you make with the three main credit reporting bureaus (Experian, Equifax and TransUnion) that they won't allow new accounts (credit card, banking, brokerage, loans, rental agreements, etc.) to be attached to your name/social security number unless you contact the credit bureau, give them a password and allow them to unfreeze or thaw your account for a short period of time. Yes, freezing your credit takes a bit of time (maybe an hour of work), can be a little inconvenient when you want to set up a new account) and it can cost a few dollars (generally about $10 to unfreeze, a small price compared to the recovery costs of identity theft). And it is worth it! It's like putting locks on your doors.

Don't let anyone talk you out of freezing your credit. It is the number one thing you can do to prevent credit fraud. To learn more about freezing your credit, visit the three credit bureau credit-freeze sites here: Experian, Equifax, and TransUnion.

4 **Use** Identity Monitoring to track your data.

? Your private information is floating around on the Internet and exposing you to risk.

! Monitor your online identity conveniently with sophisticated identity surveillance.

When my audiences learn that only about 25% of identity theft can be caught by monitoring their credit report, they often ask me to evaluate the more sophisticated identity theft monitoring and protection services in the market place. Not all identity monitoring services are created equal. I recommend an identity surveillance service that monitors the following aspects of your identity:

- 24/7 monitoring of your credit file (most services provide only this - nothing more)
- Non-credit loans (pay-day loans, etc)
- Government records
- Public records disclosure (court cases, real estate transactions, etc.)
- Nation-wide criminal databases
- Cyber-trafficking of your private information over the internet
- The better services will also offer recovery services and identity theft insurance

I choose a particular identity theft monitoring company because of the quality and volume of monitoring they provide, the convenience of their service, and the safety of their data centers. Here's how it works. Rather than waste hours monitoring all of the potential sources of identity theft myself, the product does it for me, automatically. Every month, a report shows up in my email inbox letting me know if there are any areas that I should be concerned about. That way, I only have to think about it when necessary. Again, convenience is crucial – if we make it easy to be safe, we will be safe! You should expect to spend approximately $200 per year for a good service (far less than you probably spend to insure your car and home, which are worth far less than your identity).

5 **Lock** your identity documents in a bolted-down, fire-resistant document safe.

?

Identity documents that are left unlocked in our homes and offices open up profitable opportunities for identity thieves.

!

Purchase a fire-resistant document safe to securely store all of your identity documents.

A majority of our most valuable identity documents (passports, birth and death certificates, wills, trusts, deeds, brokerage information, passwords, health records, customer data, employee records, etc.) are exposed to identity theft (and natural disasters, such as fire and floods) as they sit in unlocked filing cabinets, bankers boxes, office drawers or out in the open, on our desks. To complicate matters, the problem of data theft goes beyond paper documents to digital media. More than ever we need to be concerned with the physical protection of hard drives, cell phones, thumb drives, CDs and DVDs with sensitive personal or business data on them.

To store them securely, purchase a fire-resistant safe. Think of it this way. Your identity is probably worth something close to $300,000 (even if your credit is poor), not to mention the value of any business data for which you are responsible (customer records, employee information, intellectual capital). Spending a few hundred dollars to lock up the keys to your identity is simple. Look for a fire safe that meets these requirements:

- Able to withstand 1500° F for 30 minutes
- Lockable by key or combination
- Able to be secured to the foundation of your home (to prevent safe theft)
- Preferably waterproof (where there's fire, there's water)

I recommend fire-resistant stackable filing cabinets because they are nearly indestructible, inexpensive and protect your data from both fires and theft. They also allow you to expand your storage capacity as you protect more and more of your identity.

One important note: increasingly, thieves are breaking into homes and businesses in order to steal identity documents. By placing them all in a central location (such as a fire safe), you are making it easier for them to steal everything at once. I suggest that you have your fire safe bolted into the foundation of your home or business. This small expense could save you hundreds of thousands of dollars. It's no more expensive than putting dead-bolt locks on your doors.

6 **Protect** your computer with security software, a firewall, secure Wi-Fi, encryption and strong passwords.

? The information stored on your computer can be compromised if left unprotected.

! Follow the 7 Steps to a System Lock-down listed below.

In order to protect all of the identity documents stored on our home and work computers, it is important to close all of the potential data leaks. The following suggestions will get you started, but please hire a computer security professionally to help you protect this very valuable asset in the fight against identity theft.

1. Create strong, alphanumeric passwords. Read your copy of Privacy Means Profit for further details.
2. Employ a highly-rated security software suite on every computer you own. It should include: anti-virus and anti-spyware scanners; password protection, phishing and pharming filters and a firewall.
3. Configure your Windows systems for automatic security updates. Apple computers do this by default.
4. Utilize encryption software (for professional-level protection). Encryption is more complicated than I can explain in a bullet-point, so please read for details in *Privacy Means Profit*.
5. Physically lock-down your computers (especially if you use a laptop or hand-held). Desktop computers and workstations should be locked in your office, both at work and at home. More private data disappears because of stolen laptops, tablets and mobile phones than any other source.
6. Secure your wireless network. Make sure that the connection is not open to anyone with a wireless device and that you use WPA2 encryption or better, NOT WEP. For additional security, enable SSID Masking, MAC-specific addressing and VPN tunneling (see PMP for more details).
7. Secure your Mobile Data Devices (iPhones, Androids, BlackBerrys, Thumb Drives, Laptop Computers) using all of the tools above. Just because they are small doesn't mean that the data on them isn't worth a mint.

7 **Track** your credit report 3 times per year for FREE at www.AnnualCreditReport.com.

?

Scammers can be using your credit and you don't even know it.

!

Monitor your credit report for free, 3 times per year at AnnualCreditReport.com.

A credit report records a history of how you repay money you borrow from others. When an identity thief or credit fraudster uses your Social Security number to set up new credit accounts, you will never know it… unless you actively monitor your credit bureau accounts. By law, you are entitled to a free report every year from each of the three credit reporting agencies, Equifax, Experian and TransUnion. Details on how to read your report and detect and rectify fraud can be found in *Privacy Means Profit*.

Naturally, these steps will get you started down the road to protecting yourself from identity theft and cyber fraud. But there are many more suggestions than the ones above to continue protecting your identity. For a detailed plan of action, consult your copy of *Privacy Means Profit* or visit my blog at www.Sileo.com. To bring me in to speak to your group about identity theft, cyber security, online privacy or social engineering, contact me directly on 303.777.3221.

John Sileo's identity was stolen from his business and used to **embezzle almost a half-million 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 corporation** and consumed two years of his life as he fought to stay out of jail. But John chose to fight back and speak out.

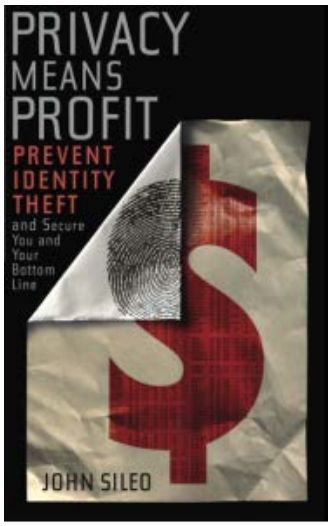
Emerging from this crisis, John became America's leading professional speaker on information survival, including **identity theft prevention**, data breach, cyber security, human manipulation and social media exposure. John is the **award-winning author** of *Stolen Lives, The Facebook Safety Survival Guide* and *Privacy Means Profit* (Wiley), and has recently appeared on ***60 Minutes*** and *Fox and Friends*, for which he is a regular contributor.

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

For further tools, purchase your copy of Privacy Means Profit

This book builds a bridge between good personal privacy habits (protect your wallet, online banking, trash, etc.) with the skills and motivation to protect workplace data (bulletproof your laptop, server, hiring policies, etc.).

In *Privacy Means Profit*, John Sileo demonstrates how to keep data theft from destroying your bottom line, both personally and professionally. In addition to sharing his gripping tale of losing $300,000 and his business to data breach, John writes about the risks posed by social media, travel theft, workplace identity theft, and how to keep it from happening to you and your business.



Your Price: **$20**
Regularly: ~~$24.95~~

Available at **Sileo.com/store**