Why You Should Get Security Freezes Before Your Information is Stolen

Tips To Protect Yourself Against Identity Theft & Financial Fraud

MASSPIRG Education Fund

Why You Should Get Security Freezes
BEFORE
Your Information is Stolen

MASSPIRG Education Fund

Mike Litt and Edmund Mierzwinski

October 2015

Acknowledgements

MASSPIRG Education Fund sincerely thanks Beth Givens, Director at Privacy Rights Clearinghouse; Paul Stephens, Director of Policy and Advocacy at Privacy Rights Clearinghouse; and Susan Grant, Director of Consumer Protection and Privacy at the Consumer Federation of America for their review of drafts of this document, as well as for their insights and suggestions.

MASSPIRG Education Fund thanks the Digital Trust Foundation and the In Re Netflix Fund for support of privacy education efforts.

The authors bear responsibility for any factual errors. The recommendations are those of MASSPIRG Education Fund. The views expressed in this report are those of the authors and do not necessarily reflect the views of our funders or those who provided review.

With public debate around important issues often dominated by special interests pursuing their own narrow agendas, MASSPIRG Education Fund offers an independent voice that works on behalf of the public interest. MASSPIRG Education Fund, a 501(c)(3) organization, works to protect consumers and promote good government. We investigate problems, craft solutions, educate the public, and offer Bay Staters meaningful opportunities for civic participation. On the web at masspirgedfund.org.

Contents

Summary

A never ending stream of news reports about data breaches – including T-Mobile, Target Corporation, the IRS, numerous Blue Cross Blue Shield and other health plans, the University of Maryland, and the U.S. Office of Personnel Management (OPM) - is a constant reminder that you're at risk of a data breach and therefore, identity theft if you:

- Shop with credit or debit cards;
- Pay taxes;
- Have health insurance;
- Attend college;
- Patronize any business that keeps customer records; or,
- Work for the government or a company

These constant breaches reveal what's wrong with data security and data breach response. Agencies and companies hold too much information for too long and don't protect it adequately. Then, they might wait months or even years before informing victims. Then, they make things worse by offering weak, short-term help such as credit monitoring services.

The first defense against any kind of identity theft is to be vigilant about protecting your personal information by taking steps like creating secure passwords, installing anti-virus and anti-malware software, and shredding personal documents. (See Appendix A for more tips on protecting your personal information.) **However, if and when someone does steal enough of your information to commit identity theft, there is really only one type that you can stop before it happens: New account identity theft, where someone opens a new account in your name.** All other types of identity theft and fraud, at best, can only be detected after the fact. Unfortunately, the services and steps that are most offered and recommended to consumers are the ones that only detect identity theft or fraud but don't stop it.

Peace of Mind

Whether your personal information has been stolen or not, **your best protection against someone opening new credit accounts in your name is the security freeze (also known as the credit freeze), not the often-offered, under-achieving credit monitoring.** Paid credit monitoring services in particular are not necessary because federal law requires each of the three major credit bureaus to provide a free credit report every year to all customers who request one. You can use those free reports as a form of do-it-yourself credit monitoring.

Credit monitoring only lets you know after someone has opened a new account in your name. A security freeze, on the other hand, prevents new accounts from being opened in the first place.

How does a security freeze prevent new accounts from being opened? It works by blocking your credit report from being shared with potential new creditors, such as banks or credit card companies. Most creditors will not issue new credit to a customer if they cannot see that customer's credit report or score derived from it from at least one of the three major national credit bureaus. So if a thief applies for a new account in your name with *your* Social Security number and *his or her* own address, but your credit report is frozen, creditors will simply not open a new account. That's why a security freeze offers peace of mind and is the only way to prevent someone from opening a new account in your name. (Note: Some creditors, such as some cell phone and utility companies, may not check with the bureaus before opening new accounts.)

So, the best course of action for most consumers is to place security freezes with the three major credit bureaus. Consumers in every state can choose to have their credit reports frozen until they want to apply for credit, at which time they can easily unfreeze or "thaw" their reports by lifting their freezes.[1]

Consumers who choose a security freeze should account for the time it can take to thaw their reports if they want to apply for credit in the future. In most cases if you request a thaw online or over the phone, your report can be unfrozen within 15 minutes.[2] However, it can take longer if you don't have your PIN number that was assigned to you when you froze your report. By law, credit bureaus have up to three days of receipt of your request to lift a freeze.

This report explores the best options you have against new account identity theft, walks you through freezing and unfreezing your credit reports and explains defenses against other types of identity theft.

Best Options against New Account Identity Theft

These steps are recommended **for all consumers** whether their information has been stolen in a data breach or not:

- Place a security freeze, also known as a credit freeze, on your credit report at each of the three major national credit bureaus – This is the ONLY reliable prevention of someone opening new financial accounts in your name.
- Next steps, after placing security freezes include:
  - Use your free annual credit reports as a form of "free credit monitoring."
  - Opt out of allowing your credit reports to be used to generate pre-approved (pre-screened) credit & insurance offers.

In addition to the above steps, the following steps are also recommended for **consumers whose information has been stolen** in a data breach:

- Sign up for free ID protection services and credit monitoring, if they are offered for free as a result of your personal information being stolen.
- Place free, renewable fraud alerts on your credit report (if your Social Security number was stolen and if you decide not to place security freezes on your credit reports.)
- Additionally, Identitytheft.gov is the government's official website that will walk you through clear checklists of actions you can take to recover from identity theft.

How Stolen Data is Used

From 2005 to October 27, 2015, there have been over 4,600 data breaches in the United States. Over 889,500,000 records have been breached.[3]

This year alone, from January 2015 to October 27, 2015, there have been well over 100 data breaches affecting over 153,000,000 records. These statistics are a low estimate.[4]

Many of these data breach victims are at risk of identity theft of one form or another. Once data is stolen, there are a variety of ways it can be used, depending on how much data was taken:

Financial Identity Theft

- **Existing Account Fraud:** If a thief obtains a full name and credit or debit card number, the thief can access existing bank and credit accounts for in person transactions, which do not require the Card Security Code on the back of cards that online transactions require.
- **New Account Identity Theft**: With a full name and Social Security number (SSN), a thief can open up new credit accounts.

Fraud on existing accounts is considered identity theft under federal law – this is to make sure consumers receive strong protections and banks are incentivized to stop such fraud. However, most data security advocates reserve the term "identity theft" for the much more serious, although less common, crime of establishing new accounts in other peoples' names.

Tax Refund Fraud or Medical Services Fraud

With a full name, SSN and a birthdate (and sometimes an existing health insurance account number), a thief can attempt to receive benefits and services in your name.

Reputational & Physical Harm

Some breaches involve personal information that can be used to blackmail, stalk, or otherwise inflict reputational or physical harm against data breach victims.

Warning: If a Thief Gets Some of the Information, Phishing is How They Try for More

Even if the thief only obtains some of your information - for example, if he/she didn't get your card info or SSN but obtained phone numbers or e-mail addresses - watch out! The thief can use social engineering or "phishing" scams to attempt to collect more information needed to commit any of the above more severe crimes. Also, you can still be a victim of "phishing" even if none of your information was stolen in a data breach because a lot of personal information is already available on the internet. See one of the next sections on "What is Social Engineering? What is Phishing" for more information.

Some Recent Breaches

The following chart provides examples of different types of crimes and techniques involved in recent data breaches:

	*When Reported	# of Records	Existing Credit Card or Checking Acct Fraud	Phishing for More Info	New Acct ID Theft	Tax Refund Fraud	Medical Services Theft	Reputation/ Physical Harm
Excellus Blue Cross Blue Shield[5]	Sept 2015	~10 million	X	X	X		X	X
Experian[6]	Oct 2015	~15 million		X	X	X		
IRS[7]	May 2015	Up to 330,000		X	X	X		
Michael's[8]	Jan 2014	~3 million	X					
OPM (2 breaches)[9]	April & June 2015	~26 million		X	X			X
Target[10]	Dec 2013	~110 million	X	X				

***Note that we use the date that breaches were reported to the media. Breaches may have occurred or been discovered earlier. In some cases, all victims may still not have been personally notified.*

Blue Cross Blue Shield Health Insurance Plans: Several breaches have affected affiliates of Blue Cross Blue Shield, but the breaches may have affected customers of other health plans whose family members may, for example, have received out-of-network care at a breached

plan. Information breached could allow new account identity theft or, in some cases, theft of medical services.

- **Anthem** – A breach of the nation's second largest health care plan, California's Anthem, in February 2015, is estimated to have affected 80 million consumers, but was not reported to have included health information.
- **Premera**—The March 2015 breach of the Pacific Northwest affiliate Premera, affected 11 million customers and is reported to have included health-related information.
- **CareFirst—**In May 2015, the DC-area affiliate CareFirst reported a breach affecting over 1 million customers. The company says Social Security numbers and health care records were not breached.
- **Excellus:** In August 2015, the upstate New York Blue Cross affiliate Excellus reported a breach affecting over 10 million customers. Excellus has reported that attackers "may" have obtained Social Security numbers, membership numbers and claims information as well as other personal information. (The company has also determined that evidence shows that the breach may have begun in 2013. Such a pattern of delayed discovery and reporting is probably true of other breaches in this list.)

Experian and T-Mobile: On October 1, 2015, wireless phone company T-Mobile announced that data for 15 million of its customers and applicants had been stolen from Experian computers. T-Mobile uses Experian, one of the three big national credit bureaus, to conduct credit application review for applicants before opening new accounts. Lost data includes names, addresses and birth dates and Social Security numbers, among other information breached from the consumer files.

This breach is particularly concerning because credit bureaus are subject to very high security standards, but losing Social Security numbers -- the keys to new account identity theft – makes this breach much worse. Experian, which lost the data, offered its own branded "ProtectMyID" credit monitoring for two years. It has also offered other services, including internet scans for personal information and access to identity theft resolution specialists – these types of services are further explained in the "Detection VS. Prevention" section of this report. T-Mobile has also offered an alternative credit monitoring service with CSID.[11] Experian has denied that its consumer reporting (credit bureau) servers were breached.[12]

Internal Revenue Service (IRS): In February, some state tax officials and then the private tax filing firm Turbotax temporarily suspended online tax filing following reports of widespread fraudulent theft of state tax refunds. In May 2015, the IRS reported its own breach as initially affecting 100,000 taxpayers; in August the estimate was raised to over 334,000. Breached

information included prior year tax returns. The breach was enabled using SSNs, DOBs, tax filing status, address, and personal security questions from multiple sources.

In October 2015, the IRS announced new efforts to fight fraudulent tax returns[13]. These efforts include an agreement among the IRS, states and tax preparation companies to share suspicious activity on 20 data points on tax returns to help spot fraud sooner. Additionally, tax preparation companies will ask tax filers three identity verification questions and require more secure passwords. Software companies will also notify customers when changes are made to their accounts or if second tax refunds are filed using their Social Security numbers.

Michaels Stores and Target Corporation: In December 2013, **Target Corporation** announced it was the victim of a retail credit and debit card breach initially affecting 40 million customers at the cash register. The number affected was later increased to 70-110 million customers, after it was determined that thieves also had access to backroom computers containing details of registered Target customers or Target-branded cardholders. In general, the first set of consumers faced a large risk of existing account fraud. The second set of consumers were also at risk of phishing scams—even though their Social Security numbers were not included in the theft, thieves could use their email addresses or phone numbers to try to obtain this additional information, which would make it easier to commit new account financial fraud. In January 2014, Michael's Stores reported a similar breach of credit and debit card data affecting over 3 million customers.

U.S. Office of Personnel Management (OPM): In April and June 2015, OPM reported on breaches affecting 26 million federal employees, as well as their spouses, co-workers and friends listed as references on security clearance applications. Information breached may have included dates-of-birth, Social Security numbers, fingerprints, usernames & passwords, personal info from interviews and information obtained in security investigations which could be used not only for new account identity theft but also to damage reputations or commit espionage (for example, reports of arrests, whether or not convicted, prior drug use, marital affairs, etc.)

Detection vs. Prevention

The first defense against any kind of identity theft is to be vigilant about protecting your personal information by taking steps like creating secure passwords, installing anti-virus and anti-malware software, and shredding personal documents. (See Appendix A for more tips on protecting your personal information.) However, if and when someone does steal your information, there is only one type of identity theft that can actually be prevented before it

happens: New account identity theft, where someone opens a new account, such as a credit card, bank account, or loan in your name. And for this type of fraud, a security freeze is the best line of defense and the only way to achieve peace of mind. All other types of identity theft and fraud, at best, can only be detected after the fact.

Unfortunately, the services and steps that are most offered and recommended to consumers are the ones that only detect fraud. These services and steps include credit monitoring, identity protection services, and fraud alerts that can be placed on your credit reports by law. Depending on your circumstances, you might decide one or more of these are right for you. But you should know the limitations of each:

Credit Monitoring:

Credit monitoring is often offered to data breach victims for free and is also available for purchase to all consumers for a monthly fee ranging from $9.99/month-$19.99/month or more. The range of features varies but can include access to one or more of your credit reports, monitoring of one or more of your credit reports, alerts on changes to your report(s), access to one or more of your FICO scores, monitoring of one or more of your FICO scores, and alerts on changes to your score(s).

Credit monitoring doesn't prevent any type of fraud and can only detect one type: new account fraud, where someone opens a new account in your name. If consumers don't know about the following shortcomings, credit monitoring may even provide a false sense of security.

Does Not Help With Existing Account Fraud

Credit monitoring is not able to prevent or even detect fraud on existing accounts. Banks and credit card companies have their own security measures in place to prevent, detect, and resolve such fraud. (We discuss these measures in further detail in the "Security Measures for Existing Credit Accounts" section of this report.)

Does Not Prevent Fraud

Credit monitoring services don't prevent any type of fraud. They only alert you *after* new financial accounts have been opened in your name.

Still Might Not Catch New Account ID Theft!

Consumers should be further aware that fraudulent accounts opened in your name still might not be caught if the service doesn't monitor your credit reports at all three major national credit bureaus.

Target, for example, offered their customers a free version of Experian's ProtectMyID service after its 2013 holiday season data breach. This free version only monitored

consumers' Experian credit reports, making it possible for any fraudulent activity on consumers' Equifax and TransUnion reports to go undetected.[14] Also, these "free" services are generally provided for a limited time, up to a year or 18 months.

Paid Services Charge You Monthly

In particular, these services should not be paid for because it is already possible to monitor your own credit by staggering requests for your free annual credit reports available by law. We acknowledge that a credit monitoring service might detect theft faster than you might on your own, depending on when the theft occurs and when you check your reports. But is it worth the $10 - $20 or more in monthly fees to find out about theft after someone has already attempted to or successfully opened a new account in your name when you can monitor your own accounts and prevent such activity with less costly security freezes?

Note: It doesn't hurt to take free credit monitoring and identity protection services if you have been a victim of a data breach. If you already have security freezes placed on your credit reports when your information is stolen, there is really no need for credit monitoring because there won't be anything to monitor. But if other identity protection services like the ones listed below are part of what is offered, it doesn't hurt to take the whole package offered. If you already have freezes on your reports, you will need to lift your freezes before signing up for the credit monitoring and reinstate your freezes. If you don't have freezes on your credit reports yet, sign up for the free credit monitoring first, then place your freezes.

Identity Protection Services:

Some of these services are sometimes offered to data breach victims and are also available for purchase to all consumers for a monthly fee. The range of service features varies but can include:

Scanning of Personal Information

These features scan the dark corners of the internet and public (and in some cases nonpublic) records to detect any changes in or selling of your personal information. These types of scans and surveillance could be helpful in detecting fraud besides new and existing account fraud, such as crime committed in your name.

Identity Theft Insurance

This is a feature that reimburses you for costs incurred from identity theft. It's worth noting that you might already have some sort of insurance or equivalent protection from fraud resulting from id theft that is extended to you voluntarily by your employer, your insurance company (as a rider on your existing homeowner's or renter's insurance), or your credit card issuer (as a perk), etc. It's also important to point out that

ID theft insurance, whether offered free or as part of a service that you're paying for always has limitations, exclusions, and requirements and usually only covers incidental expenses to clear ID theft problems up such as postage and notary fees. It doesn't usually reimburse you for money that's been stolen from you, and if it claims to cover attorney's fees, remember that such coverage is usually extremely limited.[15]

Identity Theft Resolution

In the event of identity theft, a specialist will assist you in contacting the right people and going through the right steps. Some services claim that they will do all the work for you.[16] While this feature can be helpful, these steps can also be found on identitytheft.gov and be done by yourself for free.

Fraud Alerts By Law:

Fraud alerts are recommended for consumers whose information was stolen in a data breach. Active military have additional protections.

By law, it is possible to place renewable fraud alerts on your credit reports for free for 90 days at a time. These alerts will let a creditor know that they should not approve a line of credit without verifying your identity first, which means they might try to contact you. However, just know that creditors are not *legally* bound to get your approval first before issuing credit, although they do face greater legal liability if they do not take further verification steps.

When you sign up for a fraud alert with one credit bureau, it is required by law to contact the other two major credit bureaus on your behalf to file fraud alerts with them too. If you are not a victim of identity theft fraud, you will have to renew these alerts every 90 days.

If you have been a victim of identity theft you can sign up for an extended fraud alert for seven years without having to renew it every 90 days. This requires filling out an identity theft report, which is made up of an identity theft affidavit and a police report - both steps are walked through at identitytheft.gov. If you are on active military duty, you can sign up for these alerts for one year, whether you are a victim of identity theft or not – your name will also be removed from pre-approved credit offers for two years.[17]

How to Apply for Fraud Alerts

Equifax

Online: https://www.alerts.equifax.com

Phone: 1-888-766-0008

Experian
Online: https://www.experian.com/fraudalert (Click on the "Add An Initial Security Alert for 90 Days" button or select "Add a Fraud Alert Message" and click the "Continue" button for extended and active duty alerts.
Phone: 1-888-397-3742

TransUnion
Online: http://www.transunion.com/fraud
Phone: 1-800-680-7289

Innovis (This is a fourth, smaller bureau. Fraud alerts with Innovis do not get shared to or from the three major credit bureaus above. If you want an alert placed with Innovis, you need to do it separately from the other three bureaus.).
Online: https://www.innovis.com/fraudActiveDutyAlerts/index
Phone: 1-800-540-2505
Mail: Send this form (https://www.innovis.com/pdf/InnovisFraudandActiveDutyAlertRequest.pdf)
Walk in: 875 Greentree Road, 8 Parkway Center, Pittsburgh PA 15220

Security Measures for Existing Credit Accounts

Many banks and credit card companies already have mechanisms in place to detect fraudulent use of existing accounts and remove unauthorized purchases. Also, nearly all credit and debit cards are being replaced with "chip" cards. In a related development, by October 1, 2015, most bigger merchants replaced their "swipe" terminals with "swipe or dip" terminals. A "chip" card that is dipped does not transfer your account number to the merchant's computer at all, greatly reducing the odds that you will be a victim of in-person retail fraud. The chip also makes it harder for crooks to take your account information and create a counterfeit card to use for purchases.

However, online fraud could still occur, so we advise using credit cards, not debit cards, for online purchases, if you have a credit card and are confident you can avoid the real risk of piling up excessive credit card debt. There are some online PIN debit systems that work, but most banks do not yet allow their use. Your legal rights are substantially stronger with a credit card; plus, you don't face the risk of waiting for the bank to replace money into your checking account after a fraud investigation involving your debit card. (Provided a consumer has not lost the debit card itself, she or he has up to 60 days to notify the bank of fraudulent activity on a debit card to face zero liability. However, some liability kicks in after just 48 hours if you've actually lost the card).

Of course, consumers should also check their statements regularly to detect any fraudulent purchases. It is also recommend that consumers check their online accounts frequently and not just wait for their statements – this can be done safely as long as precautions are taken to keep computer and/or mobile devices secure. You can also set up either text messages or email alerts to notify you of transactions. Many financial institutions allow you to set parameters for specific notifications, such as online transactions and transactions over a dollar amount you specify.

What is Social Engineering? What is Phishing?

Even if enough personal information hasn't been stolen in a data breach to commit fraud, we remind you that bad guys will try to use what was stolen or take advantage of publicly available information to trick you into providing the "keys" to identity theft, such as your SSN. They may also try to obtain passwords, full account numbers or security codes in this manner. Typically, these attempts come in the form of spam emails or messages on social media from well-known companies, prompting you to reply with personal information or to click on a link or attachment that will download malware onto your computer and steal personal information. This is called a social engineering or "phishing" scam. A bad guy may call and say "I am from the bank security department; I will verify that by reading the last four digits of your account number. Now, please confirm I am speaking to the correct consumer by reading me the security code on the back of the card." Of course, many consumers don't realize that the last four digits of account numbers are widely available but security codes are not.

Such attempts tend to increase after well publicized data breaches, as other identity thieves, even wannabees not involved in the initial theft, will take advantage of heightened fears of identity theft and try to "verify" additional personal information for "security precautions."[18] The current "scam of the day" is to call consumers concerning the widely publicized, but slow, transition to "chip" credit and debit cards and attempt to scare them into giving up their account numbers and security codes.

Identity thieves will also take advantage of the tons of information now available in a two-second google-search or for sale on an underground network (these networks are generically called the "darknet").

They'll contact you personally and try to impress you with what they already know ("come on, I know so much, I must be legitimate"), so that they can get more. When phishing is directed towards a particular person, it is called a "spear phishing" scam.[19] If someone calls you and says "I am from your bank," hang up and call the number on your card, not the number they give you. And certainly don't call any numbers or click on any links in any email supposedly "from

your bank." There is an even more nefarious version of this scheme against senior employees of a company, bank or government agency who may unwittingly grant the thief deeper access to a particular computer containing military, financial or corporate secrets. So, while information may be obtained on millions of consumers, the true target list may be smaller.[20]

Summary: Remember that any bad guy with some information about you wants to "phish" for even more to fill in the blanks. Don't click on email links; don't call the numbers in emails or provide information to "corporate security" when they call. Instead, hang up and call the number on your bank card. You may indeed get a legitimate call or message from your bank or someone else you have an account with asking to verify a transaction because fraud is suspected – but in that case, they won't ask for your account number or other personal information because they already have it.

I'm an Identity Theft Victim! What Should I Do?

Identitytheft.gov is the government's official website that will walk you through clear checklists of actions you can take to recover from identity theft. Here are examples.

Other Steps

Depending on your situation, you might need to take additional steps.

- Resolve tax-related identity theft.
- Report a misused Social Security number.
- Stop debt collectors from trying to collect debts you don't owe.
- Replace government-issued IDs.
- Resolve child identity theft.
- Resolve medical identity theft.
- Clear your name of criminal charges.

For certain types of accounts, you might have to contact additional offices.

- Utilities
- Checking accounts
- Student loans
- Investment accounts
- Bankruptcy filed in your name

Feedback

The Security/Credit Freeze

What is It?

A security freeze, also known as a credit freeze, works by preventing your credit report from being shared with potential new creditors, such as banks or credit card companies.

Ok, so what's my credit report again?
Your credit report is a record of your credit history and is used to determine your credit score – potential new creditors look at both your credit report and credit score to decide whether to extend you credit and at what interest rates. (Credit reports are also used for employment and insurance decisions.) There are three major national credit bureaus, also known as credit reporting agencies: **Equifax, Experian, and TransUnion**. Each bureau has its own report and score for you. Mortgage companies may check all credit reports; other creditors may check only one or two, depending on what region of the country you live in, or what sort of or amount of credit you are applying for. There is also a newer, fourth smaller national credit bureau, Innovis, used primarily by creditors buying lists of consumers for marketing (prescreening) purposes, not (so far) for credit decision-making. All of these national bureaus accept security freezes.

The Bottom Line
Most creditors will not issue you new credit if they cannot see your credit report first. So if a thief applies for a new account in your name, but your credit report is frozen, creditors that cannot see it will simply not open a new account. That's why a security freeze placed on your credit report at each of the three major national credit bureaus offers peace of mind and is the only way to prevent someone from opening a new account in your name. (Note: Some creditors, such as some cell phone and utility companies, may not check with the bureaus before opening new accounts.)

Main Features of a Security Freeze

- You can easily "unfreeze" your credit report when you want to apply for new credit. Freezes can be temporarily or permanently lifted when you want.
- A security freeze does not affect your credit score. In fact, a security freeze helps protect your score by preventing your credit from being negatively scored if someone tries to fraudulently apply for credit in your name. This is because you can potentially lose points every time your credit report is checked by a new creditor when you apply for credit. Your credit score is what potential creditors look at when deciding to give you credit. (Feel free to look at your credit score or report as often as you want; your own inquiries have no effect on your score.)

- Your credit will continue to be scored for your use of existing credit. In other words, a security freeze does not affect your ability to use existing credit you already have, such as a credit card or loan, nor does it prevent existing creditors from reviewing your continued eligibility for current or additional credit.
- Debt collection companies acting on behalf of credit companies you already have a relationship with can still access your credit report. Also, according to the FTC, "government agencies may have access in response to a court or administrative order, a subpoena, or a search warrant."[21]
- Security freezes are available to consumers in all 50 states and the District of Columbia. A security freeze costs between $3-10 for each of the three big national credit bureaus, depending on the state. (There is no fee to place a freeze with the fourth, smaller bureau, Innovis.) There is a $2-12 fee, depending on the state, for unfreezing your credit report with each bureau. All states give you the right to place free security freezes if you can prove that you are an identity theft victim. Some states offer them for free to consumer 65 years+. There are seven states where freezes are free to all consumers, whether they are identity theft victims or not[22]:
    - Colorado (first freeze is free)
    - Indiana
    - Maine
    - New Jersey
    - New York (first freeze is free)
    - North Carolina (free online only)
    - South Carolina

  Lifting freezes both temporarily and permanently is free to all consumers in: D.C., Delaware, Indiana, Maine, North Carolina, South Carolina, Tennessee, and Virginia.

  Lifting freezes permanently (but not temporarily) is free to all consumers in Alaska, Idaho, Missouri, Montana, Nebraska, North Dakota, and Pennsylvania.

  You can see all applicable fees for you state on Equifax's "Security Freeze Fees and Requirements" webpage: http://bit.ly/1LUIF0P

- Security freezes can also be placed by parents and legal guardians of minors and medically incapacitated consumers. Why a security freeze for children? Security freezes can stop child identity theft, a growing problem that might not be discovered for years. Twenty states require credit bureaus to offer security freezes for minors.[23] The credit bureau Equifax is now providing them in every state.
- **Warning:** It is important to note that neither credit monitoring nor a security freeze can detect or prevent unauthorized use of your existing credit accounts, tax refund fraud,

medical fraud, or reputational or physical harm, by thieves. A security freeze prevents identity theft on new accounts, such as credit cards, loans, and bank accounts.

How to Freeze (and Unfreeze) Your Credit Reports

- It is recommended you freeze your credit report with at least the three main credit bureaus (Experian, Equifax and TransUnion). Unlike fraud alerts, placing a freeze with one bureau does not automatically freeze your account with the other bureaus. You have to place a freeze with each bureau where you want one. Some creditors use one, while some will use the others, so your best coverage is to freeze all three.
- You will receive a PIN number for your security freeze with each bureau. You will use this PIN number when you want to unfreeze your credit report any time you want to apply for new credit.
- If you want to temporarily lift a freeze because you are applying for credit or a job, try to find out which credit bureau the business uses to check credit reports. You can save some money and time by only lifting your freeze for that credit bureau.

  You can temporarily lift a freeze for a specific period of time, from one day to one year, in all states. In 29 states and the District of Columbia, you also have the option of temporarily lifting a freeze for just a particular creditor that you specify. You can see all applicable fees for you state on Equifax's "Security Freeze Fees and Requirements" webpage: http://bit.ly/1LUIF0P

- Make sure to account for the time it can take to thaw your report. In most cases if you request a thaw online or over the phone, your report can be unfrozen within 15 minutes. However, it can take longer if you don't have your PIN number that was assigned to you when you froze your report, so make sure to keep your PIN number in a safe, memorable place where you can quickly retrieve it when needed. By law, credit bureaus have up to three days of receipt of your request to lift your freeze.

Placing and Lifting a Security Freeze with Each Credit Bureau

You can place a freeze online, over the phone, or in writing.

Equifax
Online: https://www.freeze.equifax.com
Phone: 1-800-685-1111 (NY residents please call 1-800-349-9960)
Mail: Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348

Experian

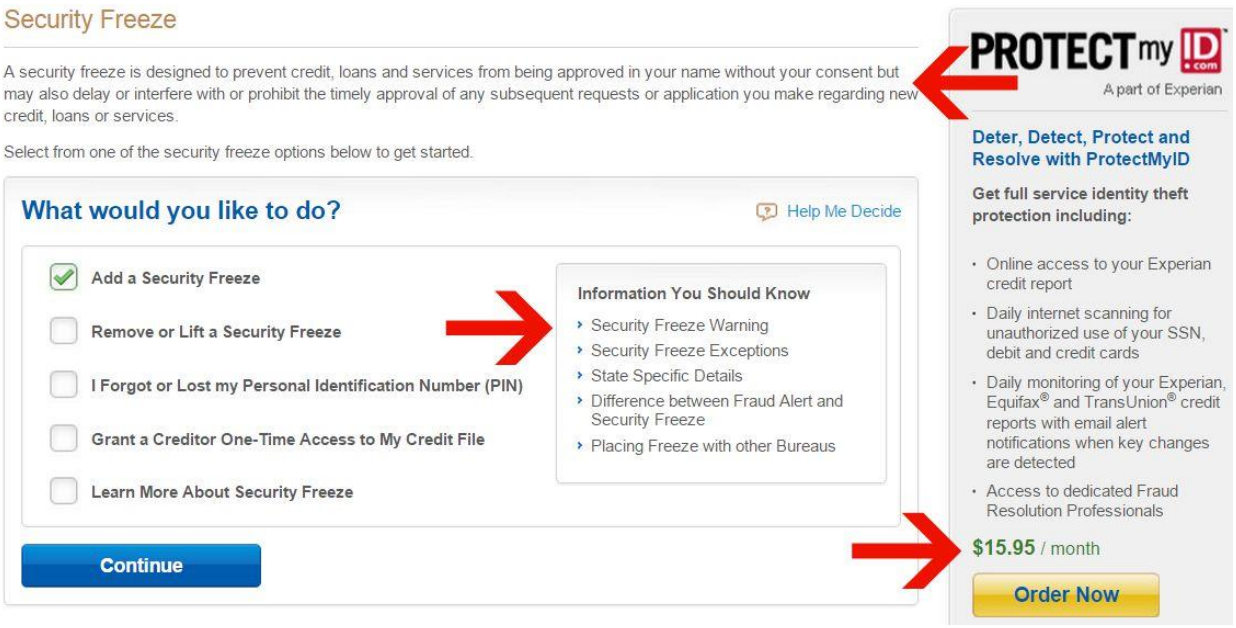
Online: https://www.experian.com/freeze/center.html

Phone: 1-888-397-3742

Mail: Experian Security Freeze, P.O. Box 9554, Allen, Texas 75013

Experian includes a potentially confusing three paragraph "Security Freeze Warning." They are just explaining that you will need to unfreeze your credit report before applying for credit if you ever wish to do so in the future. You might also notice right next to their warning is an offer to purchase their credit monitoring service for $15.95 a month – again, the security freeze is the ONLY way to prevent new accounts from being fraudulently opened in your name and is much cheaper than paid credit monitoring.

Figure (Arrows are ours to show Experian's warnings and sales pitch)



TransUnion

Online: http://www.transunion.com/securityfreeze

Phone: 888-909-8872

Mail: TransUnion LLC, P.O. Box 2000, Chester, PA 19022

Innovis (smaller, new bureau)

Online: https://www.innovis.com/personal/securityFreeze

Phone: 1-800-540-2505

Mail: Fill out this form (https://www.innovis.com/pdf/InnovisSecurityFreezeRequest.pdf)

In person: 875 Greentree Road, 8 Parkway Center Pittsburgh, PA 15220

Fun Fact: We worked on the original Security Freeze Law

We worked on the first security freeze law, in California, and then **promoted it nationwide, state by state, with a model data breach notice and security freeze law**[24], written with Consumers Union/ Consumer Reports and also promoted by many state AARP chapters. Between 2005 and 2009 a version was passed by nearly every state, forcing the credit bureaus to eventually provide the freeze everywhere.

How to Get Free Credit Monitoring

Use Your Free Annual Credit Reports

Federal law requires each of the three major credit bureaus to provide a free credit report every year to all customers who request one.[25]

If you stagger a request for a report from one of the three credit bureaus every four months or so, you've got free credit monitoring! Even if you choose to do a security freeze, it is still advisable to request and monitor your free annual credit reports.[26]

You can request your **free credit reports online, over the phone, or by mail.**

> **Online: annualcreditreport.com** – this is the official website authorized by the government for requesting these reports. Make sure to type this accurately. As of the printing of this report, misspelled websites are currently inactive but have existed in the past to misdirect people to unofficial services.
>
> **Phone**: 1-877-322-8228.
>
> **Mail**: Complete the Annual Credit Report Request Form (http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf) and mail it to:
>
> Annual Credit Report Request Service
> P.O. Box 105281
> Atlanta, GA 30348-5281.

If you want your Innovis credit report, you will need to request it directly from them by phone (1-800-540-2505), mail (send in this form: https://www.innovis.com/pdf/InnovisCreditReportRequest.pdf), or walk-in (875 Greentree Road, 8 Parkway Center, Pittsburgh, PA 15220).

Additional Free Annual Reports

Consumers in each of the following seven states can get an additional free report from each bureau each year under state law: Colorado, Georgia (two additional reports), Maine, Maryland, Massachusetts, New Jersey, and Vermont.[27]

An additional free annual report is also available to consumers in all states for people that are unemployed and intend to apply for employment within 60 days, are receiving public welfare assistance, believe their credit report contains inaccurate information because of fraud, or have received adverse action like denial of credit or insurance in the last 60 days. Additionally, if you have already received your free annual reports this year but have since placed a fraud alert, you can follow the instructions in your fraud alert confirmation letter to get an additional free report.[28]

Reduced fees for additional annual reports are available to all consumers in: California ($8), Connecticut ($5), Minnesota ($3), and Montana ($8.50).[29]

All consumers in all other states can be charged no more than $12 for an additional report.[30]

Order Your Additional Reports

Requests for additional annual reports need to be made to each credit bureau separately.

Equifax
Online: http://www.equifax.com/CreditReportAssistance (Click "Expand" next to "Get Your Credit Report" and click on "Get Started" under "Other Ways to Obtain a Free or Discounted Credit Report")
Phone: 1-800-685-1111
Mail: Equifax Disclosure Department, P.O. Box 740241, Atlanta, GA 30374

Experian
Online: https://www.experian.com/reportaccess/ (Click on "Request My Credit Report")
Phone: 1-888-EXPERIAN

TransUnion
Online: https://disclosure.transunion.com/dc/disclosure/disclosure.jsp
Phone: 1-800-888-4213
Mail: Send this form (https://disclosure.transunion.com/pdf/DisclosureRequest.pdf) to TransUnion LLC, P.O. Box 1000, Chester, PA 19022

Innovis

Innovis doesn't have an online way to order credit reports
Phone: 1-800-540-2505

Mail: Send this form (https://www.innovis.com/pdf/InnovisCreditReportRequest.pdf)
Walk in: 875 Greentree Road, 8 Parkway Center, Pittsburgh, PA 15220

Other Free Credit Reports

There are other non-official sites that offer free reports. Some sites offer free credit scores too. Beware of sites that promise free reports and scores but may use trial offer gimmicks to urge you to switch to paid credit monitoring or other services.

There are some sites that offer no strings attached, free services - just expect to see ads and also know that the credit scores are these sites' own estimates based on your credit reports and not a FICO score as used by most creditors (some FICO scores may be slightly customized by different bureaus or lenders). Here are a few of these sites:

- Credit.com offers a free credit score based on your Experian report.
- Credit Karma (creditkarma.com) provides free weekly access to your Equifax and TransUnion credit reports and updated credit scores based on those credit reports. They also provide free daily credit monitoring of your TransUnion credit report.
- Credit Sesame (creditsesame.com) offers a free credit score based on your Experian report and free credit monitoring of your Experian report. They will also send you daily alerts via text, email, or through their app, of any changes to your Experian credit report.
- FreeCreditReport.com offers a free Experian credit report.

Free Credit Scores From Your Credit Card Company: More and more credit card companies are joining a FICO program that is being encouraged by the U.S. Consumer Financial Protection Bureau (CFPB). Look for information on your monthly statement. If you cannot find a free credit score disclosure, ask your credit card company to start providing one.

Also: Opt Out of Pre-approved Credit & Insurance Offers

Opting out of pre-approved (pre-screened) credit & insurance offers is your legal right and is recommended for all consumers. Credit and insurance companies buy "prescreened" lists from the credit bureaus to make pre-approved offers to prospective customers. While such offers provide consumers with information about possible credit options, identity thieves may steal these pre-approved offers and apply for them with your personal information.

Optoutprescreen.com is the official website sponsored by the four national credit bureaus where by law you can opt out of receiving these offers for five years or permanently. You can also opt back in any time using this website. Alternatively, you can call the opt-out number toll-free 1-888-5-OPT-OUT (1-888-567-8688). Note that while opting out dramatically slows the flow

of credit card offers, it doesn't stop it. Any company you have a business relationship with can still make offers of its own card or its partners' cards.

Conclusion

Whether your personal information has been stolen or not, **your best protection against new account identity theft is the security freeze (also known as the credit freeze).**

Credit monitoring only lets you know after someone has opened a new account in your name. A security freeze, on the other hand, prevents most new accounts from being opened in the first place.

The best course of action for most consumers is to have their credit reports at each of the three major national credit bureaus frozen until they want to apply for credit, at which time they can easily unfreeze or "thaw" their reports.

If you chose the security freeze, it is still advisable to request and monitor your free annual credit reports, available under federal law with each of the three major credit bureaus. It is also recommended that you consider opting out of pre-approved credit and insurance offers.

Appendix A: AVOIDING IDENTITY THEFT

1. Do not disclose your full nine-digit Social Security number unless absolutely necessary, and never use it as an identifier or password. Question those who ask for it.
2. Avoid paper billing by requesting secure electronic statements instead. If you require hard copies, you can print and store them safely without risking mail theft.
3. Lock your mailbox if it is lockable.
4. Shred documents containing personal information (name, account numbers, Social Security number, birth date) before throwing them away.
5. Configure your computer and/or smartphone to require a password for use, and set another password for sensitive files. Use unique passwords that include a combination of letters, numbers, and symbols. Do not use your birth date, a close relative's birth date, or a combination of letters and numbers on Splashdata's annual list of the most stolen passwords (https://www.teamsid.com/worst-passwords-of-2012). Avoid "security questions" such as "What is your favorite food" with answers such as "Pizza."
6. Avoid using the same password for different accounts, and change your passwords once or twice per year.
7. Install and update antivirus, anti-malware, and security programs on all computers, tablets, and smartphones.
8. Don't disclose information commonly used to verify your identity on social networking sites, such as date of birth, city of birth, mother's maiden name, name of high school, etc. If you do, don't use that information to verify your identity.
9. Avoid using credit or debit cards or conducting online banking transactions or making purchases, paying bills, or sending sensitive information over unsecured WiFi networks (e.g., any network without a password log-in, such as on trains, at airports, coffee shops, or hotels).
10. Disable Bluetooth connections on devices when not in use.
11. Watch out for "phishing" and other "social engineering" scams. Phishing is when identity thieves request personal information by pretending to be a legitimate entity, such as a bank or the IRS. Ignore unsolicited requests for personal information by email or over the phone, and only contact entities by means you know to be authentic. Do not contact an entity by clicking a link sent as part of an email requesting personal information, because phishers often link to authentic-looking, fake webpages. You can also call the phone number on the back of a card previously issued to you, or call the phone number on an old statement from that issuer.
12. Fight "skimmers." Do not give your debit card to a restaurant server or anyone who could have a hand-held skimming device out of sight. When using an ATM, look for suspicious cameras and holes, and touch to confirm that extra parts (loose or slightly different colors) have not been installed over the card reader. Always cover your hand while hand typing a PIN, and avoid using ATMs in secluded locations.
13. When accessing financial information on your smartphone, only use apps authorized by your bank or published by reputable app makers. Apps that show thousands of downloads are probably safe. Do not access apps on public open WiFi.

14. Place security, or credit freezes, on your credit report. Guarantee peace of mind against new account identity theft by freezing your credit reports, then thawing them only when you are in the credit markets. A creditor will deny credit to an imposter who applies for credit using the name and Social Security Number of a consumer who has placed a freeze.

DETECTING IDENTITY THEFT

1. Check your monthly statements for unauthorized charges. Be suspicious of phone calls about surprise debts.
2. Sign up to receive email and/or text notifications of account activity and changes to account information.
3. Instead of paying for over-priced subscription credit monitoring, use your free annual credit reports by law as your own credit monitoring service. Every 12 months, federal law gives you the right to receive one free credit report from each of the three main consumer reporting agencies, Equifax, Experian and TransUnion. Instead of requesting three at the same time, request one credit report from one of the bureaus every four months. Verify that the information is correct, and an account has not been opened without your knowledge. Free credit reports are available online at **AnnualCreditReport.com** or by calling 1-877-322-8228. Seven states – Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey and Vermont also provide an additional free report by state law, available by contacting each bureau directly.

Endnotes

[1] By law, 49 states and the District of Columbia require the availability of a security freeze. In 2007, the three major credit bureaus started offering the security freeze voluntarily to consumers in Michigan, the one state that doesn't have a security freeze law. See Consumers Union, *Consumers Union's Guide to Security Freeze Protection*, 5 February 2014.

[2] North Carolina Department of Justice, *Lifting a Security Freeze*, accessed at www.ncdoj.gov/getdoc, 27 October 2015. See also Experian, *How Long it Takes to Thaw a Frozen Credit Report*, accessed at www.experian.com/blogs, 27 October 2015.

[3] Privacy Rights Clearing House, *Chronology of Data Breaches/Security Breaches 2005 – Present*, accessed at www.privacyrights.org/data-breach, 27 October 2015. The Identity Theft Resource Center has their own numbers too. According to them, from 2005 – September 22nd, 2015, there have been 5,593 breaches and 828,937,722 breached records. See Identity Theft Resource Center, *Data Breaches*, accessed at www.idtheftcenter.org/id-theft/data-breaches.html, 27 October 2015.

[4] For many of the breaches listed with the Privacy Rights Clearinghouse, the number of breached records is unknown. Additionally, their list does not include all breaches. They include every reported breach with more than nine affected individuals. They include every reported breach affecting nine or fewer individuals if there is a compelling reason to alert consumers. Breaches that were not reported to consumers or a government agency are not included. See Privacy Rights Clearinghouse, *Chronology of Data Breaches: FAQ*, accessed at www.privacyrights.org/data-breach-FAQ, 27 October 2015.

[5] USA Today, "Cyber Breach Hits 10 Million Excellus Healthcare Customers," *USA Today*, 10 September 2015.

[6] Robert Hackett, "Experian Data Breach Affects 15 Million People Including T-Mobile Customers," *Fortune*, 1 October 2015.

[7] John D. McKinnon and Laura Saunders, "IRS Says Cyberattacks More Extensive Than Previously Reported," *The Wall Street Journal*, 17 August 2015.

[8] Amrita Jayakumar, "Michaels Says 3 Million Customers Hit by Data Breach," *The Washington Post*, 19 April 2014

[9] United States Office of Personnel Management, *Cybersecurity Resource Center Frequently Asked Questions*, accessed at www.opm.gov/cybersecurity/faqs, 27 October 2015.

[10] Clare O'Connor, "Surprise! Target Data Breach Could Include Your Info from Purchases Made a Decade Ago," *Forbes*, 16 January 2014. See also Ross Kerber, Phil Wahba, and Jim Finkle, "Target Apologizes for Data Breach, Retailers Embrace Security Upgrade," *Reuters*, 13 January 2014.

[11] T-Mobile also offered its customers and applicants an alternative to Experian's ProtectMyID credit monitoring service. It is a service through CSID. Enrollment can be done at www.protectmyid.com/alt.

[12] U.S. PIRG joined other organizations in a letter to the CFPB and other regulators asking a number of questions about this breach. See U.S. PIRG, *PIRGs, Others Ask CFPB & FTC to Investigate Experian/T-Mobile Data Breach* (press release), 8 October 2015.

[13] Jonnelle Marte and Lisa Rein, "IRS Enhances Efforts to Combat Identity Fraud, Claiming Upcoming Tax Season Will Be 'More Secure,'" *The Washington Post*, 20 October 2015.

[14] Jeff Blyskal, Consumer Reports, *Expect Less and Pay More with Target's Credit Monitoring*, 6 February 2014

[15] Susan Grant, Director of Consumer Protection and Privacy, Consumer Federation, personal communication, 17 September 2015

[16] According to the FTC, "Some companies offer services to help you rebuild your identity after a theft. Typically, you give these services a limited power of attorney, which allows them to act on your behalf

when dealing with consumer reporting companies, creditors, or other information sources." See Federal Trade Commission, *Identity Theft Protection Services*, accessed at www.consumer.ftc.gov/articles/0235-identity-theft-protection-services, 27 October 2015.

[17] The ability to place free fraud alerts on your reports comes from the Fair and Accurate Credit Transactions Act of 2003 (FACTA). This act amended the Fair Credit Reporting Act (FCRA), in order "to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes." See 108th Congress, *Fair and Accurate Credit Transactions Act of 2003*, 4 December 2003.

[18] As an example, Target acknowledged the rise of phishing scams in the wake of its 2013 holiday season data breach. See Jeff Blyskal, Consumer Reports, *Expect Less and Pay More with Target's Credit Monitoring*, 6 February 2014.

[19] Federal Bureau of Investigation, *Spear Phishers Angling to Steal Your Financial Info*, 1 April 2009.

[20] John Markoff, "Larger Prey Are Targets of Phishing," *The New York Times*, 16 April 2008.

[21] Federal Trade Commission, *Credit Freeze FAQs*, March 2014.

[22] Equifax, *Security Freeze Fees and Requirements*, 7 October 2015.

[23] Ibid.

[24] U.S. Public Interest Research Group and Consumers Union, *The Clean Credit and Identity Theft Protection Act: Model State Laws*, November 2005.

[25] The ability to request a free annual credit report from each of the three main credit bureau and to place free fraud alerts on your reports comes from the Fair and Accurate Credit Transactions Act of 2003 (FACTA). This act amended the Fair Credit Reporting Act (FCRA), in order "to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes." See 108th Congress, *Fair and Accurate Credit Transactions Act of 2003*, 4 December 2003.

[26] For additional information about alternatives to paid monitoring, Privacy Rights Clearinghouse has a fact sheet about monitoring services. See Privacy Rights Clearinghouse, *Identity Theft Monitoring Services*, October 2015, available at www.privacyrights.org/fs/fs33-CreditMonitoring.htm

[27] Innovis, *Credit Report Fees*, accessed at www.innovis.com/personal/creditReportFees, 27 October 2015.

[28] Federal Trade Commission, *What To Do Right Away*, accessed at Identitytheft.gov, 27 October 2015.

[29] Innovis, *Credit Report Fees*, accessed at www.innovis.com/personal/creditReportFees, 27 October 2015.

[30] Consumer Financial Protection Bureau, *How Much Does it Cost to Get a Copy of My Credit Report if I've Already Received All of My Free Credit Reports?*, 6 January 2015. Also, state laws change, so consumers can check with their state or local consumer protection agencies about their rights to free or reduced cost credit reports.