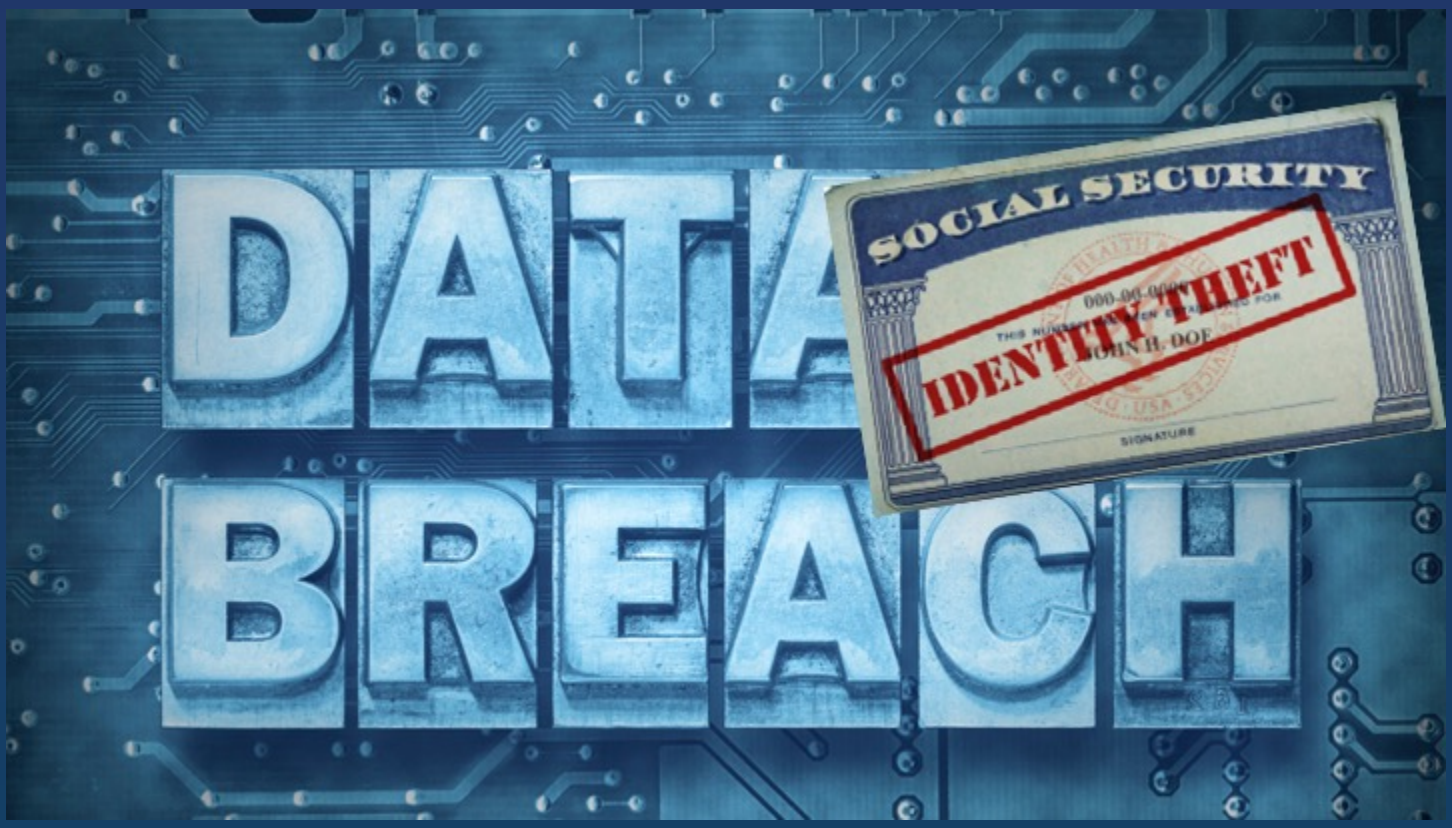

EQUIFAX BREACH: ONE YEAR LATER

How to Protect Yourself Against ID Theft & Hold Equifax Accountable

Arizona PIRG Education Fund

September 2018

EQUIFAX BREACH: ONE YEAR LATER

How to Protect Yourself Against ID Theft and Hold Equifax Accountable

Arizona PIRG Education Fund

Mike Litt and Ethan Lutz
September 2018

Acknowledgments

Arizona PIRG Education Fund thanks The Ford Foundation and the Colston Warne Fund of Consumers Union for making this report possible.

Thanks to Edmund Mierzwinski for review. We thank Jordan Leatherwood and Manuel Villagran, PIRG interns (summer 2018) for assistance on the report.

The authors bear responsibility for any factual errors. The recommendations are those of Arizona PIRG 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, the Arizona PIRG Education Fund offers an independent voice that works on behalf of the public interest. The Arizona PIRG Education Fund works to protect consumers and promote good government. We investigate problems, craft solutions, educate the public, and offer citizens meaningful opportunities for civic participation.

For more information, please visit our website at arizonapirgedfund.org.

Cover images from iStock: Data Breach by yuriz. Identity Theft inset by zimmytws.

Table of Contents

Introduction

One year after publicly announcing the worst data breach in history, Equifax still hasn't paid a price or provided the information and tools consumers need to adequately protect themselves.

On September 7th, 2017, Equifax publicly announced a breach of its data belonging to approximately 143 million U.S. consumers.[1] It later updated that number to 145.5 million[2] and then to nearly 148 million affected consumers.[3] By exposing sensitive personal information, including social security numbers and birthdates, and for some people, credit card numbers and driver's license numbers, Equifax put consumers at risk of several types of identity theft and fraud.

The purpose of this report is to make sure consumers have the information they need to protect themselves as much as possible, review what has happened in the last year, and point out the need for Congressional action to prevent breaches as bad as this one from ever happening again.

Equifax's Many Failures

Had Equifax not been so careless, the breach may never have happened. Four months before the hacking, Equifax could have fixed a known security vulnerability[4]. The company also botched its response by:

- Delaying public notification for at least six weeks[5]
- Setting up an online search tool that provided faulty results to those who used it about whether they were affected by the breach[6]
- Initially understaffing its call center[7]
- Initially including arbitration language that forced consumers to sign away their rights to a day in court[8]
- Directing consumers to a fake website[9]
- Failing to provide consumers full protection from new account identity theft -- which it still hasn't done. (See Appendix A for a summary of Equifax's offerings to consumers in response to the breach and how they fall short of protecting consumers.)

An investigative report released by Senator Elizabeth Warren further explains the numerous ways Equifax failed consumers.[10]

Understanding the Real Threats of Identity Theft

Up to 145.5 million consumers affected by the breach had both their social security numbers and birthdates accessed by hackers. Additional information taken from a portion of these consumers includes: 99 million addresses, 20.3 million phone numbers, 17.6 million driver's license numbers, 1.8 million email addresses, and 209,000 credit card numbers.[11] (*See Table 1 and Figure 1.*)

Figure 1 Type of Personal Information Lost in the Equifax Data Breach by Number of U.S. Consumers Impacted

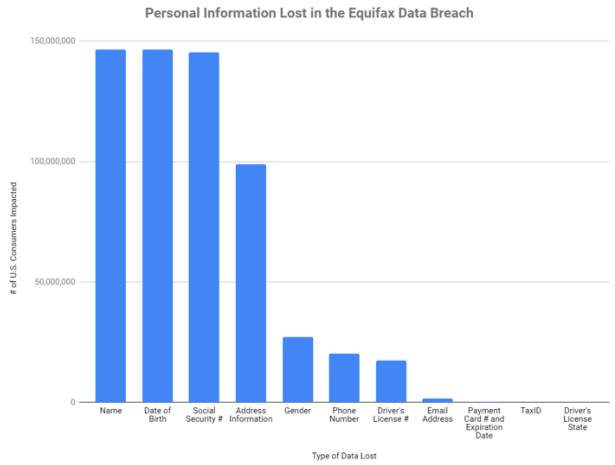

Table 1. Type of Personal Information Lost in the Equifax Data Breach by Number of U.S. Consumers Impacted

Type of Personal Information Lost	# of U.S. Consumers Impacted
Name	146,600,000
Date of Birth	146,600,000
Social Security #	145,500,000
Address Information	99,000,000
Gender	27,300,000
Phone Number	20,300,000
Driver's License #	17,600,000
Email Address	1,800,000
Payment Card # and Expiration Date	209,000
TaxID	97,500
Driver's License State	27,000

The exposure of such information means identity thieves can commit various types of identity theft and fraud. (*See Table 2.)*

We all know credit card numbers can be used to make fraudulent purchases on your existing credit accounts. But what makes the Equifax breach particularly bad is that with your stolen social security number and birthdate in hand, an identity thief has the keys to commit new account identity theft and several other types of fraud.

For example, an ID thief can try to apply for new credit cards or loans, order the latest smart phones on payment plans, open utility accounts, create bank accounts, file taxes, collect social security benefits, and possibly get healthcare or medical services, all in your name. Coupled with your driver's license number, which could be used to create a fake ID card, an identity thief might also try to apply for a job, get insurance, lease an apartment, or even commit crimes in your name.

And as long as social security numbers continue to be used to verify our identities, you are at risk of such fraud and the accompanying harm to your finances, reputation, and peace of mind for the rest of your life.

Table 2. Examples of Identity Theft & Fraud Made Possible by Personal Data Lost in the Equifax Breach

Type of ID Theft or Fraud	Phone Number or Email Address	Credit Card Number	Name and Social Security Number (SSN)	Name, SSN, and Birthdate	Name, SSN, and Driver's License Number
Phishing for More Information	X				
Existing Account Fraud		X			
New Account Fraud (including cell phone, credit card, loan, and utilities)			X		
Tax Refund Fraud				X	
Social Security Benefits Fraud				X	
Health Care Services / Medical Benefits Fraud				X	
Other (including applying for a job, committing crimes, getting insurance, or renting a home)					X

How to Protect Yourself After the Equifax Breach (whether your info was stolen or not)

Due to the prevalence of data breaches, we recommend taking steps to protect yourself against identity theft, whether your information was stolen in the Equifax breach or not. See Table 3.

Table 3. Steps Consumers Can Take to Prevent and/or Detect Different Types of ID Theft and Fraud

Type of ID Theft or Fraud	Prevention Method	Detection Method
Existing Account Fraud	Can only be detected after the fraud has occurred	Check your monthly credit card and bank statements. Sign up for free text and/or email alerts about changes to your accounts. If you receive a call -- supposedly from your bank and alleging fraud -- never provide any personal information. Instead, call the number on the back of your bank card and check with the security department.
New Account Fraud (including cell phone, credit card, loan, and utilities)	Get credit freezes at all three nationwide credit bureaus - Equifax, Experian, and TransUnion. Fraud alerts suggested if you don't get freezes. Freeze at NCTUE also recommended.	Check your free annual credit reports at Equifax, Experian, TransUnion, and NCTUE or sign up for free credit monitoring (but don't pay for subscription services.)
Tax Refund Fraud	File your taxes as soon as possible, before thieves do. Also, if you qualify, get an Identity Protection (IP) PIN.	Be alert to notices about a return already filed, additional taxes you owe, refund offsets, collection for a year you didn't file, or records showing income from an employer for whom you did not work.
Social Security Benefits Fraud	Sign up for your "my Social Security" (MySSA) account before thieves claim it and change your direct deposit info to their own checking accounts. A freeze on your Equifax credit report also blocks thieves from claiming your online account.	Periodically check your MySSA account for any changes to your personal information that might indicate thieves trying to claim your benefits over the phone.
Health Care Services / Medical Benefits Fraud	Can only be detected after the fraud has occurred	Sign up for online accounts with your health care and insurance providers to periodically check for any fraudulent services on your statements.
Other Fraudulent Activity (including applying for a job, committing crimes, getting insurance, opening a checking account, or renting a home in your name.)	Can only be detected after the fraud has occurred	Check your free annual consumer reports with companies that specialize in collecting particular information, including your check writing, employment, insurance claims, and tenant histories.

New Account Identity Theft

If you fall victim to new account identity theft, where someone successfully opens a new credit or loan account and racks up debt in your name, that could mean you get denied credit, a home mortgage or other loan, or even employment, due to a damaged credit score.

According to the Federal Trade Commission, fraud related to new credit card accounts was the most reported type of identity theft by consumers in 2017, making up 22% of all identity theft reports.[12] (See Appendix B for number of ID theft reports by type.) Also, 7,418 consumer complaints to the Consumer Financial Protection Bureau since September 8th, 2017, were categorized as problems with credit inquiries on credit reports not recognized by the consumer, debt as a result of identity theft, or credit cards opened as a result of identity theft or fraud.[13] (See Appendix C for samples of stories submitted to the CFPB.)

New account identity theft is the most preventable kind of identity theft. Below are steps you can take to detect, and better yet, prevent it:

- Request credit reports for free by law at all three nationwide credit bureaus to spot any unauthorized activity. If you request a copy of your report every 4 months -- one bureau at a time -- throughout the year, you are essentially doing your own free credit monitoring (instead of paying for it from a monthly subscription service.) The official website authorized by the government for requesting these free reports is **annualcreditreport.com**.[14] You can also request these reports by mail or telephone as explained by the FTC.[15]
- Place credit freezes on your credit reports with all three nationwide consumer reporting agencies, also known as credit bureaus - Equifax, Experian, and TransUnion. A credit freeze, also known as a security freeze, is a commonsense tool that allows consumers to freeze access to their credit history and scores, denying thieves the ability to open fake credit accounts in their names. We also recommend credit freezes at a fourth bureau, the National Consumer Telecom & Utilities Exchange (NCTUE) because some news outlets have reported fraudulent accounts being opened by cell phone companies using credit reports provided by the NCTUE.[16] The "Credit Freezes: How to Prevent New Account Identity Theft" section of this report explains how to freeze your credit reports.
- Place free, renewable fraud alerts if you decide not to place credit freezes on your credit reports. They don't block access to your credit reports, but they do notify creditors that they should try to verify your identity before opening a new account in your name.

A lot of attention has been paid to checking your credit reports and getting credit freezes. But there are steps you can take to help prevent and detect other types of fraud made possible by the Equifax breach, including the following:

Social Security Benefits Fraud

Sign up for your “my Social Security” (MySSA) account.[17] This will help prevent a scammer from opening an account in your name and changing your direct deposit information to his or her own checking account. A credit freeze on your Equifax credit report will also block the creation of a MySSA account because the Social Security Administration uses Equifax credit reports for identity verification.

Even if you don’t receive social security benefits yet, checking your MySSA account can help you spot changes to your personal information that might indicate thieves trying to claim your benefits over the phone.

Tax Refund Fraud

To help prevent someone from filing taxes and taking your tax refund, file your taxes as early as possible. Also, some people qualify for an Identity Protection (IP) PIN that must be entered before a tax filing can be submitted. The IP PIN is available to identity theft victims and is also currently offered to all taxpayers in Florida, Georgia, and Washington, D.C., as part of a pilot program.[18]

Be alert to notices about a return already filed, additional taxes you owe, refund offsets, collection for a year you didn't file, or records showing income from an employer for whom you did not work.

Existing Credit Card Fraud

Check your monthly statements for unauthorized charges. Be suspicious of phone calls about surprise debts.

Driver’s License Fraud

Requesting your driving record could help you spot any traffic violations committed in your name.[19]

Health Care/Medical Fraud

Sign up for online accounts with your health care and insurance providers to monitor any fraudulent services on your statements.

Other

There are many other consumer reporting companies besides the three big nationwide credit bureaus that specialize in collecting other types of information about you, including bounced check activity, criminal and other public records, employment information, insurance claims, and tenant history. **Requesting free reports with these specialty bureaus every year could help you spot various fraudulent activities done in your name.**[20]

Phishing Scams

Watch out for "phishing" scams where 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, links, phone calls, pop-up windows, or text messages. Scammers might bring up the limited information they already have on you to sound like the real deal and get you to give up even more.

Only contact entities by means you know to be legitimate. For example, if someone calls you purporting to be from your bank's security department, call the back of the number on your bank card and ask for the security department.

The "Protect Yourself from Identity Theft" section of this report provides more tips for preventing and detecting identity theft. 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.[21]

Actions Taken but Failure to Hold Equifax Accountable

Although there have been Congressional hearings, government investigations, lawsuits, proposed legislation, and a consent order in the last year, Equifax still has not paid a price for putting so many consumers in harm's way. As its earnings continue to rise, there need to be financial consequences if we want the credit bureaus to do everything possible to take our data security seriously. Any reasonable action should stop the bad behavior, punish the wrongdoer, and compensate the victims.

Below is a rundown of major actions related to the Equifax breach that have been taken since the breach was announced.

Agency Action

Federal investigations into the breach include those by the Consumer Financial Protection Bureau and Federal Trade Commission.[22] Agencies from eight states and Equifax reached an agreement, requiring Equifax to fix weaknesses in its data security operations.[23] The Securities and Exchange Commission and

Department of Justice charged a former software development manager[24] and a former executive[25] with insider trading for allegedly selling Equifax stock before the breach was made public.

Company Action

Last September, Equifax announced the retirement of three executives, including its CEO.[26] In its end of year report, Equifax outlined changes to its information data security, breach disclosure protocols, and executive leadership team, in response to its breach.[27]

Congressional Action

Congressional Hearings

Former Equifax CEO Richard Smith testified at three Congressional hearings.[28] He testified a fourth time when he was joined by then Interim CEO of Equifax, Paulino do Rego Barros, Jr.[29] (PIRG also testified at three Congressional hearings in response to the Equifax breach.[30])

Data Acquisition and Technology Accountability and Security Act

The House Financial Services Committee held a hearing on a draft bill this March that would require merchants, telecoms, and some other companies to notify the public when they are breached.[31] It exempts Equifax, other credit bureaus, and all banks from such breach notification requirements.[32] It also preempts, or replaces stronger requirements that many states already have in place.[33] This draft bill has not moved in committee.

Data Breach Prevention and Compensation Act Proposal

Current law prevents the federal government from issuing mandatory fines against the credit bureaus when they fail to protect our information. Furthermore, no single agency has the ability to establish data security requirements for the credit bureaus and make sure the firms are following them.

Legislation introduced earlier this year by Senators Elizabeth Warren (MA) and Mark Warner (VA) would give the Federal Trade Commission the authority to annually inspect large credit bureaus for cybersecurity and levy fines against them if they get breached.

If this policy had been in place during the Equifax incident last year, Equifax would have paid at least a $1.5 billion penalty, half of which would be returned to consumers affected by the breach.[34] Instead, the company reported earnings of $876.9 million in the second quarter of 2018, a 2 percent increase compared to last year.[35]

The legislation does not appear to have traction to move out of the Senate Banking Committee.

FCRA Liability Harmonization Act and the Credit Services Protection Act

Ironically, on the exact same day that Equifax publicly announced its breach last year, the Financial Institutions and Consumer Credit Subcommittee in the House had held a hearing on two consumer-opposed bills that would directly benefit the credit bureaus. The first, HR 2359, the FCRA Liability Harmonization Act (Congressman Loudermilk (GA)) would eliminate punitive damages and cap other damages payable to consumers harmed by violations of the Fair Credit Reporting Act. The second, HR XXXX, the Facilitating Access to Credit Act (Congressman Royce (CA)), would have exempted the credit bureaus from rules preventing misleading promises about repairing your credit. In June 2018, the Royce bill was formally introduced as the Credit Services Protection Act (HR 6192).[36] No further action has been taken on the Loudermilk proposal to make it harder for consumer-victims to recover damages from credit bureaus.[37]

Free Credit Freezes

A new federal law will eliminate fees for credit freezes across the country at all three nationwide credit bureaus on September 21st, 2018 for consumers, including minors and incapacitated individuals.[38] As an alternative option to credit freezes, it also increases the length of an initial fraud alert for consumers from 90 days to 1 year. While the new law has this minor provision which may save consumers money on credit freezes, overall, the comprehensive deregulatory law it was added to has broadly negative implications because its primary, unrelated provisions increase the likelihood of bad mortgages, racial discrimination in the marketplace, and risky banking practices.[39]

Lawsuits

Hundreds of class action lawsuits have been consolidated into several cases, each one representing a different class, including consumers, small businesses, financial institutions, and shareholders.[40] Equifax moved to dismiss the consumer class action case, claiming it has no obligation to safeguard the personal information it lost.[41] For basics on how class action lawsuits work, see Consumer Reports' "Should You Participate in a Class Action Against Equifax" story.[42]

State Attorneys General Leading the Way

According to Equifax's latest filing with the SEC, the company is being investigated by attorneys general in 48 states and DC. Other actions include lawsuits brought by the attorneys general of Massachusetts,[43] Puerto Rico[44], and West Virginia;[45] a bipartisan letter signed by 32 state attorneys general against the above-mentioned draft data breach notification bill;[46] and bipartisan calls for Equifax to get rid of its arbitration clause, fees for credit freezes, and links to paid credit monitoring services.[47]

Conclusion and Recommendations

Ultimately, we are not the customers of Equifax or the other credit bureaus; we are their product. We did not ask or give them permission to collect or sell our personal information. Congressional action, state and federal agency enforcement and private rights of action are needed to provide both the necessary financial consequences and oversight that will help prevent anything like last year's Equifax breach from happening again. Additionally, breached companies should be required to provide consumers with clear, complete, and concise information about what can be done to prevent, detect, and resolve most kinds of identity theft and fraud.

Types of Identity Theft

There are a variety of ways stolen data can be used, depending on what was taken. Different types of ID theft and fraud include:

Financial Identity Theft

Existing Account Fraud

If a thief obtains a credit or debit card number, the thief can access existing bank and credit accounts for in-person transactions.

New Account Identity Theft

With a full name and Social Security number (SSN), a thief can open new credit accounts.

Health Care/Medical Fraud

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

Social Security Benefits Fraud

With a full name, birthdate, and SSN, a thief can try to open a "my Social Security" (MySSA) account in your name and change your direct deposit information to his or her own checking account. Coupled with other information that can easily be found online, such as place of birth, a thief can also try to claim your benefits over the phone.

Tax Refund Fraud

With a full name, birthdate, and SSN a thief can attempt to file your taxes and claim your refund.

Other Fraud

With a full name, birthdate, SSN, and driver's license number (which can be turned into a fake license card), a thief can attempt numerous types of fraud, such as applying for a job, getting insurance, renting a home, or even committing crimes 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.

Phishing

With just a phone number or email address, a thief can use "phishing" scams to attempt to collect more information needed to commit any of the above more severe crimes.

Protect Yourself from Identity Theft

Use these checklists to help you prevent, detect, and resolve identity theft.

Preventing Identity Theft

The first key to protecting yourself from ID theft is prevention.

ID Theft Prevention for Online & Electronic Activity

- ❑ Consider locking your laptop at your work desk or when you're in a public place.
- ❑ Set passwords for your computer, smartphone, and tablet. Use six digits instead of four for your smartphone password.
- ❑ Set online account passwords that include at least 10 characters and a combination of capital letters, numbers, and symbols in the middle of the password, not the beginning or end.
- ❑ Avoid using the same password for different accounts. Consider using a password manager.
- ❑ Turn on two-factor authentication for your online accounts if available. You will receive additional codes for accessing your online accounts, in addition to your passwords.

- ❑ Keep all software updated. Turn on automatic updates for all software, including antivirus programs.
- ❑ Don't show information on social networking sites that is commonly used to verify your identity, 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.
- ❑ Turn on your laptop's firewall and turn off file sharing and "network discovery" for public Wi-Fi connections.[48]
- ❑ Turn off automatic connections to Wi-Fi networks on your electronic devices.
- ❑ Send personal information online through fully encrypted websites or apps. Encrypted websites start with **https**. The non-profit Electronic Frontier Foundation has the **HTTPS Everywhere** extension for your web browser that will make sure you're using encrypted communications on websites that support encryption.[49] In addition to using encrypted websites, online transactions are best conducted over secure encrypted Wi-Fi connections[50] or your phone's data network,[51] versus an unsecure Wi-Fi connection.
- ❑ Consider using a Virtual Private Network (VPN) when in public.[52]
- ❑ Secure your home router. Steps for doing so are available on the Federal Trade Commission's website.[53]
- ❑ Disable Bluetooth connections on devices when not in use.
- ❑ Watch out for "phishing" scams where 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, links, pop-up windows, texts, or over the phone - and only contact entities by means you know to be legitimate. For example, if you receive a call purportedly from your bank's security department, don't give out information. Instead, call the number on your bank card and ask for the security department.
- ❑ Use credit cards instead of debit cards for all online and in-person purchases if possible. Consumers have more legal protections against fraud with credit cards and can also avoid having to wait for stolen funds from checking accounts to be replenished. Consider only carrying debit cards for trips to the ATM or cash-back transactions.
- ❑ Sign up for your "my Social Security" (MySSA) account.[54] This will help prevent a scammer from opening an account in your name and changing your direct deposit information to his or her own checking account. A credit freeze on your Equifax credit report will also block the creation of a MySSA account because the Social Security Administration uses Equifax credit reports for identity verification.
- ❑ Dispose of your old computers and mobile devices safely to keep data out of the wrong hands. You'll want to look up steps for your specific device, but below are basic steps.
  For computers: Save data you want to keep and transfer, "wipe" or overwrite your hard drive many times, and keep it out of the landfill by recycling, donating, or reselling it.[55] (Deleted files can still be recovered if you don't wipe your hard drive clean many times.) For mobile devices: Backup your phone, reset your device, remove or erase SD & SIM cards, and keep it out of the landfill by recycling, donating, reselling, or trading it.[56]

ID Theft Prevention for Offline Activity

- ❑ 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. If someone calls claiming to be from your bank security department, it's best to hang up and call the number on your card.
- ❑ Lock your records and financial documents at home.
- ❑ Lock your mailbox if it is lockable.
- ❑ Shred documents containing personal information (name, account numbers, any part of your social security number, and birthdate) before throwing them away.
- ❑ Opt-out of pre-approved (pre-screened) credit & insurance offers. 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 where by law you can opt out of receiving these offers for five years or permanently. You can also opt back in any time.[57] Note that this action only slows credit card and loan offers as only credit bureaus are subject to this rule. Airlines or retailers or others you do business with are not.
- ❑ Use the chip side of chip enabled cards, instead of the magnetic strip side, for in-person purchases whenever possible. Beware devices called skimmers[58] and shimmers[59] that criminals install on ATMs and card readers at checkout lines or gas pumps to steal your credit card information. When using ATMs and card readers, look and touch for signs of tampering, such as mismatched colors or loose parts. Always cover your hand while hand typing a PIN, and avoid using ATMs in secluded locations. ATMs at banks are the least likely to have skimmers.
- ❑ Use credit cards instead of debit cards for online and in-person purchases if possible. Consumers have more legal protections against fraud with credit cards and can also avoid waiting for stolen funds from checking accounts to be restored.
- ❑ Watch out for "phishing" scams where 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, links, pop-up windows, texts, or over the phone - and only contact entities by means you know to be legitimate. For example, if you receive a call purportedly from your bank's security department, don't give out information. Instead, call the number on your bank card and ask for the security department.
- ❑ Place credit freezes on your credit reports. The "Credit Freezes: How to Prevent New Account Identity Theft" section of this report explains how to freeze your credit reports.
- ❑ File your taxes as soon as possible to help prevent tax refund fraud. A fraudster can still file taxes in your name even if you're not required to file taxes or aren't eligible for a refund. Also, some people qualify for an Identity Protection (IP) PIN that must be entered before a tax filing can be submitted. The IP PIN is available to identity theft victims and is also currently offered to all taxpayers in Florida, Georgia, and Washington, D.C., as part of a pilot program.[60]

- ❑ Protect your deceased loved ones from identity theft by notifying appropriate institutions of their deaths.[61]

Detecting Identity Theft

- ❑ Check your monthly statements for unauthorized charges. Be suspicious of phone calls about surprise debts.
- ❑ Sign up to receive email and/or text notifications of account activity and changes to account information.
- ❑ Instead of paying for over-priced subscription credit monitoring, use your free annual credit reports 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 credit bureaus, 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 that accounts have not been opened without your knowledge. Free credit reports are available online at **AnnualCreditReport.com**, by phone at 1-877-322-8228, or by mail.[62] There are other non-official sites that offer free reports too. Beware of sites that promise free reports and credit 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 know that the credit scores on those sites are most likely not FICO scores as used by most creditors.
- ❑ There are many other consumer reporting companies besides the three big nationwide credit bureaus that specialize in collecting other types of information about you, including bounced check activity, criminal and other public records, employment information, insurance claims, and tenant history.[63] Requesting free reports with these specialty bureaus every year could help you spot various fraudulent activities done in your name. Note that many of these companies will not have files on you at all. For example, if you've never had a bank account closed for "bounced check activity," it is likely that you won't have files at bounced check specialty bureaus.
- ❑ Sign up for your "my Social Security" (MySSA) account. Even if you don't receive social security benefits yet, checking your MySSA account can help you spot changes to your personal information that might indicate thieves trying to claim your benefits over the phone.[64]
- ❑ Request your driving record to help spot traffic violations committed in your name.
- ❑ Sign up for online accounts with your health care and insurance providers to monitor any fraudulent services on your statements.
- ❑ Be alert to notices about a tax return already filed, additional taxes you owe, refund offsets, collection for a year you didn't file, or records showing income from an employer for whom you did not work.
- ❑ Check if your online accounts have been hacked. Have I Been Pwned is a free tool you can use to check whether your online accounts may have been compromised in data breaches.[65]

Resolving Identity Theft

- ❑ Take the following steps to resolve new account identity theft:

  Step 1: Notify your financial institutions. If you discover that your wallet, checkbook, credit card, or other sensitive information has been lost or stolen, immediately notify the issuing bank, credit card issuer, or relevant institution to close all existing accounts.

  Step 2: Get copies of your credit reports and place fraud alerts on them. If you haven't already, it's time to get credit freezes.

  Step 3: File an Identity Theft Report. If you suspect identity theft, report it to the Federal Trade Commission using the online complaint form at identitytheft.gov or by calling 1-877-ID-THEFT.

  Step 4: You might decide to file a police report.

- ❑ Visit **Identitytheft.gov**, the government's official website that will walk you through clear checklists of actions you can take to recover from new account identity theft and other types of fraud.[66]

Credit Freezes: How to Prevent New Account Identity Theft

Defense against any kind of identity theft starts with vigilance about protecting your personal information by taking steps such as creating secure passwords, keeping your social security number private, and shredding personal documents.

However, if and when someone does steal your information, there are a variety of ways it can be used, depending on what was taken. One of those uses is known as new account identity theft, where someone opens a new account in your name and then proceeds to rack up a ton of debt. New account identity theft can be prevented by getting security freezes, also known as credit freezes.

What Are Credit Freezes & Why Should I Get Them?

A credit freeze blocks potential creditors such as a credit card company, a cell phone company, or a lender from viewing your credit report, which shows your credit history. Most creditors will not issue new credit to a customer if they cannot see that customer's credit report or the credit score derived

from it from at least one of the three big nationwide consumer reporting agencies - Equifax, Experian, and TransUnion. (Consumer reporting agencies are also known as credit bureaus.) By blocking creditors from accessing your credit report, you're stopping identity thieves who apply for new accounts in your name with your stolen Social Security number.

Credit freezes do not affect your ability to use existing credit you already have, such as a credit card or loan. Nor do freezes affect your credit score. In fact, freezes help protect your score by preventing your credit from being negatively scored if someone racks up debt in your name.

You can easily remove a freeze or "thaw" your credit report when you want to apply for new credit. Freezes can be temporarily or permanently removed when you want.

Because creditors run credit checks with any one or a combination of the three big credit bureaus, you need to block access to your reports with all three.

What Are the Differences Between Credit Freezes, Credit Locks, Credit Monitoring, and Fraud Alerts?

Credit locks offered by the credit bureaus appear to block access to credit reports the same way that credit freezes do. Therefore, freezes and locks both deny thieves the ability to open fake accounts in your name.

However, freezes are a right mandated by law, while locks are conditional on terms of use agreements that are set by the credit bureaus and could change at any time. Your rights as a consumer are on stronger ground with freezes. Whether you chose to get freezes or locks, remember you'll need to get them at all three national credit bureaus.

Fraud alerts don't block access to your credit reports, but they do notify creditors that they should try to verify your identity before opening a new account in your name. If you choose not to block access to your reports at the three main credit bureaus, you should at least place fraud alerts on your reports.[67]

Credit monitoring alerts you to changes to your credit reports, which can help you spot unauthorized credit accounts opened in your name. Credit monitoring can only help *detect* new account identity theft after it has already occurred, not prevent it.

How Much Do Freezes Cost And When Do They Become Free Nationwide?

All 50 states and the District of Columbia have their own laws that determine the maximum amount that the credit bureaus can charge for credit freezes, temporary removals or "thaws," and permanent removals.[68]

Due to a wave of new state laws passed during 2018 in response to last year's massive Equifax data breach, getting and removing credit freezes at the three big credit bureaus is currently free in 23 states.[69] In the other states, freezes cost between $3-10 at each bureau. There is also a $2-12 fee in those states for unfreezing your credit report at each bureau. You can look up the fees for your state on our interactive map.[70] Some of those states offer freezes for free to consumers under 16 and over 65. Additionally, all states provide free freezes if you're already a victim of ID Theft.

As of the date of the updated version of this document, Equifax is not charging for freezes in any state.

A new federal law will eliminate fees for credit freezes across the country at all big three credit bureaus on September 21st, 2018.[71]

Do I Need to Freeze My Report with Other Credit Reporting Agencies?

As the Consumer Financial Protection Bureau lists, there are many other consumer reporting companies besides the three big nationwide providers of consumer reports.[72] Some websites have recommended getting freezes with Innovis and ChexSystems, but as far as we know, their reports are not used by creditors for credit approvals.

However, some news outlets have reported fraudulent accounts being opened by cell phone companies using credit reports provided by the National Consumer Telecommunications & Utilities Exchange (NCTUE).[73] **We therefore also recommend freezing your credit report at NCTUE, in addition to at the big three credit bureaus.**

How to Freeze (and Unfreeze) Your Credit Reports

- ❑ You can place freezes online, over the phone, or in writing (info provided below)
- ❑ You will receive a PIN for your credit freeze with each bureau. You will use this PIN when you want to unfreeze your credit report to apply for new credit.

- ❑ If you want to temporarily lift a freeze because you are applying for credit, 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 particular creditor or for a specific period of time, from one day to one year.
- ❑ 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 that was assigned to you when you froze your report, so make sure to keep your PIN in a safe, memorable place where you can quickly retrieve it when needed. It can also take up to three days of receipt of your request if you make it via postal mail.

Equifax

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

Phone: 1-800-349-9960 (automated), 1-888-298-0045 (live operator)

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.

TransUnion

Online: https://www.transunion.com/credit-freeze/place-credit-freeze

Phone: 888-909-8872

Mail: TransUnion LLC, P.O. Box 2000, Chester, PA 19016

National Consumer Telecommunications & Utilities Exchange

Online: https://www.exchangeservicecenter.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Phone: 1-866-349-5355

Mail: NCTUE Security Freeze P.O. Box 105561 Atlanta, GA 30348

Protect Your Online Privacy

Although protection from identity theft is largely about data security, privacy also plays an important role. Data security and privacy often go hand-in-hand with each other. Privacy generally refers to the control or choice you have over how your personal information is used or shared. Data security refers to the measures put in place to protect that control and make sure data is used as intended.[74]

Use this checklist to help you control how your personal information is used or shared online.

- ❑ Cover the camera on your laptop to prevent hackers from watching and recording you.
- ❑ Consider your options for blocking websites, advertisers, and others from tracking your online activity on your computer, including: adjusting your cookies settings on your browser, installing a tracking blocker for your web browser, or opting out of targeted advertising.[75] Note that "private browsing" settings by themselves still allow your activity to be communicated to third-parties *during* a browsing session.
- ❑ Consider your options for blocking advertisers from tracking your online activity on your mobile device, including turning off ad tracking and resetting "device identifiers."[76] You can also research ways of controlling ad tracking on your other smart devices, such as internet connected entertainment systems.
- ❑ Check the privacy settings on your mobile device to control the access that different apps have to your personal information, including location, personal contacts, photos, calendar, and health data.[77] Many apps have the ability to track your location **even when you're not using them**.
- ❑ Check your privacy and other settings in your Facebook account to control tools such as face recognition, location history, and ad preferences.[78]
- ❑ Check your privacy settings in your Google account to control tools such as the collection of your web searches and other activity and the ads you see.[79]
- ❑ Check your privacy settings in your other apps and social media accounts.

Identity Theft & Privacy Resources

- AnnualCreditReport.com (Phone and mail options available.[80])
- Consumer Federation of America's IDTheftInfo.org[81]

- Consumer Reports' "66 Ways to Protect Your Privacy Right Now"[82]
- Electronic Frontier Foundation's HTTPS:// EVERYWHERE[83]
- Facebook's privacy and security page[84]
- Google's privacy and security page[85]
- Have I Been Pwned[86]
- Krebs On Security[87]
- OptOutPrescreen.com[88]
- Privacy Rights Clearinghouse[89]
- The Federal Trade Commission's IdentityTheft.gov website[90] & Online Security tips[91]
- The Identity Theft Resource Center[92]
- The Social Security Administration's "my Social Security" website[93]
- U.S. PIRG's Identity Theft & Privacy Checklists[94]

Appendix A: Equifax's Offerings to Consumers in Response to its Data Breach

Equifax initially offered a package called TrustedID Premier to anyone, whether their info was lost or not, made up of five different products or services. The deadline for signing up for this package was January 31st, 2018, when this offer was replaced by a new offer called Lock & Alert. Both the original package and the newer offer fall short of protecting consumers.

TrustedID Premier

It doesn't hurt to use these services if you signed up for them. However, you should know they are limited and, at best, only alert you to identity theft after it has occurred. Therefore, we also recommend you freeze your credit reports with all three national credit bureaus and the National Consumer Telecom & Utilities Exchange.

Here are the five services and products included with TrustedID Premier and what the limitations of each are:

1. Copies of Your Equifax Credit Report
   Looking at your credit report is a good idea because you can spot unauthorized activity in your name. It's a good idea to check your credit report at all three bureaus, not just Equifax. You can request free copies of your credit report at all three bureaus at annualcreditreport.com, the official website authorized by the government for requesting these free reports.[95]

2. Credit Monitoring for One Year at All Three Nationwide Credit Bureaus

Credit monitoring alerts you to changes to your credit reports, which can help you spot unauthorized activity in your name. The types of stolen information, particularly social security numbers and dates of birth, can be used to commit new account identity theft against everyone whose info was breached. This means bad guys could open fraudulent credit accounts and rack up tons of debt in your name. Due to huge marketing pushes by credit monitoring services that only alert consumers to fraud after the fact, most Americans are not aware that they can actually prevent id thieves from opening new credit accounts in their names in the first place by placing freezes on their credit accounts at all three national credit bureaus. Credit freezes help prevent new account identity theft because they keep potential creditors from seeing consumer credit history, without which new accounts are typically not opened. Equifax's package includes credit monitoring at all three bureaus for only one year. Equifax should make it clear that monitoring only alerts people to fraudulent activity after it has occurred, and they should offer it indefinitely, not just one year. The stolen information does not have a shelf life.

3. Equifax Credit Report Lock

   Equifax's package also includes something like a credit freeze, something they call a "credit report lock," but only for Equifax reports. Bad guys could still try to open credit accounts with companies that use the other two credit bureaus for credit checks. So, a freeze or "lock" with only one bureau is incomplete protection. Equifax should make clear the benefits of the credit freeze. You're better off getting actual credit freezes with all three bureaus, not the one "lock" with Equifax. The "Credit Freezes: How to Prevent New Account Identity Theft" section of this report explains how to freeze your credit reports.

4. Social Security Number Monitoring

   Equifax advertises this service as searching "suspicious websites for your Social Security number." This service by itself wouldn't' hurt, but it's better to act as if your social security number is already out there and take the actions that can help prevent and detect use of it against you. Again, the most preventable identity theft using your social security number is new account identity theft. You're best off getting credit freezes with all three nationwide bureaus and the NCTUE. See other proactive steps you can take, starting with pages 9 and 17 of this report.

5. $1M 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.

Lock & Alert

January 31st was the launch date for Lock & Alert, a service that lets consumers lock and unlock their Equifax credit reports indefinitely for free. This service only blocks access to Equifax credit reports, not credit reports at the other two national bureaus.

Locks appear to block access to credit reports the same way freezes do. Freezes and locks both deny thieves the ability to open any fake accounts in your name. However, freezes are a right mandated by law and not conditional on terms set by companies.

Appendix B: Number of ID Theft Reports from 2017 in the Federal Trade Commission's Sentinel Database

The Sentinel is an online secure database of reports by consumers about problems in the marketplace. It is made up of reports submitted to the Federal Trade Commission, other federal agencies, state agencies, and other organizations.[96] Full details and individual reports are only available to law enforcement. Below is a table of numbers of reports in 2017 by types of ID theft available in the Sentinel, as provided by the FTC.[97]

Table B-1. Number of ID Theft Reports in 2017 by Type of Theft

Theft Type	Theft Subtype	# of Reports	% of All Types of Theft	% Difference from Previous Year
Credit Card Fraud	New Accounts	105,209	22.3%	3%
	Existing Accounts	34,260	7.3%	20%
Employment or Tax-Related Fraud	Tax Fraud	62,682	13.3%	-46%
	Employment or Wage-Related Fraud	21,214	4.5%	23%
Phone or Utilities Fraud	Mobile Telephone - New Accounts	26,062	5.5%	18%
	Utilities - New Accounts	22,064	4.7%	-2%
	Landline Telephone - New Accounts	6,034	1.3%	150%
	Mobile Telephone - Existing Accounts	4,675	1.0%	11%

Theft Type	Theft Subtype	# of Reports	% of All Types of Theft	% Difference from Previous Year
	Landline Telephone - Existing Accounts	1,162	0.2%	109%
	Utilities - Existing Accounts	1,107	0.2%	-5%
Bank Fraud	Debit Cards, Electronic Funds Transfer, or ACH	23,229	4.9%	19%
	New Accounts	17,487	3.7%	2%
	Existing Accounts	12,754	2.7%	24%
Loan or Lease Fraud	Business\Personal Loan	11,129	2.4%	3%
	Auto Loan\Lease	9,935	2.1%	43%
	Student Loan	5,717	1.2%	121%
	Real Estate Loan	4,411	0.9%	3%
	Apartment or House Rented	3,625	0.8%	39%
Government Documents or Benefits Fraud	Government Benefits Applied For\Received	17,793	3.8%	34%
	Other Government Documents Issued\Forged	5,396	1.1%	-31%
	Driver's License Issued\Forged	3,768	0.8%	-14%
	Passport Issued\Forged	520	0.1%	-15%
Other Identity Theft	Other	39,667	8.4%	6%
	Online Shopping or Payment Account	8,685	1.8%	43%
	Email or Social Media	7,645	1.6%	35%
	Medical Services	6,805	1.4%	40%
	Evading the Law	4,127	0.9%	18%
	Insurance	2,952	0.6%	19%
	Securities Accounts	1,634	0.3%	18%
Total		**471,748**		

Appendix C: Examples of Identity Theft Problems Reported by Consumers to the Consumer Financial Protection Bureau

The Consumer Financial Protection Bureau (CFPB) was established in 2010 as part of comprehensive Wall Street reform in the wake of the worst financial crisis in decades. To help accomplish its mission of protecting consumers in the financial marketplace, the CFPB created and made available to the public

the Consumer Complaint Database. Due to the public nature of the database, there is a 97% response rate by companies,[98] and many of the complaints result in monetary and non-monetary relief for consumers (such as getting mistakes or fraudulent activity on credit reports resolved.)

7,418 consumer complaints to the Consumer Financial Protection Bureau from September 8th, 2017 through August 17th, 2018, were categorized as problems with credit inquiries on credit reports not recognized by the consumer, debt as a result of identity theft, or credit cards opened as a result of identity theft or fraud.[99] 3,372 of these complaints include written explanations or "narratives" about the problems experienced by consumers. Breakdowns of complaints to the CFPB specifically against Equifax since its breach are available in a report released by Senators Brian Schatz (HI), Elizabeth Warren (MA), and Robert Menendez (NJ).[100]

Below is a sampling of complaint narratives against the three national credit bureaus that shows signs of identity theft in the aftermath of the Equifax data breach. Although it's not possible to confirm the cause of these individual cases of identity theft, these explanations give us a better understanding of the personal impacts of identity theft, of which the Equifax breach has definitely put consumers at risk. The CFPB redacts information that could potentially be used to identify customers and replaces it with "XXXX." Other than the redactions, these narratives are presented as they were originally submitted by the consumers.

All of the following complaints were responded to by the companies with "non-monetary relief," suggesting that they removed fraudulent credit inquiries from these consumers' credit reports. Disappointingly, Mick Mulvaney, the temporary director of the CFPB, is considering hiding the database from public view.[101] These results made possible by the public nature of the database demonstrate the importance of keeping the database public.

This narrative complaint against TransUnion from a consumer in California illustrates the fear and real impacts caused by identity theft.[102]

> *On XX/XX/XXXX I went on XXXX XXXX and it stated a message that I may have been effected in recent breaches and to put in my info to check and see. Once I did that it stated just by my email which I use for everything I was affected by 3 breaches which makes sense because I have been getting unknown inquiries from sources that I dont recongnize. Its really scary to know Im not protect by the 3 credit bureaus. I called back at the beginning of XX/XX/XXXX but got the generic message of inquiries being factual and no actual work was put into investigating the inquiries and ultimately removing them. My score has plummeted since then because I have over 40 inquiries and I have not authorized quite a few of them.*

This narrative complaint against Experian from a consumer in Florida shows signs of attempted identity theft in the wake of the Equifax data breach.[103]

My credit report now has 42 inquires all of which are fraudulent. i have advised Experian XXXX and XXXX All of these companies referred me back to the creditors that submitted the request who referred me back to the companies. I do believe the spike in these request came from the data breach i want these inquiries removed XXXX XXXX Never Applied XXXX XXXXNever Applied XXXX XXXX- No Knowledge XXXX XXXX - this creditor has attempt to pull my credit 14 time in the past 6 months obviously it is not me XXXX- Never Applied XXXX XXXX Was never my card i disputed this account and it was removed

This narrative complaint against Equifax from a consumer in Ohio shows the negative effects fraudulent credit inquiries can have on credit scores.[104]

I have inquiries on my credit report that are not mine, I know that there was a data breach and my personal information was compromised. I have a whole list of inquires that were made by an unknown source. These inquires were not made by me. I am a victim and it has truly hurt my credit score. I have provided the list of inquiries that were not mad by me. XXXX XXXX XXXX-XX/XX/XXXX XXXX/XXXX- XX/XX/XXXX XXXX/XXXX- XX/XX/XXXX XXXX XXXX- XX/XX/XXXX XXXX XXXX - XX/XX/XXXX XXXX XXXX XX/XX/XXXX XXXX XXXX- XX/XX/XXXX XXXX XXXX- XX/XX/XXXX XXXX XXXX- XX/XX/XXXX XXXX XXXX XXXX- XX/XX/XXXX XXXX XXXX- XX/XX/XXXX XXXX/XXXX-XX/XX/XXXX XXXX XXXX XXXX - XX/XX/XXXX XXXX XXXX XXXXXXXX- XX/XX/XXXX XXXX XXXX XXXX -XXXX XXXX XXXX XXXX XXXX/XXXX- XX/XX/XXXX XXXX/XXXX- XX/XX/XXXX, XX/XX/XXXX XXXX XXXX XXXX - XX/XX/XXXX XX/XX/XXXX

This narrative complaint against Equifax from a consumer in Texas shows the frustration of having to go through hoops to resolve fraud on one's credit report.[105]

Starting in XXXX, I began sending certified letters to Equifax this year in regards to unauthorized inquiries. I noticed that my mail box was flooded with denial letters for things I had no knowledge of and did not authorize. In my attempts to have the situation resolved, I have received a generic response that the inquiries are of factual record and will remain on file for 2 years. I do n't understand how this information is of factual record when I did not authorize them and are fraudulent. I was informed by a Equifax employee that I was affected by the breach and was told they would dispute the information. However, I received another letter that stated " contact the creditors ". I am disappointed in Equifax as well as their customer service. This is XXXX company that truly can not be trusted.

Endnotes

[1] Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (press release), 7 September 2017.
[2] Equifax, *Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident* (press release), 2 October 2017.
[3]Equifax, *Equifax Releases Updated Information on 2017 Cybersecurity Incident* (press release), 1 March 2018.
[4] The Apache Software Foundation, *The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache® Struts™ Exploit* (media alert), 14 September 2017.
[5] See note 1.
[6] Ron Lieber, "How to Protect Yourself After the Equifax Breach," *The New York Times,* 16 October 2017.
[7] Equifax, *A Progress Update for Consumers* (press release), 8 September 2017.
[8] Ibid.
[9] Maggie Astor, "Someone Made a Fake Equifax Site. Then Equifax Linked to It," *The New York Times,* 20 September 2017.
[10]The Office of Senator Elizabeth Warren, *Warren Unveils New Investigative Report Uncovering Equifax's Failure to Protect Americans' Personal Data* (press release), 7 February 2018.
[11] Equifax, *Form 8-K Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934*, 4 May 2018, 2.
[12] Federal Trade Commission, *Consumer Sentinel Network Data Book 2017,* March 2018.
[13] Consumer Financial Protection Bureau, *Consumer Complaint Database,* accessed at bit.ly/2oCokLj, 31 August 2018. Also, breakdowns of complaints to the CFPB specifically against Equifax since its breach are available in a report released by Senators Brian Schatz (HI), Elizabeth Warren (MA), and Robert Menendez (NJ): The Office of Senator Elizabeth Warren, *Warren, Menendez, Schatz Reveal that CFPB Received More than 20,000 Consumer Complaints following Equifax Breach,* 30 April 2018.
[14] AnnualCreditReport.com, accessed at www.annualcreditreport.com, 31 August 2018.
[15] Federal Trade Commission, *Free Credit Reports*, accessed at www.consumer.ftc.gov/articles/0155-free-credit-reports, 31 August 2018.
[16] Kathy Kristof, "This Equifax Credit Database Can Boost Your Risk of Phone Fraud," *MoneyWatch,* 16 May 2018.
[17] Social Security Administration, *Create Your Personal My Social Security Account Today,* accessed at www.ssa.gov/myaccount/, 31 August 2018.
[18] Florida, Georgia, and Washington, D.C. were chosen for the pilot program because those locations have the highest per capita percentage of tax related identity fraud. Internal Revenue Service, *Get an Identity Protection Pin (IP Pin),* accessed at www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin, 31 August 2018.
[19] Jeff Blyskal, A Credit Freeze Won't Help With All Equifax Breach Threats, *Consumer Reports*, 13 October 2017.
[20] Consumer Financial Protection Bureau, *List of Consumer Reporting Companies*, 2018.
[21] Federal Trade Commission, *Report Identity Theft and Get a Recovery Plan,* accessed at www.identitytheft.gov/, 31 August 2018.
[22] Federal laws regarding the collection, use, and protection of consumer credit data that are enforced by the CFPB and FTC are listed on page 11:
Equifax, *Form 10K Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934,* 1 March 2018, 11.
[23] The state agencies that are part of this agreement are the Alabama State Banking Department, California Department of Business Oversight, Georgia Department of Banking and Finance, Maine Bureau of Consumer Credit Protection, Massachusetts Division of Banks, New York State Department of Financial Services, North Carolina Office of Commissioner of Banks, and Texas Department of Banking. Multi-State Regulatory Agencies, *Consent Order*, 25 June 2018.
[24] Alex Soderstrom, "Former Equifax Worker Pleads Guilty to Insider Trading Related to Hack," *Atlanta Journal-Constitution,* 23 July 2018.
[25]Michael Kanell, "Ex-Equifax Exec is Arraigned and Freed; Pleads Not Guilty," *Atlanta Journal-Constitution,* 15 March 2018.
[26] Ron Lieber and Stacy Cowley, "Trying to Stem Fallout From Breach, Equifax Replaces C.E.O." *The New York Times,* 26 September 2017.
[27] Equifax, *Form 10-K Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934,* 1 March 2018.
Explanation about its spending related to the breach:
Equifax, *Form 8-K Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934,* 25 July 2018, 10.
[28] Energy & Commerce Committee, *Oversight of the Equifax Data Breach: Answers for Consumers*, 3 October 2017.
Subcommittee on Privacy, *Technology and the Law, Equifax: Continuing to Monitor Data-Broker Cybersecurity*, 4 October 2017.
Financial Services Committee, *Hearing Entitled Examining the Equifax Data Breach*, 5 October 2017.
[29] Committee on Commerce, Science, and Transportation, *Protecting Consumers in the Era of Major Data Breaches*, 8 November 2017.

[30] Financial Services Committee, *Continuation of Hearing Entitled Examining the Equifax Data Breach*, 25 October 2017. Financial Services Committee, *Hearing Entitled Data Security: Vulnerabilities and Opportunities for Improvement*, 1 November 2017. Energy & Commerce Committee, *Identity Verification in a Post-Breach World*, 30 November 2017.
[31] Financial Services Committee, *Hearing Entitled Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime,* 7 March 2018.
[32] This draft bill exempts firms already covered under the Gramm-Leach-Bliley Act of 1999 (GLBA) which includes all banks and "other financial institutions," including Equifax and the other big credit bureaus. However, under GLBA, they do not have to provide breach notices, only breach response plans.
[33] If these industries want a uniform standard, which is often the selling point behind this and other bad federal data breach bills we've seen before, they could take the strongest state laws and apply them to all consumers across the country - they don't need Congress for that. This is simply an attempt to set weaker federal laws as the ceiling for what states can do to protect consumers.
[34] The Office of Elizabeth Warren, *Warren, Warner Unveil Legislation to Hold Credit Reporting Agencies Like Equifax Accountable for Data Breaches* (press release), 10 January 2018.
[35] Equifax, *Equifax Releases Second Quarter Results* (press release), 25 July 2018.
[36] Financial Services Committee, *Subcommittee Examines Legislation to Improve Regulations,* 7 September 2017.
[37] For a discussion of the bills, see Edmund Mierzwinski, "U.S. House Considers Trojan Horse Bill to Weaken Credit Bureau Laws," *The Huffington Post*, 6 September 2017.
[38] Congress, *Economic Growth, Regulatory Relief, and Consumer Protection Act*, 24 May 2018.
[39] S2155 (Crapo-ID) became Public Law 115-174 on 24 May 2018, available at https://www.congress.gov/bill/115th-congress/senate-bill/2155 See Mike Litt, *U.S. PIRG Statement on House Passage of Bank Lobbyist Act (S2155)*, 22 May 2018, available at uspirg.org/news/usp/us-pirg-statement-house-passage-bank-lobbyist-act-s2155.
[40] Equifax, *Form 10-Q Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934,* 26 July 2018, 21.
[41] Equifax, *Motion to Dismiss Consolidated Consumer Class Action Complaint*, 27 June 2018.
[42] Anthony Giorgianni, "Should You Participate in a Class Action Against Equifax?," *Consumer Reports,* 19 September 2017.
[43] Nate Raymond, "Massachusetts Can Sue Equifax over Data Breach, Judge Rules" *Reuters,* 4 April 2018.
[44] See note 39.
[45] "Attorney General Sues Equifax Regarding Data Breach," MetroNews, 12 April 2018.
[46] Lisa Madigan, Office of the Attorney General State of Illinois, *Committee Leaders Letter,* 19 March 2018
[47] Offices of the Attorneys General of Connecticut, District of Columbia, Illinois, and Pennsylvania, *Letter to Equifax*, 19 September 2017.
[48] "66 Ways to Protect Your Privacy Right Now", *Consumer Reports,* 21 February 2017.
[49] Electronic Frontier Foundation, *HTTPS:// Everywhere*, accessed at www.eff.org/https-everywhere, 31 August 2018.
[50] Federal Trade Commission, *Securing Your Wireless Network*, September 2015.
[51] Federal Trade Commission, *Tips for Using Public Wi-Fi Networks*, March 2014.
[52] Federal Trade Commission, *Virtual Private Network (VPN) apps*, March 2018.
[53] See Note 50.
[54] See note 17.
[55] Federal Trade Commission, *Disposing of Old Computers*, September 2011.
[56] Federal Trade Commission, *Disposing of Your Mobile Device*, June 2012.
[57] OptOutPrescreen.com, accessed at www.optoutprescreen.com/, 31 August 2018.
[58] Max Eddy, "How to Spot and Avoid Credit Card Skimmers," *PC Magazine*, 15 February 2018.
[59] Brian Krebs, *ATM 'Shimmers' Target Chip-Based Cards*, 27 January 2017.
[60] See note 18.
[61] Sid Kirchheimer, "Protecting the Dead from Identity Theft," AARP Bulletin, accessed at www.aarp.org/money/scams-fraud/info-03-2013/protecting-the-dead-from-identity-theft.html, 31 August 2018.
[62] Federal Trade Commission, *Annual Credit Report Request Form,* accessed at www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf, 31 August 2018
[63] See note 20.
[64] See note 17.
[65] Troy Hunt, *Have I Been Pwned*, accessed at haveibeenpwned.com/, 31 August 2018.
[66] See note 21.
[67] Federal Trade Commission, *Place a Fraud Alert*, September 2017.
[68] PIRG worked on the first security freeze law in California and then promoted it nationwide, state by state. We wrote a model data breach notice and security freeze law with Consumers Union/Consumer Reports and promoted it with 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. See U.S. Public Interest Research Group and Consumers Union, *The Clean Credit and Identity Theft Protection Act: Model State Laws*, November 2005.
[69] Several state PIRGs helped work on free freeze legislation, including in California, Colorado, Illinois, Maryland, Massachusetts, Oregon, and Washington State.
[70]U.S. PIRG, *Credit Freezes by State*, accessed at bit.ly/pirgfreezemap, 31 August 2018.
[71] See note 38.
[72] See note 20.
[73] See note 16.
[74] Laura Moy, Center on Privacy & Technology at Georgetown Law, *Statement Before the Financial Services Committee Hearing on Continuation of Hearing Entitled Examining the Equifax Data Breach*, 25 October 2017, 18.
[75] Federal Trade Commission, *Online Tracking*, June 2016.
[76] Ibid.
[77] Federal Trade Commission, *Understanding Mobile Apps*, February 2017.
[78] Facebook, *Tools to Help You Control Your Privacy and Security on Facebook,* accessed at www.facebook.com/privacy/, 31 August 2018.
[79] Google, *Privacy*, accessed at privacy.google.com, 31 August 2018.
[80] See note 15.
[81] Consumer Federation of America, *IDTheftInfo.org*, accessed at idtheftinfo.org/, 31 August 2018.
[82] See note 48.
[83] See note 49.
[84] See note 78.
[85] See note 79.
[86] See note 65.
[87] Brian Krebs, Krebs on Security, accessed at krebsonsecurity.com, 29 August 2018.
[88] See note 57.
[89] Privacy Rights Clearinghouse, accessed at www.privacyrights.org/, 31 August 2018.
[90] See note 21.
[91] Federal Trade Commission, *Online Security*, accessed at www.consumer.ftc.gov/topics/online-security, 31 August 2018.
[92] Identity Theft Resource Center, accessed at www.idtheftcenter.org/, 31 August 2018.
[93] See note 17.
[94] U.S. Public Interest Research Group, *Identity Theft and Privacy Checklists,* 3 August 2018.
[95] See note 14.
[96] See note 12.
[97] Federal Trade Commission, *Consumer Sentinel Network Data Book 2017: Identity Theft Reports by Type,* March 2018.
[98] Consumer Financial Protection Bureau, "Standing Up for You," accessed at www.consumerfinance.gov/, 31 August 2018.
[99] Although the Equifax breach was publicly announced on September 7th, 2017, narrative complaints about the breach first appeared in the Consumer Complaint Database on September 8th.
[100] See note 13.
[101] Donna Borak, Sara Ganim, Ellie Kaufman, Gregory Wallace, "Mulvaney's Long History with Key Consumer Tool Puts its Future in Doubt" *CNN Politics,* 23 August 2018.
[102] CFPB, *CFPB Consumer Complaint Database*, accessed at www.consumerfinance.gov/data-research/consumer-complaints/search/detail/2806069, 6 February 2018
[103] CFPB, *CFPB Consumer Complaint Database*, accessed at www.consumerfinance.gov/data-research/consumer-complaints/search/detail/2820217, 20 February 2018
[104] CFPB, *CFPB Consumer Complaint Database*, accessed at www.consumerfinance.gov/data-research/consumer-complaints/search/detail/2932374, 11 June 2018
[105]CFPB, *CFPB Consumer Complaint Database*, accessed at www.consumerfinance.gov/data-research/consumer-complaints/search/detail/2707473, 21 October 2017