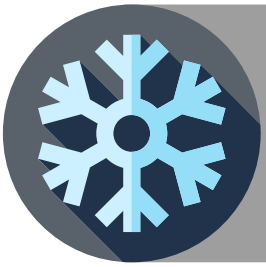
A Publication of the South Carolina Department of Consumer Affairs

IDENTITY THEFT

WHAT TO DO AFTER A SECURITY BREACH

Your Information has been Breached... What Now?

Page 2



Fraud Alerts, Freezes and ID Theft Protection Services, Oh My! So, What's the Difference?

Page 3

Security Freeze FAQs, Protecting Your Child's Identity and Tools to Consider.

Pages 4-5

Get in the Habit: Everyday Practices that Help You Avoid Identity Theft.

Page 6

Are YOU a Victim of Identity Theft? What to do.

Page 7

YOUR INFORMATION HAS BEEN BREACHED... WHAT NOW?

1 CONSIDER A SECURITY FREEZE AND FRAUD ALERT

Prevent scammers from opening new accounts using your information by placing a **FREE** security freeze on your credit reports. A security freeze puts your credit report on lockdown, limiting access to it without your OK, and lasts until you lift it.

A fraud alert will allow a business to pull your credit report, but only after taking extra steps to verify the applicant is really you.

2 MONITOR YOUR STATEMENTS

Make sure your bills and benefits, medical and financial statements are arriving on time and are correct. Identity thieves can use your info, like a social security number, the same way you do. Including to get:

- Government benefits
- Driver's License/ID
- Cell phones/utilities
- Medical benefits
- Tax Refund
- A Job

Find signs of identity theft? Flip to page seven for the next steps.

3 DEFEND AGAINST SCAMS

Scam artists use information from breaches to make their requests seem legit. Never reply to calls, texts, pop-ups, or e-mails that ask you for, or to verify, personal information.

Fraudsters may even pose as a monitoring service and send emails with subject lines or content like: "Identity Theft Alert" or "Your Score Has Dropped." Avoid clicking on links or downloading attachments from suspicious emails or texts.

4 INTERESTED IN A MONITORING SERVICE?

Think you might need some help keeping track of everything? Monitoring services (also called ID theft protection services) often offer to do what you can do yourself for free (see steps 1-3 above).

Just remember to research the company to ensure they are:

1. TRUSTWORTHY, RELIABLE, and LEGITIMATE.
2. Their services fit your needs.

Even if you enroll in a service, it doesn't take you out of the picture. You are the best tool you have for detecting identity theft.

WHO TO CONTACT:

SECURITY FREEZE: You MUST contact EACH credit reporting agency to place, thaw or lift the freeze.
FRAUD ALERT: You only need to contact one of the credit reporting agencies to place a fraud alert and they will notify the other two.

EQUIFAX	EXPERIAN	TRANSUNION
Online: equifax.com/personal/credit-report-services	***Online:*** experian.com/help	***Online:*** transunion.com/credit-help
Phone: (800) 685-1111	***Phone:*** (888) 397-3742	***Phone:*** (800) 680-7289

Having trouble finding what you need? Call us at (844) 835-5322.

SO, WHAT'S THE DIFFERENCE?

FRAUD ALERT:

What is it? Federal law gives consumers the right to place a fraud alert on credit reports for **FREE.** It alerts potential creditors pulling your report to take extra steps to verify your identity before issuing credit or services in your name.

How long will it last? Lasting one year, the alert entitles you to a free credit report from each of the three credit reporting agencies. A fraud alert can be renewed. But if you have proof you are a victim of identity theft, you can place an extended fraud alert that lasts 7 years.

Who do I contact? You only have to contact one of the credit reporting agencies, Equifax, TransUnion or Experian, and they'll notify the other two. See page two for contact info.

SECURITY FREEZE:

What is it? When a freeze is in place, a business that receives an application for products or services cannot access your credit report without your permission. Utilities, credit cards and insurance companies all commonly require a credit check. A freeze doesn't affect your existing lines of credit and will need to be thawed if you decide to apply for new credit or services.

How long does it last? The freeze lasts until **YOU** lift it. You can lift for a specified amount of time. After the time has elapsed, the freeze will go back into place. It can also be lifted permanently. When you place the freeze, you will receive a PIN number or password to use when you want to temporarily lift ("thaw") or permanently remove the freeze. Make sure to keep it in a safe place.

Who do I contact? Each of the three major credit reporting agencies. See page two for contact info.
If you are the caregiver for a minor or incapacitated adult, consider the protected consumer freeze. See page five for more information on how it works.

FREE ID THEFT PROTECTION SERVICES:

What is it? Identity theft protection services often include either credit report monitoring, identity monitoring, or resolution services…or a combination of those.

- Credit monitoring is when a third party monitors your credit reports for identity theft red flags.
- Identity monitoring is when a third party searches databases, chatrooms or "underground" websites for signs your information is in the hands of fraudsters.
- Resolution or recovery services are meant to assist you in the process of remedying an identity theft event.

How long will it last and who do I contact? Check the security breach notice you receive for more information on opting in and the duration of the service. If a service is not offered and you would like to have one, be sure to do your research and find the best fit for you.

✻**Remember:** *All of these tools are independent of one another. That means you MUST opt into them separately. The freeze and fraud alert only mitigate the effects of identity theft related to products or services where your credit report is viewed as part of the application process. Not all companies check credit reports.*

SECURITY FREEZE FAQS

COMMON QUESTIONS ABOUT THIS FREE ID THEFT PROTECTION TOOL.

DOES A SECURITY FREEZE ON MY CREDIT REPORT AFFECT MY CREDIT SCORE?

No. A security freeze does not affect your credit score. Lifting or removing the freeze does not affect your score either.

DOES PLACING A SECURITY FREEZE ON MY CREDIT REPORT STOP PRESCREENED CREDIT OFFERS?

No. Prescreened/ "preapproved" offers for credit and insurance can be stopped by calling 1-888-5-OPT-OUT (1-888-567-8688) or visiting www.optoutprescreen.com.

DOES A SECURITY FREEZE PREVENT ME FROM USING MY CREDIT CARDS?

No. A security freeze restricts access to your credit report to prevent new accounts or services from being opened in your name. It does not prevent you, or an identity thief, from using existing accounts/ cards.

WILL A SECURITY FREEZE PREVENT ME FROM PULLING MY OWN CREDIT REPORT OR ENROLLING IN CREDIT REPORT MONITORING SERVICES?

No. The freeze will not affect your ability to pull your own credit report or receive credit monitoring services. Businesses you currently have a relationship with can still access your report as well.

IS A SECURITY FREEZE THE SAME AS A CREDIT LOCK?

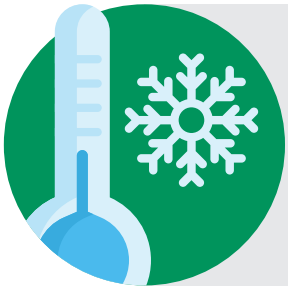
No. A security freeze is a free identity theft protection tool provided by law. A credit lock is a product offered by consumer reporting agencies that consumers can contract for, sometimes for a fee, and provides a similar effect of limiting access to a credit report. Because the lock is not provided for by law, who can access your credit report when a lock is in place may change as can other terms of the product, including fees. Legal protections for consumers when a lock goes awry are also unclear.

PROTECTING YOUR CHILD'S IDENTITY

STAY ON GUARD.

CHECK FOR A CREDIT REPORT.

Generally, children will not have a credit report unless an identity thief uses their information. A thief may use it for many years before the crime is discovered. Parents are encouraged to check to see whether their child has a credit report. Contact each of the three credit reporting agencies for information on how to request a search.



CONSIDER THE PROTECTED CONSUMER FREEZE.

A protected consumer freeze is **FREE** and available for children under the age of 16 and incapacitated adults. The freeze allows a parent, guardian or representative of the consumer to create a credit file in the person's name and place a freeze on it, helping to deter identity theft. Remember to place your request with **EACH** of the three credit reporting agencies. You will be asked to give proof of the protected consumer's identity, your identity, and proof of authority to act on behalf of the protected consumer.

To request a credit report search or place a freeze, see page two for credit reporting agency contact information. *Having trouble finding what you need? Call us at (844) 835-5322.*

ACCOUNT MONITORING TOOLS

CONSIDER THESE TOOLS FOR PROTECTING YOUR ACCOUNTS.

ACCOUNT ALERTS.

Most banks and credit unions offer alert programs to help you easily track your accounts. You can setup alerts for purchases, low balances, available credit and more. The options are almost endless because you can tailor them to your liking. You can also choose how you'd like to receive the alert (ie: text/email)

SIGN UP FOR MY SOCIAL SECURITY.

This online tool lets anyone still working view estimates of future retirement, disability and survivor benefits, earnings and Social Security and Medicare taxes you've paid. If an identity thief is using your SSN to work, their earnings may show up in your account. Once you create an account, it prevents others from creating an account in your name. Visit www.ssa.gov/myaccount.

LOGIN PROTECTIONS.

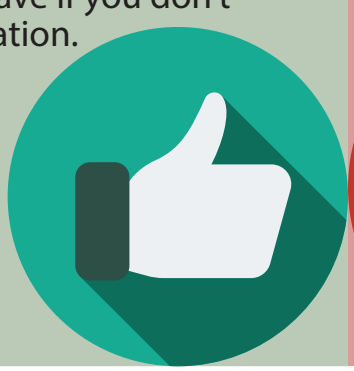
Logging in online? Research any extra security options offered such as: **(1) two-factor authentication** - requires an extra step to verify it's you attempting to login, and **(2) login alerts** - give you notice when someone logs into your account from a device you don't normally use.

GET IN THE HABIT

EVERYDAY PRACTICES THAT HELP YOU AVOID IDENTITY THEFT.

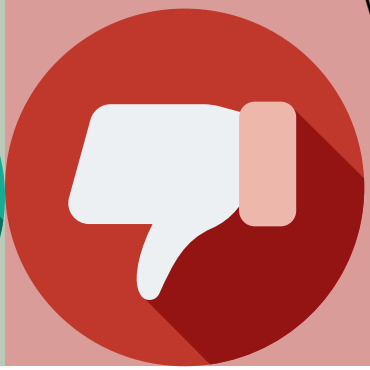
DO THESE THINGS:

- Shred items that include personal information before getting rid of them.
- Before sharing information at the doctor's office, your child's school or a business ask: why they need it, how it will be protected, and what options you have if you don't want to give the information.
- Take those outgoing bills to a USPS blue mailbox.
- Use anti-virus software and update it often.



DON'T DO THESE THINGS:

- Never release your personal identifying information (PII) to someone you don't know. That means keep your SSN, date of birth and financial account numbers to yourself!
- Don't use your debit card when shopping online.
- Don't use public wi-fi to make purchases or login to your mobile banking site.
- Don't carry around your social security card or birth certificate.



PASSWORDS AND SECURITY QUESTIONS

Make sure security questions cannot be answered with information found on your social media accounts. Use strong, creative passwords (uppercase, lowercase and special characters) and don't share them with anyone. Don't use the same passwords or security questions for multiple accounts.

REQUEST YOUR FREE ANNUAL CREDIT REPORT

It's easy, FREE and you get three each year: one from Equifax, Experian and TransUnion. Just call: (877) 322-8228 or visit www.annualcreditreport.com

LIKE TO SURF THE WEB, SHOP, BANK OR CONNECT ONLINE?

Take stock of the personal information you share online. Once it's shared, it is difficult—or near impossible—to erase. Review privacy settings to see who can see your information and make any needed changes. Read privacy policies before signing up to see what the business does with your info.

STAY ON GUARD ONLINE!

ARE YOU A VICTIM OF IDENTITY THEFT?

AFTER PLACING A FRAUD ALERT AND A SECURITY FREEZE ON YOUR CREDIT REPORTS:

1 CLOSE AFFECTED/FRAUDULENT ACCOUNTS AND DISPUTE THEM

- Notify the company ASAP and request a dispute form.
- Send the form certified mail, return-receipt requested.
- Once the dispute process is complete, ask for a letter that confirms the accounts and fraudulent debts are resolved.
- Keep copies of ALL correspondence.
- Are signs of fraud showing up on your credit report? Send a letter explaining the errors/mistakes to the 3 credit reporting agencies, too.

2 CONTACT SCDCA'S ID THEFT UNIT

The Identity Theft Unit offers specific tips for the type(s) of ID theft you are experiencing. If you're feeling overwhelmed, contact the Unit and fill out an intake form. Call (844) 835-5322 or visit www.consumer.sc.gov.

South Carolina Department of Consumer Affairs
IDENTITY THEFT UNIT
education. guidance. enforcement.

3 FILE A COMPLAINT WITH THE FTC

The Federal Trade Commission shares complaint data with law enforcement officials nationwide. You need the complaint affidavit to serve as part of your official "ID Theft Report" for disputing any further fraudulent activity. Report to (877) 438-4338 or identitytheft.gov.

4 FILE A POLICE REPORT

Take your FTC affidavit with you. If the officer is hesitant to fill out the report, request an information only report. You need the police report to complete your ID Theft Report.

WHEN RESOLVING IDENTITY THEFT, KEEP DETAILED RECORDS

Create a phone log and note who you talked to and when.

When sending supporting documents, send copies, not originals.

Send letters by certified mail, return-receipt requested.

Be aware of deadlines or time constraints.

Checklist & Notes

☐ Fraud Alert

Date Placed: _____

Credit reports requested after placing Fraud Alert:

☐ Experian - Date Requested_____ Date Received_____

☐ TransUnion - Date Requested_____ Date Received_____

☐ Equifax - Date Requested_____Date Received_____

☐ Security Freeze

☐ Experian - Date Placed_____ PIN_____

☐ TransUnion - Date Placed_____ PIN_____

☐ Equifax - Date Placed_____ PIN_____

NOTES

_____

_____

_____

_____

_____

_____

_____

_____

_____

Look here for updates & educational materials.
facebook.com/SCDepartmentofConsumerAffairs

Check out our YouTube channel.
youtube.com/scdcatv

Find the latest scam alerts and news here.
twitter.com/scdca

South Carolina Department of Consumer Affairs
2221 Devine St. STE 200 • PO Box 5757 • Columbia, SC 29250
(800) 922-1594 • www.consumer.sc.gov

- Spring 2019 -