BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Credit Freezes, Credit Reports & Identity Theft

Freezing at all three bureaus, reading your free reports,
and recovering step by step if your identity is stolen

A plain-English guide to keeping your name your own

Free, permanent protection — one calm step at a time

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

Equifax, Experian, TransUnion, FTC, IRS & SSA · facts current November 2026

What's Inside

This is your guide to protecting your credit and your identity. Read it in any order and at your own pace. If you only do one thing, freeze your credit at all three bureaus (Part 2) — it's free, it's permanent, and it stops most new-account fraud cold. If you think something has already gone wrong, turn to Part 5. Every phone number and website here was checked against the official source in November 2026.

Part 1 — Understanding Credit & Identity Theft

1 A Note from Bill
2 What Identity Theft Really Is
3 The Three Credit Bureaus — and Why They Matter
4 Freeze, Lock or Fraud Alert?

Part 2 — Freezing Your Credit

5 How to Freeze Your Credit: The Afternoon Plan
6 Freezing at Equifax
7 Freezing at Experian
8 Freezing at TransUnion
9 Keeping Track of Your Freezes
10 Lifting a Freeze to Apply for Credit
11 Fraud Alerts: Initial, Extended & Active Duty

Part 3 — Protecting the People You Love & the Other Freezes

12 Freezing a Child's or Grandchild's Credit
13 Helping a Spouse or an Aging Parent
14 The Other Freezes: ChexSystems, NCTUE & Innovis
15 Locking Your SSN Against Job Fraud: E-Verify Self Lock

Part 4 — Your Credit Reports

16 Your Free Weekly Credit Reports
17 How to Read a Credit Report
18 Disputing an Error on Your Report
19 Credit Karma & Free Credit Scores
20 Paid Monitoring & Identity Theft Insurance: Honest Answers

Part 5 — If Your Identity Is Stolen

21 Warning Signs Someone Is Using Your Identity
22 The First Steps: Call, Freeze, Alert
23 IdentityTheft.gov & Your FTC Report
24 Fixing the Damage, One Account at a Time

Part 6 — Taxes, Social Security & Medical Identity Theft

25 The IRS Identity Protection PIN
26 If Someone Files Taxes in Your Name
27 Social Security: Blocking Electronic Access
28 Medical Identity Theft

Part 7 — Scams & Everyday Protection

29 Scams Pretending to Be Credit Bureaus, the FTC or the IRS
30 Everyday Habits That Keep Thieves Out

Part 8 — When to Call Bill & Your Cheat-Sheet

31 When to Call Bill
32 Your Identity-Safety Cheat-Sheet

PART 1

Understanding Credit & Identity Theft

What identity theft really is, who the three credit bureaus are, and the three tools — freeze, lock and fraud alert — that stop a thief from borrowing in your name. Start here.

CHAPTER 1

A Note from Bill

Hello, and welcome. Whoever is reading this guide — this is for **you**. Maybe a letter arrived saying your information was caught up in a data breach. Maybe a family member told you to "freeze your credit" and you nodded along without quite knowing what that means. Or maybe something has already gone wrong: a bill you don't recognize, a call from a collector, a tax return that got rejected. Wherever you're starting from, you've come to the right place.

I'm Bill. With 30+ years of professional experience, I help folks here in Portage County, Ohio feel at home and safe with their technology. I wrote this guide the way I'd explain it at your kitchen table: slowly, in plain English, one step at a time. Any word you might not know, I'll stop and explain right then.

The good news first

Protecting your credit is one of the few safety jobs that is **free, permanent and fairly quick**. A credit freeze costs nothing, never expires on its own, and doesn't touch your credit score. Your credit reports are free every week. The government's recovery website, IdentityTheft.gov, is free too. You don't need to buy anything to be well protected.

WHAT THIS DOES FOR YOU

What this guide does for you

By the end you'll have your credit frozen at all three bureaus, know how to lift a freeze in minutes when you need a loan, read your own credit report with confidence, and know exactly what to do — in order — if someone ever does steal your identity. You'll also protect the people you love: a child, a spouse, or a parent you help look after.

How to use this guide

- **Just want to be protected?** Read *Freeze, Lock or Fraud Alert?* (Chapter 4), then follow *How to Freeze Your Credit: The Afternoon Plan* (Chapter 5). That's an afternoon's work, and it's the single biggest step.
- **Worried something already happened?** Go straight to *The First Steps: Call, Freeze, Alert* (Chapter 22). It's written for a stressful moment.
- **Tax season?** See *The IRS Identity Protection PIN* (Chapter 25) — and note the IRS online tool's yearly maintenance window.

- **Helping someone else?** See *Freezing a Child's or Grandchild's Credit* (Chapter 12) and *Helping a Spouse or an Aging Parent* (Chapter 13).

And you're never stuck alone. If you'd like a hand, call me at **(330) 200-8042** and we'll sort it out together, with no judgment. There's no such thing as a silly question here.

— Bill

CHAPTER 2

What Identity Theft Really Is

The Federal Trade Commission (the FTC, the government agency that handles consumer protection) puts it simply: **identity theft is when someone uses your personal or financial information without your permission.** That might be your name and address, a credit card or bank account number, your Social Security number, or your medical insurance number.

What a thief can do with your information

According to the FTC, someone with your details could:

- Buy things with your existing credit cards.
- Open **new** credit cards or loans in your name.
- Open a phone, electricity or gas account in your name.
- Steal your tax refund by filing a return as you.
- Get a job using your Social Security number.
- Get medical care using your insurance.
- Even give your name if they're arrested.

Two kinds of trouble

Kind	What it looks like	Main protection
Misuse of an account you already have	Strange charges on your card, money missing from your bank	Call the bank or card company right away; watch statements
New accounts opened as you	A card, loan or phone plan you never applied for	A credit freeze at all three bureaus

Most of this guide is about the second kind, because that's where a credit freeze does its quiet, powerful work. A freeze stops lenders from looking at your credit file, and without a look at your file, almost no lender will open a new account.

GOOD TO KNOW

It isn't your fault

Identity theft usually starts with information stolen from a company — a store, a hospital, an insurer — in a data breach you had no control over. Being a victim says nothing about how careful you are. What matters is what you do next, and this guide walks you through every step.

STAY SAFE

The one rule that prevents most of it

The FTC notes that organizations that need your Social Security number — like the IRS, your bank and your employer — **won't call, email or text you to ask for it.** If someone does, it's a scammer. Hang up and call the organization back on a number you look up yourself.

Checked against the FTC's "What To Know About Identity Theft" on November 13, 2026.

CHAPTER 3

The Three Credit Bureaus — and Why They Matter

A **credit bureau** (also called a credit reporting company) is a private company that keeps a file on how you've handled credit: your cards, loans, mortgage, addresses and payment history. When you apply for a loan, a credit card, an apartment or sometimes insurance, the business asks a bureau for a copy of your file — your **credit report**.

Meet the big three

Bureau	What to know
Equifax	Freezes are managed through a free **myEquifax** account, by phone or by mail.
Experian	Freezes are managed through a free Experian account, by phone or by mail.
TransUnion	Freezes are managed through the free **TransUnion Service Center**, by phone or by mail.

Each bureau keeps its **own** file on you. The FTC explains that not every lender reports to all three, so the three reports can differ. That's why two things in this guide must be done at **each** bureau separately:

- **A credit freeze** — freezing at one bureau does nothing at the other two.
- **Checking your reports** — look at all three, because a thief's account might show up on only one.

One thing is different: a **fraud alert**. You only contact one bureau, and the law requires it to tell the other two. More on that in *Fraud Alerts: Initial, Extended & Active Duty* (Chapter 11).

GOOD TO KNOW

There are smaller bureaus too

Banks use a company called ChexSystems to check your history before opening a checking account. Phone and utility companies use one called NCTUE. Innovis is a fourth, smaller credit bureau. You can freeze those too, for free — see *The Other Freezes: ChexSystems, NCTUE & Innovis* (Chapter 14).

Checked against the FTC's "Free Credit Reports" page on November 13, 2026.

CHAPTER 4

Freeze, Lock or Fraud Alert?

You'll hear three different words for protecting your credit. They sound alike, but they work differently and only two of them are free. Here's the plain-English version.

Credit freeze (also called a security freeze)

- **What it does:** While a freeze is in place, nobody can open a new credit account in your name — including you, until you lift it.
- **Cost:** Free to place and free to lift, by federal law.
- **How long:** Until you remove it. It never expires on its own.
- **Your credit score:** Not affected at all.
- **Where:** You must contact **all three** bureaus.

Fraud alert

- **What it does:** Tells businesses to check with you — usually by calling you — before opening new credit. It does *not* block them from seeing your report.
- **Cost:** Free.
- **How long:** One year for an initial alert (renewable); seven years for an extended alert if you're an identity theft victim.
- **Where:** Contact **one** bureau; it must tell the other two.

Credit lock

- **What it does:** Works much like a freeze, but it's a product a bureau offers under a contract, usually with an app and alerts.
- **Cost:** Usually part of a paid subscription. Experian says its CreditLock is included in a paid membership; TransUnion lists its monitoring with locking at $29.95 a month.
- **Where:** Each bureau's own product covers only its own file (TransUnion's paid plan says it locks TransUnion and Equifax).

	Freeze	Fraud alert	Lock
Blocks new credit?	Yes	No — asks lenders to verify you	Yes
Cost	Free	Free	Usually paid
Contact	All three bureaus	One bureau	Each bureau's product

	Freeze	Fraud alert	Lock
How long	Until you lift it	1 year (7 if extended)	While you subscribe

FROM BILL

My recommendation for most people

Freeze at all three bureaus, for free, and leave it frozen. When you need a loan or a new card, lift it for a few days. That's it. You don't need to pay for a lock to be well protected. If you've already been a victim, add a fraud alert on top — the FTC says you can have both at once.

Checked against the FTC's "Credit Freezes and Fraud Alerts," Experian's freeze page and TransUnion's freeze page on November 13, 2026.

PART 2

Freezing Your Credit

The afternoon plan: freezing at Equifax, Experian and TransUnion online, by phone or by mail — plus how to lift a freeze when you need it, and when a fraud alert makes sense.

CHAPTER 5

How to Freeze Your Credit: The Afternoon Plan

Freezing your credit takes three short visits — one to each bureau. Online is fastest. If you'd rather talk to a person or use paper, phone and mail work too. Set aside an afternoon, a cup of coffee, and the things below.

Have these ready

- Your **Social Security number** and **date of birth**.
- Your **current address**, and your previous address if you've moved in the last two years.
- Your **email address** and **cell phone** (bureaus often text a one-time code to confirm it's you).
- A **notebook** or a password manager, to record each login (see *Keeping Track of Your Freezes* (Chapter 9)).

The order I suggest

1. Freeze at **Equifax** — see *Freezing at Equifax* (Chapter 6).
2. Freeze at **Experian** — see *Freezing at Experian* (Chapter 7).
3. Freeze at **TransUnion** — see *Freezing at TransUnion* (Chapter 8).
4. Write down where and how you froze each one, with the date.
5. Optional but wise: freeze at ChexSystems, NCTUE and Innovis too — see *The Other Freezes: ChexSystems, NCTUE & Innovis* (Chapter 14).

How fast it works

Under the federal law that made freezes free in 2018, a bureau must put a freeze in place within **one business day** of an online or phone request, and within **three business days** of receiving a request by mail. In practice, Experian and TransUnion say online changes usually happen in real time.

TIP

Typing the address yourself

Type each bureau's web address into your browser yourself rather than clicking a link in an email or an ad. The official freeze pages are **equifax.com/personal/credit-report-services/credit-freeze**, **experian.com/freeze/center** and **transunion.com/credit-freeze**.

HEADS UP

Questions you might not expect

To prove it's you, a bureau may ask questions only you would know — like which of several streets you once lived on, or the size of a past car loan. If you get stuck or locked out online, don't worry. Use the phone or mail option for that bureau instead; the result is exactly the same.

WHAT THIS DOES FOR YOU

What this does for you

Once all three are frozen, a thief holding your name, birthday and Social Security number still can't open a new credit card or loan with them. You'll sleep better the next time you hear about a data breach on the news.

Checked against the FTC's 2018 "Free credit freezes are here" guidance and each bureau's freeze page on November 13, 2026.

CHAPTER 6

Freezing at Equifax

Equifax says placing, lifting and removing a security freeze is free. You can do it three ways.

Online, with a myEquifax account

1. Go to **equifax.com/personal/credit-report-services/credit-freeze**.
2. Choose to create a **myEquifax** account (or sign in if you already have one).
3. Enter your name, address, date of birth and Social Security number, and verify your identity.
4. Choose the option to **place a security freeze**.
5. Confirm. You can check your freeze status anytime by signing in to myEquifax.

By phone

Call Equifax at **(888) 298-0045**. You'll be asked for information to verify your identity. Equifax says you can choose to get a one-time PIN by text message or answer questions based on your Equifax credit report.

By mail

Download the Security Freeze Request Form from Equifax's freeze help page; it has the instructions and the mailing address. Equifax notes that if you ask by mail to *lift or remove* a freeze, you'll need to include documents that prove your identity and address.

GOOD TO KNOW

There's also a myEquifax app

Equifax offers a myEquifax app for iPhone and Android where you can manage a freeze. Use whichever you're most comfortable with — the website works just as well.

HEADS UP

Skip the upsell

While you're on the site you may see offers for paid monitoring plans. You don't need one to freeze. Look for the free freeze option and stay on that path.

Checked against Equifax's "How do I place, temporarily lift, or permanently remove a security freeze?" help page on November 13, 2026.

CHAPTER 7

Freezing at Experian

Experian says a security freeze is free and stays on your file until you remove it. Experian no longer uses a freeze PIN; you manage everything with a free Experian account.

Online

1. Go to **experian.com/freeze/center** (it opens Experian's credit freeze help page).
2. Choose **Create a free account**, or **Sign in** if you have one.
3. Verify your identity when asked.
4. Place the freeze. Experian says online freezes and unfreezes happen in real time.
5. Watch your email: Experian sends an alert every time you freeze, unfreeze, or schedule or cancel a thaw.

By phone

Call **1-888-EXPERIAN (1-888-397-3742)** to add or remove a freeze.

By mail

Write to **Experian Security Freeze, P.O. Box 9554, Allen, TX 75013**. Experian asks you to include:

- Your full name and Social Security number.
- Complete addresses for the past two years.
- Your date of birth.
- A copy of a government-issued ID, such as a driver's license.
- A copy of a utility bill or bank statement.

Make sure each copy is readable and shows your name, current mailing address and the issue date. Experian says mailed requests take up to three days after it receives them.

> **TIP**
>
> **A handy Experian extra: scheduled thaws**
>
> Experian lets you schedule an unfreeze ahead of time, with a start date and an end date. It's perfect when you know you'll be shopping for a car next week — the freeze lifts and comes back on its own. See *Lifting a Freeze to Apply for Credit* (Chapter 10).

Checked against Experian's "Freeze your credit file for free" page on November 13, 2026.

CHAPTER 8

Freezing at TransUnion

TransUnion says it's free to freeze, unfreeze and temporarily lift a freeze, and that a freeze won't affect your credit score. The quickest way is its online **TransUnion Service Center**.

Online

1. Go to **transunion.com/credit-freeze**.
2. Create a free account in the TransUnion Service Center, or log in.
3. Verify your identity.
4. Add the freeze. TransUnion says it often happens in real time, but to be safe, allow up to one hour.
5. Log in anytime to see your freeze status. (A freeze doesn't send you alerts, TransUnion notes.)

By phone or mail

TransUnion's freeze line is **1-888-909-8872**, the number the FTC lists for TransUnion. TransUnion's freeze-by-mail address, which Experian also publishes, is **TransUnion, P.O. Box 160, Woodlyn, PA 19094**. Check TransUnion's freeze page for the current form and what to include.

HEADS UP

Freeze, not lock

TransUnion sells a paid monitoring plan (it lists $29.95 a month) that includes a credit *lock*. You don't need it. The free **freeze** blocks new accounts just as well. If a page is asking for a credit card, you're on the wrong path.

GOOD TO KNOW

Spouses can help each other

TransUnion says spouses can add or remove freezes for each other by phone at 1-888-909-8872. For a child or an adult you have power of attorney for, see *Freezing a Child's or Grandchild's Credit* (Chapter 12) and *Helping a Spouse or an Aging Parent* (Chapter 13).

Checked against TransUnion's "Credit Freeze" page and the FTC's "Free Credit Reports" page on November 13, 2026.

CHAPTER 9

Keeping Track of Your Freezes

A freeze is only as handy as your ability to lift it later. Five years from now, when you're buying a car, you'll want to know exactly how to get back in. A little record-keeping today saves a lot of frustration.

Your freeze record

Bureau	How I froze it	Date	Login email / username	Where my password is kept
Equifax				
Experian				
TransUnion				
ChexSystems / NCTUE / Innovis				

PINs: who still uses them

- **Experian:** no PIN anymore — just your Experian account.
- **Equifax and TransUnion:** managed through your online account, or by phone with identity verification.
- **Innovis:** mails you a 10-digit Security Freeze PIN after it places the freeze. Keep that letter.
- **ChexSystems:** may mail you a PIN as well. Keep it with your records.

TIP

A password manager is ideal

If you use a password manager, save each bureau login there with a note: "credit freeze." If you keep a paper notebook instead, keep it somewhere safe at home — not in your wallet or purse.

STAY SAFE

Lost your login?

That's okay. Each bureau can verify you again by phone or by mail and let you lift or remove the freeze. Losing a password never locks you out of your own credit for good.

Checked against Experian's freeze page and Innovis's Security Freeze page on November 13, 2026.

CHAPTER 10

Lifting a Freeze to Apply for Credit

A freeze stops everyone — including you — from opening new credit. So when you're applying for a credit card, a car loan, a mortgage, or sometimes a new phone plan, apartment or insurance policy, you'll lift the freeze for a short time and then put it back.

The smart way to lift

1. Ask the lender, landlord or company: **"Which credit bureau will you check?"**
2. Lift the freeze at **just that bureau**. The FTC suggests this rather than lifting all three.
3. Online or by phone, the law requires the bureau to lift it within **one hour**. By mail, within three business days of receiving your request.
4. Apply for the credit.
5. Put the freeze back once the credit check is done (or use a scheduled thaw so it returns by itself).

Temporary lift vs. permanent removal

Choice	What it means
Temporary lift (thaw)	The freeze is off for a set time, then returns. Experian lets you pick a start and end date online.
Permanent removal	The freeze is gone until you place a new one. You'd have to remember to turn it back on.

TIP

Not sure which bureau they use?

Some lenders won't say, or they check more than one. In that case, lift all three for a short window — a few days is plenty — and let them come back on.

Who can still see a frozen report

Experian lists a few exceptions. Even with a freeze in place, these can still access your report:

- You, checking your own report.
- Lenders and card companies you already have accounts with.
- Landlords screening you as a new tenant, and debt collectors seeking payment.

- Card companies sending prescreened offers.
- Employers you've authorized to run a background check.
- Child support agencies and government agents with a court order or warrant.

GOOD TO KNOW

A freeze can block your own application

Experian points out that if you forget about your freeze, your own application can be turned down because the lender can't see your file. If that happens, simply lift the freeze and ask the lender to try again.

Checked against the FTC's "Credit Freezes and Fraud Alerts," the FTC's 2018 freeze guidance and Experian's freeze page on November 13, 2026.

CHAPTER 11

Fraud Alerts: Initial, Extended & Active Duty

A fraud alert is a note on your credit file that tells businesses to check with you before opening new credit. It's free, and unlike a freeze you only have to contact **one** bureau — the FTC says that bureau must tell the other two. You can have a fraud alert and a freeze at the same time.

The three kinds

Alert	Who can get it	How long	Extras
Initial	Anyone who is, or suspects they may be, affected by identity theft	1 year, renewable	A free credit report from each of the three bureaus
Extended	Identity theft victims with an FTC report (IdentityTheft.gov) or a police report	7 years	Removes you from prescreened credit and insurance offer lists for 5 years
Active duty	Active duty servicemembers	1 year, renewable for the deployment	Removes you from prescreened offer lists for 2 years

How to place an alert

1. Contact any **one** bureau: Equifax, Experian or TransUnion (online, or the phone numbers in *Freezing at Equifax* (Chapter 6), *Freezing at Experian* (Chapter 7) and *Freezing at TransUnion* (Chapter 8)).
2. Ask for an **initial fraud alert**, or an **extended fraud alert** if you have an FTC identity theft report or police report.
3. Give a phone number where lenders can reach you, so they can confirm it's really you.
4. Watch for confirmation, and order your free reports (see *Your Free Weekly Credit Reports* (Chapter 16)).

GOOD TO KNOW

When an alert is the better fit

If you're about to apply for credit soon and don't want to keep lifting a freeze, a fraud alert still lets lenders see your report — it just asks them to verify you first. Experian describes it that way. Many people who've been victims use both: a freeze for strength, and an alert as an extra flag.

HEADS UP

An alert is a request, not a lock

Lenders are told to verify your identity, but a fraud alert doesn't physically block your file the way a freeze does. That's why a freeze is still the stronger protection.

Checked against the FTC's "Credit Freezes and Fraud Alerts" on November 13, 2026.

PART 3

Protecting the People You Love & the Other Freezes

Freezing for a child, a spouse or a parent you care for, the lesser-known freezes for bank, phone and utility accounts, and locking your Social Security number against job fraud.

CHAPTER 12

Freezing a Child's or Grandchild's Credit

Children make tempting targets because nobody checks a child's credit — a thief can use a child's Social Security number for years before anyone notices. The FTC says that if your child is **under 16**, you can request a free credit freeze, and it stays in place until you ask the bureaus to remove it.

How it's different from an adult freeze

- It's done **by mail**, not online, at each bureau.
- You send proof that **you** are the parent or guardian, plus proof of the child's identity.
- Most children don't have a credit file at all — the bureau creates one just so it can be frozen.

What each bureau says

Bureau	Child freeze
Experian	Parents and guardians can freeze the credit file of children under 16, by mail. Experian's minor-request page lists what to send.
TransUnion	Calls it a **Protected Consumer Freeze**. A parent or guardian can place one for children aged 15 and younger by mailing a request with documents proving authority. The child can ask for it to be removed at 16 or older.
Equifax	Has a "Freezing Your Child's Credit Report" FAQ with the current instructions and form.

What you'll usually gather

- Copies of the child's birth certificate and Social Security card.
- A copy of your government-issued ID and proof of your address.
- If you're a guardian rather than a parent, the court paperwork that shows it.

HEADS UP

A child with a credit report is a warning sign

TransUnion notes that minors typically won't have a credit file unless you've added them as an authorized user on one of your accounts. If your child has a report and you never did that, it may be a sign of fraud. TransUnion offers a secure Child Identity Theft Inquiry Form to check.

TIP

Grandparents can help

If you're a grandparent, this is a lovely, practical gift to suggest to your grown children: "Have you frozen the kids' credit?" It takes a few envelopes and a little postage, and it protects them for years.

Checked against the FTC's "Credit Freezes and Fraud Alerts," Experian's freeze page and TransUnion's freeze page on November 13, 2026.

CHAPTER 13

Helping a Spouse or an Aging Parent

Many of us end up helping someone else with their finances — a husband or wife, or a parent whose memory isn't what it was. Freezing their credit is one of the kindest protections you can give, because scammers often target older adults.

If they can do it with you

The simplest way is to sit side by side and let them do the freeze in their own name, with you guiding. Follow *How to Freeze Your Credit: The Afternoon Plan* (Chapter 5) together. It's their account and their login, and you can help them record it.

If you're the spouse

TransUnion says spouses can add or remove freezes for each other by phone at 1-888-909-8872. Ask the other two bureaus what they allow when you call.

If you hold power of attorney or guardianship

TransUnion's **Protected Consumer Freeze** can be placed for an **incapacitated adult** by a guardian or a person with a valid power of attorney. You mail the request along with documents proving your authority. Ask each bureau for its version of this process; the paperwork is similar.

GOOD TO KNOW

After a loved one passes

TransUnion explains you can't freeze a deceased family member's credit report, but you can update their report to show they've died, which stops it from being used. Each bureau's site explains what to send.

FROM BILL

A gentle way to bring it up

Rather than "I'm worried you'll get scammed," try "I just froze my own credit — it was free and easy. Want me to help you do yours?" Most people are happy to say yes when it's framed as something you're both doing. And if you'd like me to sit with you both, I'm glad to — $49 remote · $99 in your home.

Checked against TransUnion's "Credit Freeze" page on November 13, 2026.

CHAPTER 14

The Other Freezes: ChexSystems, NCTUE & Innovis

The big three cover credit cards and loans. But thieves also open **bank accounts**, **cell phone plans** and **utility accounts** in other people's names. Those businesses often check different companies. Freezing these is free too, and it closes the side doors.

Innovis — the fourth credit bureau

- **Online:** the Security Freeze Request form at **innovis.com** (Personal > Security Freeze).
- **Phone:** 1-866-712-4546, the freeze number on Innovis's Security Freeze page.
- **Mail:** the Security Freeze Request by Mail form on the same page.
- Innovis mails you a confirmation letter with a **10-digit Security Freeze PIN**. Keep it.

NCTUE — phone, cable and utility accounts

The National Consumer Telecom & Utilities Exchange (NCTUE) holds information that phone, TV and utility companies use. NCTUE says you can place, lift or remove a freeze through its consumer portal at **nctue.com** or by calling **1-866-349-5355** — the same number the CFPB lists for NCTUE freezes.

ChexSystems — checking and savings accounts

Many banks and credit unions check ChexSystems before opening an account. A freeze there makes it harder for a thief to open a bank account in your name. Start at **chexsystems.com** and look for **Security Freeze**. Wisconsin's consumer protection agency lists ChexSystems' number as 1-800-887-7652.

Company	What it covers	Freeze
Innovis	Credit (a smaller fourth bureau)	innovis.com · 1-866-712-4546
NCTUE	Phone, cable and utility accounts	nctue.com · 1-866-349-5355
ChexSystems	Checking and savings accounts	chexsystems.com · 1-800-887-7652

TIP

Do these after the big three

These are a "nice to have" after Equifax, Experian and TransUnion are done. If you're short on time, freeze the big three today and come back to these next week.

Checked against Innovis's Security Freeze page and the CFPB's NCTUE listing on November 13, 2026.

CHAPTER 15

Locking Your SSN Against Job Fraud: E-Verify Self Lock

A credit freeze doesn't stop someone from using your Social Security number to get a **job**. For that, the federal E-Verify program (run by the Department of Homeland Security, which employers use to confirm someone can work in the U.S.) offers a free tool called **Self Lock**.

How it works

- You create a free **myE-Verify** account at **e-verify.gov**.
- You lock your Social Security number so it can't be used in E-Verify or Self Check.
- If an employer runs a locked number, the system flags a mismatch instead of approving it.
- The lock lasts **one year**; about 30 days before it ends you can extend it.
- If you take a new job with an E-Verify employer, you can unlock it yourself before they check.

GOOD TO KNOW

Who it helps most

Self Lock is most useful if you're retired or not planning to change jobs, or if your Social Security number has been exposed in a breach. Not every employer uses E-Verify, so think of it as one more layer, not a wall.

HEADS UP

Go only to e-verify.gov

There's no fee for Self Lock. A site that charges to "lock your Social Security number" is selling you something you can do yourself for free.

Checked against E-Verify's Self Lock FAQ and SSA's program operations manual (RM 10250.200) on November 13, 2026.

PART 4

Your Credit Reports

Getting your free weekly reports, reading them line by line, fixing mistakes, and an honest look at Credit Karma, free scores and paid monitoring.

CHAPTER 16

Your Free Weekly Credit Reports

You have the right to see what the bureaus say about you, for free. The three bureaus have **permanently** extended a program that lets you check your report from each of them **once a week, free**, at **AnnualCreditReport.com**. That's on top of the free yearly report federal law guarantees.

Three ways to order

How	Details
Online	**AnnualCreditReport.com** — you see your reports right away.
Phone	**1-877-322-8228** — your reports are processed and mailed within 15 days.
Mail	Fill in the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Mailed within 15 days of receipt.

Ordering online, step by step

1. Type **AnnualCreditReport.com** into your browser yourself. Check the spelling carefully.
2. Choose to request your free credit reports.
3. Enter your name, address, Social Security number and date of birth (and your previous address if you've moved in the last two years).
4. Pick which bureaus you want — you can choose all three at once.
5. Answer each bureau's security questions. You'll answer them separately for each one, because each gets its information from different sources.
6. Read, save or print each report. Saving a copy as a PDF makes it easy to compare next time.

SCAM ALERT

Only one official site

The FTC says AnnualCreditReport.com is the **only** site authorized to fill orders for your free reports. Copycat sites use "free report" in their names or misspell the address to sell you services or collect your information. The bureaus and AnnualCreditReport.com will not email you asking for your Social Security number.

TIP

Large print, Braille or audio

Your free annual reports come in Braille, large print or audio. Call 1-877-322-8228, verify your identity, and choose the format; the FTC says it takes about three weeks. If you're deaf or hard of hearing, call 7-1-1 and ask for the TDD service at 1-800-821-7232.

Other times you get an extra free report

- You were turned down for credit, a job, insurance or housing because of your report (ask within 60 days).
- You're unemployed and plan to look for work within 60 days, or you're on public assistance.
- Your report is wrong because of fraud, or you have a fraud alert on file.

Checked against the FTC's "Free Credit Reports" page on November 13, 2026.

CHAPTER 17

How to Read a Credit Report

A credit report looks intimidating the first time, but it's really just a few sections in a predictable order. Each bureau lays it out a little differently. Here's what you'll find and what to look for.

Section	What's in it	What to check
Personal information	Names, addresses, birth date, sometimes employers	Any address you never lived at, or a name you never used
Accounts (tradelines)	Every card, loan and mortgage, with balances and payment history	Any account you don't recognize, or late payments you didn't make
Inquiries	Who has asked to see your report	"Hard" inquiries from lenders you never applied to
Public records & collections	Bankruptcies, accounts sent to collectors	Collections for debts that aren't yours
Consumer statements & alerts	Fraud alerts, freezes and notes you've added	That your freeze or alert shows as you expect

A calm way to review it

1. Print it or open it on a big screen, with a pen and your list of cards and loans handy.
2. Check your **personal information** first. A strange address is often the first sign of trouble.
3. Go through **each account**. Tick off the ones you know.
4. Circle anything you don't recognize or that looks wrong.
5. Look at the **inquiries**. Circle any from companies you never applied to.
6. Repeat for all three bureaus — the FTC notes they can differ.

GOOD TO KNOW

Soft vs. hard inquiries

A "hard" inquiry happens when you apply for credit. A "soft" inquiry happens when you check your own report or a company sends you a prescreened offer. Soft inquiries are normal and harmless; it's the hard ones from strangers you want to question.

HEADS UP

Something wrong? Don't panic

Many errors are honest mistakes, like a mixed-up address. If it looks like a thief opened an account, go to *The First Steps: Call, Freeze, Alert* (Chapter 22). If it's simply wrong, see *Disputing an Error on Your Report* (Chapter 18).

TIP

A good rhythm

Since the reports are free every week, there's no need to order all three at once. Some people look at one bureau every few months, rotating through, so they always have a fairly recent look.

CHAPTER 18

Disputing an Error on Your Report

The CFPB (the Consumer Financial Protection Bureau, a federal agency) says you have the right to dispute errors on your credit report. Fixing an error generally means contacting both the credit bureau and the company that provided the information.

STAY SAFE

If it's identity theft, start at IdentityTheft.gov

The CFPB's own tip: if the error is the result of identity theft, go to IdentityTheft.gov first. Its letters carry extra legal weight. See *IdentityTheft.gov & Your FTC Report* (Chapter 23).

Step 1: Dispute with the credit bureau

Bureau	How to dispute
Equifax	Online at equifax.com/personal/credit-report-services/credit-dispute, or call the number on your report or (866) 349-5191.
Experian	Online at experian.com/disputes/main.html, or call the number on your report or (888) 397-3742.
TransUnion	Online through TransUnion's dispute page, or call (800) 916-8800.

If you mail a dispute, the CFPB says your letter should include:

- Your full name, address and phone number.
- The credit report confirmation number, if you have one.
- Each error you want fixed, with the account number.
- A clear explanation of why it's wrong, and a request to remove or correct it.
- A copy of the part of your report with the error circled or highlighted.
- **Copies** (never originals) of documents that support you.

The CFPB suggests sending it by certified mail with a return receipt, and keeping copies of everything. The CFPB also offers free instructions and a template letter on its website.

Step 2: Dispute with the company that reported it

Banks, card companies and landlords that report to the bureaus are called **furnishers**. Send them a written dispute too, by certified mail. The CFPB says furnishers generally must investigate and respond within **30 days** of receiving it. If they find the information was wrong, they must correct it and tell all the bureaus.

If they say it's accurate

You can ask the bureaus to add a short **statement** to your file explaining your side. Anyone who pulls your report afterward will see it. You can also submit a complaint to the CFPB at **consumerfinance.gov/complaint** or by calling (855) 411-2372.

Checked against the CFPB's "How do I dispute an error on my credit report?" on November 13, 2026.

CHAPTER 19

Credit Karma & Free Credit Scores

Credit Karma and similar apps show you a free credit score and pieces of your credit report, with alerts when something changes. They can be useful — as long as you understand what they are.

What Credit Karma actually shows

- Credit Karma says its free scores are **VantageScore 3.0** scores from **TransUnion and Equifax**.
- It doesn't show your Experian report or your FICO score.
- Many lenders, especially mortgage lenders, use FICO scores, so the number a lender sees can be different.

How it stays free

Credit Karma is a business. It earns money when people sign up for credit cards, loans and other products it recommends. That doesn't make it a scam — it's a well-known company — but it does mean you'll see plenty of offers. You never have to accept one.

Tool	What it's good for	Keep in mind
AnnualCreditReport.com	Your full official reports from all three bureaus	Reports only, no score
Credit Karma	Free VantageScore and change alerts from two bureaus	Ads for cards and loans; not FICO
Your bank or card company	Many show a free score in their app	Score type varies

GOOD TO KNOW

Why your scores never match

Different scoring models weigh things differently, and each bureau may have slightly different information. A score that's 20 or 30 points different from one place to another is normal. Watch the *trend* and the *accounts*, not one number.

HEADS UP

A freeze still matters

Alerts tell you after something happens. A freeze helps stop it from happening at all. Use an app for awareness if you like, but keep your freezes on.

Checked against Credit Karma's help articles on its scores on November 13, 2026.

CHAPTER 20

Paid Monitoring & Identity Theft Insurance: Honest Answers

You'll see a lot of advertising for identity theft protection. Here's what the FTC says these services do and don't do, so you can decide calmly whether one is worth paying for.

Credit monitoring

The FTC says credit monitoring usually tells you when:

- A company checks your credit, or a new loan or card appears on your report.
- A creditor or collector reports a late payment, or your credit limit changes.
- Your personal information, like your address or phone, changes.

But it **won't** alert you when someone withdraws money from your bank account, or uses your Social Security number to file a tax return.

Identity monitoring

These services check other databases — change-of-address requests, court records, payday loan applications, websites where stolen information is traded. The FTC notes most **won't** alert you if someone uses your information to collect your tax refund, or Medicare, Social Security or unemployment benefits.

Recovery services and insurance

- **Recovery services** give you a counselor to help write letters and place freezes — things the FTC notes you can often do yourself for little or no cost.
- **Identity theft insurance** may cover costs like copying, postage, notarizing, lost wages and legal fees. The FTC says it generally **won't** pay back money a thief stole.

Questions to ask before you pay

- Which of the three bureaus do you monitor, and how often?
- Is there a limit or a charge for looking at my reports?
- What exactly does the insurance cover, and what's the deductible?
- Do I already get this free through my bank, credit card, employer or insurance company?

FROM BILL

My honest take

For most people, the free tools in this guide — three freezes, a weekly look at your reports, an IRS IP PIN and careful habits — do the heavy lifting. Paid services can add convenience and alerts, and some people value the help. Just don't let an ad convince you that you're unprotected without one. You never have to pay to freeze your credit.

Checked against the FTC's "What To Know About Identity Theft" (monitoring and insurance section) on November 13, 2026.

PART 5

If Your Identity Is Stolen

The warning signs, the first calls to make, how IdentityTheft.gov builds your personal recovery plan, and how to clean up the damage one account at a time.

CHAPTER 21

Warning Signs Someone Is Using Your Identity

Identity theft rarely announces itself. It shows up as small oddities. The FTC suggests keeping an eye on four things, and there are a few more clues worth knowing.

The FTC's four checks

- **Track the bills you owe and when they're due.** If a bill stops arriving, someone may have changed your billing address.
- **Review your bills.** Charges you didn't make, or a new bill you didn't expect, can be a sign.
- **Check your bank statements** for withdrawals you didn't make.
- **Review your credit reports** for accounts you don't recognize (see *Your Free Weekly Credit Reports* (Chapter 16)).

Other clues

- A debt collector calls about a debt that isn't yours.
- You're turned down for credit you expected to get.
- The IRS tells you more than one return was filed in your name, or your e-filed return is rejected (see *If Someone Files Taxes in Your Name* (Chapter 26)).
- Your health plan's Explanation of Benefits lists care you never received (see *Medical Identity Theft* (Chapter 28)).
- A letter from a company you've never used thanks you for opening an account.

HEADS UP

Breach letters aren't the same as theft

A notice that your information was exposed in a data breach doesn't mean it has been misused. It's a signal to protect yourself: freeze your credit if you haven't, change that account's password, and watch your statements. IdentityTheft.gov also has steps for data breaches.

WHAT THIS DOES FOR YOU

Why noticing early matters

The sooner you spot a problem, the fewer accounts a thief can open and the easier the cleanup. A monthly glance at statements and a regular look at your credit reports is a few minutes well spent.

Checked against the FTC's "What To Know About Identity Theft" on November 13, 2026.

CHAPTER 22

The First Steps: Call, Freeze, Alert

If you think someone is using your identity, take a breath. This is fixable, and you don't have to do it all today. Here's the order that limits the damage fastest.

Today

1. **Call the companies where you know fraud happened.** Use the number on your card, statement or the company's official website — not a number from a suspicious email or text. Ask for the fraud department. Ask them to close or freeze the affected accounts, and change any passwords and PINs.
2. **Freeze your credit** at Equifax, Experian and TransUnion if you haven't already (see *How to Freeze Your Credit: The Afternoon Plan* (Chapter 5)).
3. **Place a fraud alert** by contacting one bureau. It's free, it lasts a year, and it gets you a free report from each bureau (see *Fraud Alerts: Initial, Extended & Active Duty* (Chapter 11)).
4. **Get your credit reports** and circle everything you don't recognize (see *Your Free Weekly Credit Reports* (Chapter 16) and *How to Read a Credit Report* (Chapter 17)).

Within the next day or two

1. **Report it to the FTC at IdentityTheft.gov.** You'll get your official Identity Theft Report and a personal recovery plan (see *IdentityTheft.gov & Your FTC Report* (Chapter 23)).
2. **Consider a police report.** Some businesses or debt collectors ask for one. Bring your FTC report and a photo ID.
3. **If taxes, Social Security or medical care are involved,** follow *If Someone Files Taxes in Your Name* (Chapter 26), *Social Security: Blocking Electronic Access* (Chapter 27) or *Medical Identity Theft* (Chapter 28).

TIP

Keep a simple log

Get a folder and a notebook. For every call, write the date, the company, who you spoke with, and what they promised. Keep copies of every letter. This record makes each later step much easier.

SCAM ALERT

Watch for "recovery" scammers

People who've just been victimized sometimes get calls offering to "fix" things or get money back for a fee. IdentityTheft.gov is free. Your bank's fraud department is free. Be very wary of anyone who contacts you out of the blue offering help for a price.

Checked against the FTC's identity theft recovery guidance and "Credit Freezes and Fraud Alerts" on November 13, 2026.

CHAPTER 23

IdentityTheft.gov & Your FTC Report

IdentityTheft.gov is the federal government's one-stop website for reporting identity theft and getting a free, personal recovery plan. It's run by the FTC. Reporting there is free.

What it gives you

- An **FTC Identity Theft Report** — your official proof that someone stole your identity.
- A **personal recovery plan** that walks you through each step, based on what happened to you.
- The ability to **update your plan and track your progress**.
- **Pre-filled letters and forms** to send to credit bureaus, businesses and debt collectors.
- Advice for **more than 30 types** of identity theft, plus steps for data breaches.

Filing your report

1. Type **IdentityTheft.gov** into your browser (Spanish: RobodeIdentidad.gov).
2. Choose to report identity theft.
3. Answer the questions about what happened — which accounts, which companies, when you noticed.
4. Create a free account when offered, so you can come back, update your plan and print letters later.
5. Review and submit. Save or print your Identity Theft Report and recovery plan.

HEADS UP

Save it before you leave

FTC materials explain that if you don't create an account, you need to save or print your report and plan right away — once you leave the page, you can't get back to them. Creating an account avoids that worry.

GOOD TO KNOW

Prefer the phone, or another language?

You can call the FTC at **1-877-438-4338**. To report in a language other than English or Spanish, the FTC says to call that number and press 3; interpreters are available 9:00 a.m. to 5:00 p.m. Eastern.

Why the report matters

Your FTC Identity Theft Report is what lets you place a seven-year **extended fraud alert**, and it backs up your letters asking businesses and bureaus to remove fraudulent accounts and debts. It turns "I didn't do this" into a documented claim.

Checked against the FTC's "What To Know About Identity Theft" and "Credit Freezes and Fraud Alerts" on November 13, 2026.

CHAPTER 24

Fixing the Damage, One Account at a Time

Once the urgent steps are done, recovery is mostly patient paperwork. Your IdentityTheft.gov plan lists exactly what to do for your situation. Here's what that work usually looks like.

Fraudulent accounts

1. Call the fraud department of each business where a thief opened an account. Tell them it was opened by an identity thief.
2. Send them your FTC Identity Theft Report and the letter IdentityTheft.gov prepares.
3. Ask them to close the account and send you a letter confirming you're not responsible for it.

Wrong information on your credit reports

Use the letters from IdentityTheft.gov to ask each bureau to remove the fraudulent accounts and inquiries. Innovis, for example, offers a **Block** for fraudulent information caused by identity theft. The general dispute steps are in *Disputing an Error on Your Report* (Chapter 18).

Debt collectors

If a collector contacts you about a debt the thief ran up, tell them in writing that you're an identity theft victim and send a copy of your FTC report. IdentityTheft.gov provides a letter for this, too.

Your own accounts

- Change passwords on email, banking and shopping accounts, starting with your email.
- Turn on two-step verification wherever it's offered; the FTC recommends it.
- Review statements closely for the next several months.

TIP

Mark your calendar

Your initial fraud alert lasts one year. Your extended alert, if you placed one, lasts seven. Put a reminder on your calendar a month before either ends so you can decide whether to renew.

FROM BILL

You don't have to do the paperwork alone

I can sit down with you, organize your folder, and work through the IdentityTheft.gov plan step by step until every account is cleaned up. Call (330) 200-8042 — $49 remote · $99 in your home.

Checked against the FTC's "What To Know About Identity Theft" and Innovis's Security Freeze page on November 13, 2026.

PART 6

Taxes, Social Security & Medical Identity Theft

The kinds of identity theft a credit freeze can't stop — and the free tools that can: the IRS IP PIN, Social Security's electronic access block, and a careful eye on your medical statements.

CHAPTER 25

The IRS Identity Protection PIN

An **Identity Protection PIN** (IP PIN) is a six-digit number from the IRS that prevents anyone else from filing a tax return using your Social Security number. The IRS says it's known only to you and the IRS, and it helps the IRS confirm it's really you when you file.

Who can get one

Anyone with a Social Security number or ITIN who can verify their identity — you don't have to be a victim, and you can get one even if you aren't required to file a return. Parents and legal guardians can request one for dependents.

HEADS UP

Timing matters right now

The IRS says its online IP PIN system will be **offline for maintenance from Monday, November 16, 2026, until mid-January 2027**. Each year the online tool is generally available from mid-January through mid-November. If you want one before then, act quickly — or plan to sign up in January.

Getting one online (the fastest way)

1. Go to **irs.gov/ippin** or open the official **IRS app**.
2. Sign in to your IRS online account. If you don't have one, you'll register and verify your identity first.
3. Go to your **Profile** and find the **IP PIN** section.
4. Request your IP PIN. It appears on screen.
5. Write it somewhere safe, or keep it where you keep your tax papers.

If you can't verify online

Option	How it works
Form 15227	If your adjusted gross income on your last return was below **$84,000** ($168,000 married filing jointly), you can submit Form 15227 online. The IRS calls you to verify your identity, then mails your IP PIN, usually within four to six weeks.
In person	Make an appointment at a local Taxpayer Assistance Center and bring one government photo ID plus one more form of ID. Your IP PIN arrives by mail, usually within three weeks.

Option	How it works
Under 18	Anyone under 18 must use one of these alternative methods instead of the online tool.

Using it each year

- An IP PIN is good for **one calendar year**. A new one is created each year.
- If you got yours online or in the IRS app, you'll **look it up there each year** — the IRS won't mail it.
- Enter it when your tax software asks, or give it to your trusted tax preparer when they're ready to file.
- It must be used on every federal return you file that year, including returns for earlier years.
- A wrong or missing IP PIN gets an e-filed return rejected or a paper return delayed.

SCAM ALERT

The IRS will never ask for your IP PIN

In the IRS's own words: the IRS will never ask for your IP PIN. Phone calls, emails or texts asking for it are scams. Share it only with the tax professional preparing your return.

Checked against the IRS "Get an identity protection PIN" page (last updated November 10, 2026) on November 13, 2026.

CHAPTER 26

If Someone Files Taxes in Your Name

Tax identity theft usually shows up one of two ways: your e-filed return is **rejected** because a return with your Social Security number was already filed, or you get an **IRS letter** about a return, income or refund you don't recognize.

What to do

1. **Don't ignore an IRS letter.** Respond the way the letter tells you to. Use the phone number or address printed in the letter, and double-check it against irs.gov.
2. If your e-filed return was rejected as a duplicate, complete **Form 14039, Identity Theft Affidavit**, from irs.gov and follow its instructions. The Taxpayer Advocate Service explains you'll usually file a paper return with it.
3. Report the theft at **IdentityTheft.gov**, and follow the tax steps in your recovery plan.
4. Freeze your credit and review your credit reports, since a thief with your Social Security number may try other things too.
5. Once things are sorted out, the IRS can enroll you in the IP PIN program so it can't happen again (see *The IRS Identity Protection PIN* (Chapter 25)).

SCAM ALERT

The IRS doesn't start with a phone call

Scammers love to pose as the IRS, threatening arrest unless you pay right away with gift cards or a wire. The real IRS doesn't do that. If you're unsure, hang up and look up the IRS yourself at irs.gov.

GOOD TO KNOW

A confirmed victim gets an IP PIN by mail

The IRS says that if it enrolled you in the IP PIN program because you were a confirmed victim of tax-related identity theft, it mails your new IP PIN each year on a CP01A notice.

FROM BILL

This is a good time for help

Tax identity theft involves forms, deadlines and letters. Your tax preparer is a great first call. If you'd like help with the online steps, I'm here — (330) 200-8042.

Checked against the IRS IP PIN page and the Taxpayer Advocate Service's identity theft guidance on November 13, 2026.

CHAPTER 27

Social Security: Blocking Electronic Access

Thieves sometimes try to get into a person's Social Security record online to change where benefit payments go. The Social Security Administration (SSA) offers a free tool that shuts that door.

What the block does

SSA says that when you block electronic access to your record, **no one — including you — can review or change your personal information online or through SSA's automated telephone service.**

Who might want it

- Victims of identity theft.
- Victims of domestic violence.
- Anyone who simply doesn't want their record available online.

How to set it up

1. Contact Social Security. SSA's national number is **1-800-772-1213**, or visit your local office.
2. Tell them you'd like to **block electronic access** to your record.
3. Verify your identity as they ask.
4. If you change your mind later, ask SSA to unblock it. You'll need to verify your identity again.

GOOD TO KNOW

Block or not?

If you rely on your my Social Security account to check benefits or print letters, a block will stop you from using it too. Many people are better served by having their *own* secure my Social Security account with a strong, unique password. The block makes most sense after identity theft, or if you never use SSA online.

SCAM ALERT

Social Security won't threaten you

Calls saying your Social Security number has been "suspended" or that you'll be arrested unless you pay are scams. Hang up. If you're worried, call SSA yourself at 1-800-772-1213.

Checked against SSA's "Block Access to Your Record" page on November 13, 2026.

CHAPTER 28

Medical Identity Theft

The FTC describes medical identity theft as someone using another person's name or insurance information to get medical treatment, prescription drugs or surgery. Besides the bills, it can put wrong information into *your* medical records — which matters to your safety.

The warning sign to watch for

After you get care, your health plan sends an **Explanation of Benefits** (EOB). If you have Medicare, you'll see a **Medicare Summary Notice**. The FTC says an EOB for services you didn't get, or for prescriptions you don't take, can mean someone is using your medical information.

What to do

1. Read each EOB or Medicare Summary Notice when it arrives. Compare it with your own calendar of appointments.
2. If something's wrong, call your health insurer's **fraud department** (for Medicare, use the number on your Medicare Summary Notice).
3. Ask your doctors and pharmacy for copies of your records, and ask them to correct anything that isn't yours.
4. Report it at **IdentityTheft.gov** or by calling 1-877-438-4338.

STAY SAFE

Guard your insurance cards

Treat your Medicare and insurance cards like credit cards. Don't give the numbers to anyone who calls offering "free" equipment, tests or supplies. The FTC also suggests keeping your Medicare card in a safe place.

WHAT THIS DOES FOR YOU

Why this protects your health, not just your wallet

Catching medical identity theft early keeps someone else's allergies, blood type or diagnoses out of your records, so the care you get is based on *your* history.

Checked against the FTC's medical identity theft guidance on November 13, 2026.

PART 7

Scams & Everyday Protection

The scams that pretend to be credit bureaus, the FTC or a credit report site — and the simple daily habits that keep your information out of a thief's hands.

CHAPTER 29

Scams Pretending to Be Credit Bureaus, the FTC or the IRS

Because people trust the names Equifax, Experian, TransUnion, the FTC and the IRS, scammers borrow them. The goal is always the same: get your Social Security number, your account logins, or your money.

What they sound like

- "This is Equifax calling to verify your account information."
- "There's suspicious activity on your credit report. Confirm your Social Security number so we can protect it."
- An email or pop-up: "Your free credit report is ready — click here," from a site that isn't AnnualCreditReport.com.
- "This is the FTC. We can recover the money you lost, for a processing fee."
- "This is the IRS. Read me your IP PIN to confirm your identity."

SCAM ALERT

The rules that catch every one of these

The FTC says AnnualCreditReport.com and the credit bureaus **will not email you asking for your Social Security number or account information**. If you get an email, a pop-up ad or a phone call claiming to be from them, don't reply or click any link. The IRS says it **will never ask for your IP PIN**. And the FTC doesn't charge fees to get your money back.

What to do instead

1. Hang up, or close the message without clicking anything.
2. Don't trust caller ID — scammers can make any name or number appear.
3. If you're worried something is really wrong, go to the organization yourself: type its web address, or call a number from its official site or from a statement.
4. Report the scam at **ReportFraud.ftc.gov**.

HEADS UP

Fake FTC websites

On November 12, 2026, the FTC warned that many people report scammers pretending to be the FTC, including fake FTC websites. The FTC's real sites end in **ftc.gov**, and IdentityTheft.gov is the real identity theft site.

GOOD TO KNOW

"Credit repair" promises

Be cautious of anyone who promises to erase accurate negative information from your report, or to give you a "new credit identity." You can dispute real errors yourself for free (see *Disputing an Error on Your Report* (Chapter 18)).

Checked against the FTC's "Free Credit Reports" page, the FTC's November 12, 2026 consumer alert on FTC impersonators, and the IRS IP PIN page on November 13, 2026.

CHAPTER 30

Everyday Habits That Keep Thieves Out

Freezes do the heavy lifting. These everyday habits, mostly from the FTC's advice, keep your information from getting out in the first place.

At home

- Keep financial records, Social Security and Medicare cards in a safe place at home — not in your wallet.
- Shred papers with personal information before throwing them out. No shredder? Look for a community shred day, or black out account numbers with a marker.
- Bring in your mail promptly, especially statements.

When someone asks for your Social Security number

The FTC suggests asking these questions before you share it:

- Why do you need it?
- How will you protect it?
- Can you use a different identifier?
- Can you use just the last four digits?

Online and on your phone

- Use strong, unique passwords, ideally stored in a password manager.
- Turn on two-factor authentication (a code or approval on your phone) for email, banking and shopping accounts.
- Never give personal information to someone who calls, emails or texts you out of the blue.

A simple yearly routine

When	What
Every month	Glance over bank and card statements, and any EOB or Medicare Summary Notice.
Every few months	Look at one or more of your free credit reports.
January	Get your new IRS IP PIN online, if you use one.
Anytime you apply for credit	Lift your freeze at the right bureau, then let it return.

When	What
Every year	Check that your freeze record and logins (see *Keeping Track of Your Freezes* (Chapter 9)) are still current.

WHAT THIS DOES FOR YOU

Small habits, big protection

None of these takes more than a few minutes, and together they make you a much harder target than most. Scammers look for easy marks — you won't be one.

Checked against the FTC's "What To Know About Identity Theft" on November 13, 2026.

PART 8

When to Call Bill & Your Cheat-Sheet

When a second pair of hands helps, and every number and website from this guide on one page.

CHAPTER 31

When to Call Bill

Most of this guide you can do yourself, and I hope you feel ready to. But some of it involves logins, identity questions and paperwork that are easier with someone beside you. Here's when I'd like you to pick up the phone.

Call me when

- **You'd like to freeze at all three bureaus** and want someone to sit with you while you do it.
- **A bureau's website keeps rejecting you**, or the identity questions have you stumped.
- **You're helping a parent or spouse** and want to set up their protections together.
- **You think your identity was stolen** and want help working through your IdentityTheft.gov plan.
- **You got a call, email or text** about your credit or taxes and aren't sure it's real.
- **You want an IRS IP PIN** and the online sign-up is giving you trouble.

FROM BILL

How I like to help

I'm Bill, and with 30+ years of professional experience I help folks feel at home and safe with their technology, right here in Portage County, Ohio. I don't rush and I don't talk down to anyone. I'll never ask for your passwords to keep — you type them, and you keep them. Call **(330) 200-8042** or book a time at **billshometech.com/book**. $49 remote · $99 in your home.

STAY SAFE

If money has already left your account

Call your bank or card company first, using the number on the back of your card. Speed matters with them. Then follow *The First Steps: Call, Freeze, Alert* (Chapter 22) — and call me whenever you're ready for help with the rest.

Thank you for taking the time to learn this. Freezing your credit and knowing these steps puts you ahead of most people. Be proud of that.

— Bill

CHAPTER 32

Your Identity-Safety Cheat-Sheet

Copy this onto a card and keep it with your important papers at home.

Freeze your credit (free)

Bureau	Online	Phone
Equifax	equifax.com/personal/credit-report-services/credit-freeze	(888) 298-0045
Experian	experian.com/freeze/center	1-888-397-3742
TransUnion	transunion.com/credit-freeze	1-888-909-8872
Innovis	innovis.com (Security Freeze)	1-866-712-4546
NCTUE	nctue.com	1-866-349-5355
ChexSystems	chexsystems.com	1-800-887-7652

Other free protections

What	Where
Free weekly credit reports	AnnualCreditReport.com · 1-877-322-8228
Report identity theft, get a recovery plan	IdentityTheft.gov · 1-877-438-4338
Report a scam	ReportFraud.ftc.gov
IRS Identity Protection PIN	irs.gov/ippin (online tool offline Nov 16, 2026 to mid-January 2027)
Block online access to your Social Security record	SSA · 1-800-772-1213
Lock your SSN against job fraud	e-verify.gov (myE-Verify Self Lock)
Credit report complaint	consumerfinance.gov/complaint · (855) 411-2372

Freeze vs. alert in one line each

- **Freeze:** blocks new credit; free; contact all three; lasts until you lift it.
- **Fraud alert:** asks lenders to verify you; free; contact one; 1 year (7 if you're a victim).
- **Lock:** like a freeze but usually a paid product. Not needed.

If your identity is stolen

1. Call the companies where fraud happened.

2. Freeze at all three bureaus, and place a fraud alert.
3. Get your credit reports.
4. Report at IdentityTheft.gov and follow your plan.
5. Call Bill: (330) 200-8042.

SCAM ALERT

Never share these with someone who contacts you

Your Social Security number, your IRS IP PIN, bureau logins, or one-time codes texted to your phone. Real companies won't call, email or text to ask.

Checked against the FTC, IdentityTheft.gov, Equifax, Experian, TransUnion, Innovis, the CFPB, the IRS and SSA on November 13, 2026.

Bill's Home Tech · Complete Manuals Series · (330) 200-8042 · billshometech.com · Portage County, Ohio