The Grumpy Sysadmin

Identity Theft
Quick-Start Checklist

Freeze the obvious doors before someone opens accounts, files taxes, or runs up bills in your name.

Before you trust your identity protection, slow down. A strong password helps, but it doesn’t stop someone from using your personal information to apply for credit, attack your tax return, hijack account recovery, or create a fraud mess you get to clean up while everyone else acts confused.

Grumpy Rule: Identity theft protection isn’t one magic subscription. It’s credit freezes, account alerts, recovery planning, paperwork, and not assuming “I would notice” is a fraud-monitoring strategy.

1. Freeze Your Credit Before There Is a Problem

A credit freeze makes it harder for someone to open new credit in your name. You usually need to freeze your credit separately with Equifax, Experian, and TransUnion. Save the account access and PIN/recovery details before you forget where they went.

Credit Freeze Check	Done
Equifax credit freeze reviewed or placed	☐
Experian credit freeze reviewed or placed	☐
TransUnion credit freeze reviewed or placed	☐
Freeze login details saved somewhere secure	☐
You know how to temporarily lift a freeze when needed	☐
Spouse, parent, or dependent freezes considered where appropriate	☐

Grumpy Rule: A credit freeze is annoying for five minutes. Identity theft paperwork is annoying with a calendar and a migraine.

2. Set Fraud Alerts and Account Alerts

A fraud alert tells lenders to take extra steps before opening credit. Bank and card alerts help you notice suspicious activity faster. Alerts aren’t a replacement for freezing credit, but they’re useful early-warning lights.

Alert Check	Done
Fraud alert considered if identity theft is suspected	☐
Bank transaction alerts are turned on	☐
Credit card purchase alerts are turned on	☐
Large transaction alerts are enabled where available	☐
New account or credit monitoring alerts reviewed if available	☐
Account alert emails and phone numbers are current	☐

Grumpy Rule: Finding fraud six weeks later isn’t monitoring. It’s archaeology with consequences.

3. Check Your Credit Reports

Review credit reports for accounts, addresses, inquiries, collections, or loans you don't recognize. Don't only check one bureau and declare victory. Identity thieves are annoying enough without giving them the benefit of incomplete checking.

Credit Report Check	Done
Equifax report reviewed	☐
Experian report reviewed	☐
TransUnion report reviewed	☐
Unknown accounts or loans investigated	☐
Unknown addresses or employers investigated	☐
Suspicious hard inquiries reviewed	☐
Errors disputed through the appropriate bureau	☐

Grumpy Rule: One clean report doesn't mean all three are clean. Because of course the mess can be spread unevenly.

4. Protect Tax, Social Security, and Government Accounts

Identity theft isn't only about credit cards. Tax fraud, benefit fraud, medical account problems, and government account access can create expensive headaches. Review these accounts before someone else decides to be you.

Government Account Check	Done
IRS Identity Protection PIN considered or set up if appropriate	☐
IRS account access reviewed if used	☐
Social Security online account created or secured	☐
State tax account or unemployment account reviewed if relevant	☐
Medicare, insurance, or medical portals reviewed if used	☐
Recovery email, phone, and MFA are current on critical accounts	☐

Grumpy Rule: Waiting until tax season to discover someone else already played "you" is a terrible way to celebrate April.

5. Lock Down Mail, Phone Carrier, and Recovery Channels

Mail and phone numbers are often used for account recovery. If someone can steal mail, redirect mail, take over your phone number, or receive your verification codes, they may attack accounts that otherwise look protected.

Recovery Channel Check	Done
USPS Informed Delivery considered if available	☐
Mail theft warning signs watched for	☐
Phone carrier account password is unique	☐
Carrier PIN/passcode is set	☐
Port-out or number-lock protection reviewed if available	☐
Carrier verification codes are never shared with callers	☐

Grumpy Rule: Your phone number shouldn't be the wobbly chair holding up your entire identity recovery plan.

6. Make an Identity Theft Response Folder

If something goes wrong, you want one place for dates, phone numbers, case numbers, letters, screenshots, and notes. The middle of a fraud mess isn't the time to invent a filing system called "maybe it is in Downloads."

Response Folder Check	Done
Secure folder created for identity theft notes	☐
Bank and card contact numbers saved from trusted sources	☐
Credit bureau login details saved securely	☐
FTC IdentityTheft.gov recovery site bookmarked or noted	☐
Copies of dispute letters, reports, and case numbers will be saved	☐
Trusted family contact identified for help if needed	☐

> ***Grumpy Rule: Documentation is boring until everyone asks for proof. Then it becomes your new favorite boring thing.***

Final “Don’t Ignore This” Check

Final Identity Theft Check	Done
Credit freezes reviewed or placed with all three bureaus	☐
Bank and credit card alerts are enabled	☐
Credit reports have been reviewed for unknown activity	☐
IRS IP PIN and Social Security account protection considered	☐
Phone carrier PIN or number-transfer protection reviewed	☐
Mail theft and address-change risks considered	☐
Trusted contact and response folder are ready	☐
You know what to do if a new account appears in your name	☐

If several boxes are unchecked, stop pretending identity theft protection is handled. Fix the basics before the next breach, scam, or mystery account turns into paperwork with a pulse.

> ***Grumpy Rule: The goal isn’t to become a fraud investigator. The goal is to make it harder for someone else to become you.***

After You Lock It Down: Verify Before You Celebrate

Identity-theft protections should reduce risk without trapping you when you legitimately need credit, banking, tax access, or account recovery. After making changes, confirm the important pieces still work.

After-Lockdown Check	Done
You can sign into credit bureau freeze accounts	☐
You know how to temporarily lift each freeze	☐
Bank and card alerts are arriving where expected	☐
Government account recovery methods are current	☐
Phone carrier account still signs in correctly	☐
Response folder is easy to find and update	☐

> ***Grumpy Rule: The job isn’t done when you freeze credit. It’s done when your identity is harder to abuse and you can still function like a normal human being. Annoying, but useful.***

Want the Full Identity Theft & Fraud Defense Guide?

This free quick-start checklist helps you find the obvious identity-theft and fraud risks. The full guide goes deeper and walks through what each protection does, where to start, what to document, and how to respond if your information is already being misused.

Full Guide Will Include	Covered
Step-by-step credit freeze and fraud alert walkthrough	☐
Credit report review and dispute workflow	☐
IRS IP PIN, Social Security, and government account protection	☐
Bank, credit card, and transaction alert setup	☐
Phone carrier, SIM-swap, and mail-theft protection	☐
Data breach response checklist	☐
What to do if an account is opened in your name	☐
Fraud documentation and recovery worksheets	☐
Family and elder fraud protection plan	☐
Monthly identity-fraud maintenance checklist	☐

Grumpy Rule: The free checklist points at the doors. The full guide is for closing them without turning your financial life into a guessing game.

Get the full Identity Theft & Fraud Defense Guide
or the future Home Cybersecurity Survival System
https://thegrumpysysadmin.com

Final Word

You can’t stop every data breach, leaked record, fake form, stolen mail piece, or scammer with too much free time. You can make the obvious fraud paths harder, add alerts, save your recovery details, and know where to start if something happens.

Freeze what should be frozen. Turn on alerts. Review reports. Protect your phone number. Save the paperwork.

Lock it down now. Recover faster later. Stay grumpy.