Identity & Financial Hardening Guide

A practical checklist for securing your identity, whether you've received a breach notification or simply want to protect yourself proactively.

> **Guiding Principle:** Prevention beats monitoring. Monitoring beats recovery. Lock accounts first; then watch quietly.

The three factors of authentication: Security relies on proving who you are through:

- **Something you know** (a password or PIN)
- **Something you have** (your phone or a hardware key)
- **Something you are** (your fingerprint or face)

Using more than one factor makes accounts dramatically harder to break into. This guide helps you layer these factors across your most important accounts, and freeze or restrict insecure access to important institutions like credit bureaus, the IRS, and your mobile carrier.

Why This Matters (Even Without a Breach)

You don't need to wait for a breach notification to take these steps. Your personal information is already circulating from years of data collection, previous breaches, and public records. The question isn't *if* your data has been exposed; it's *how much* and *when* someone will try to use it.

Taking these precautions now means:

- Attackers hit walls instead of open doors
- You're not scrambling to react after fraud occurs
- Recovery is simpler if something does happen

This guide is organized into three tiers:

- **Critical:** Do these immediately; they block the most common attacks
- **Suggested:** Important protections that significantly reduce risk
- **Optional:** Long-term hygiene for those who want comprehensive coverage

---

Table of Contents

What We're Protecting Against

This guide helps you lock down the main ways criminals exploit stolen personal information:

- **New account fraud:** Someone opens credit cards, loans, or accounts in your name. *Solution: credit freezes.*
- **Account takeover:** Someone breaks into your existing accounts using stolen or guessed passwords. *Solution: password manager + MFA.*
- **Phone number hijacking:** Someone takes over your phone number to intercept verification codes. *Solution: carrier PIN + port-out protection + shift away from SMS-based MFA.*
- **Tax refund theft:** Someone files a fake return in your name and steals your refund. *Solution: IRS IP PIN.*
- **Benefits fraud:** Someone claims your Social Security, unemployment, or other benefits. *Solution: claim your government accounts first.*
- **Social engineering:** Someone impersonates you over the phone using breached data. *Solution: verbal PINs + skepticism.*

The goal is simple: make it harder for criminals to profit from your stolen data than it's worth for them to try.

Foundation: Password Manager

Before starting this checklist, set up a password manager. You'll be creating unique passwords and storing PINs, security questions, and recovery codes throughout this process; you need a secure place to keep them.

Why it matters: Most people use the same handful of passwords everywhere. This is the single biggest security mistake you can make. When any website gets breached (and they do, constantly), attackers take those leaked passwords and try them on banking sites, email providers, and everything else. If you reused that password, they're in. A password manager fixes this by generating and remembering a unique random password for every site. You only need to remember one master password. The result: a breach at some random shopping site you forgot you signed up for doesn't cascade into your bank account, your email, and your entire digital life.

> **But I'll forget the master password!** Use a passphrase instead: four or five random words strung together, like "correct horse battery staple" or "purple tuesday bicycle window." It's long enough to be secure but memorable enough to stick. Write it down and keep it somewhere safe while you're learning it. After a week of daily use, you won't need the paper anymore.

Recommendation: 1password.com is well-established in the security industry and designed for usability. It works across devices, supports families and teams, and can store passwords, credit cards, secure notes, and documents.

Other reputable options: Bitwarden (open source), Dashlane

Setup steps:

- ☐ Install 1Password (or your chosen manager) on your phone and computer
- ☐ Create a strong master password you can memorize (a passphrase works well)
- ☐ Enable MFA on your password manager account
- ☐ Begin storing credentials as you work through this guide

Foundation: Passkeys

Passkeys are a newer technology that replaces passwords entirely. Instead of typing a password, you unlock with your fingerprint, face, or device PIN. The site never sees a password because there isn't one; it uses cryptographic keys stored securely on your device.

Why passkeys matter:

- **Can't be phished:** There's no password to steal or trick you into entering on a fake site
- **Can't be reused:** Each passkey is unique to one site
- **Can't be guessed:** No password means no brute-force attacks
- **Nothing to remember:** Your device handles everything

Should you use them? Yes, when available. Passkeys are more secure than passwords + MFA combined. Major sites now support them: Google, Apple, Microsoft, Amazon, PayPal, and more. When a site offers passkey setup, take it.

> **How do passkeys work?** When you create a passkey, your device generates a unique cryptographic key pair. The private key stays on your device (protected by your fingerprint or face); the public key goes to the website. When you log in, the site challenges your device to prove it has the private key. Your device does this without ever sending the key itself. There's nothing for attackers to steal from the website's database and nothing to intercept in transit.

Setup steps:

- ☐ Check if your key accounts support passkeys (Google, Apple, Microsoft, Amazon)
- ☐ Set up passkeys where offered; your password manager (1Password) can store them
- ☐ Keep your password as a backup until you're comfortable with passkeys

> **What if I lose my phone?** Passkeys can sync across your devices through your password manager or iCloud/Google account. If you lose everything, you'll fall back to password recovery, which is why you should keep your password manager and recovery options in good shape.

Critical Actions

These protect against the most common and damaging attacks. Do these first.

Secure Your Primary Email (Highest Priority)

Your email is the master key to your digital life. Password resets, account verifications, and security alerts all flow through it. **If an attacker controls your email, they can reset passwords and take over nearly every other account you own.**

- ☐ **Enable app-based MFA** (not SMS)
  - ☐ Use an authenticator app: Google Authenticator, Microsoft Authenticator, or 1Password's built-in TOTP
  - ☐ Or use hardware keys (YubiKey) if supported; even stronger
- ☐ **Use a strong, unique password** generated by your password manager
- ☐ **Review recovery options**

    - ☐ Confirm recovery email and phone are current and secure
    - ☐ Remove outdated or shared recovery contacts
- ☐ **Check for unauthorized access**
    - ☐ Review recent login activity
    - ☐ Revoke access from unfamiliar devices or apps

> **Why not SMS?** SIM-swap attacks let criminals take over your phone number and intercept SMS codes. App-based MFA stays on your device and can't be redirected.

Freeze Your Credit

Credit freezes block the most common form of identity theft: opening new accounts in your name.

- ☐ **Freeze at Equifax** - my.equifax.com/membercenter/#/freeze
- ☐ **Freeze at Experian** - usa.experian.com/mfe/regulatory/security-freeze
- ☐ **Freeze at TransUnion** - service.transunion.com/dss/freezeStatus.page
- ☐ **Store PINs and logins** in your password manager
- ☐ **Skip fraud alerts;** freezes are stronger
- ☐ **Avoid paid "credit lock" products;** freezes are free and legally protected

> **Freeze vs. fraud alert - what's the difference?** A fraud alert just asks lenders to verify your identity before opening accounts - but they don't have to. A freeze actually blocks access to your credit report entirely, so lenders can't approve new accounts at all. Freezes are also free by law. "Credit locks" are a paid product some bureaus sell that does basically the same thing as a free freeze - skip them.

> **Note:** You'll need to temporarily lift freezes when applying for credit, renting, or undergoing background checks. This takes a few minutes online.

Protect Your Phone Number

Your phone number is used for MFA, account recovery, and identity verification. SIM-swap attacks are increasingly common.

- ☐ **Add a carrier account PIN** (different from your phone unlock PIN)
    - ☐ AT&T: "Extra Security Passcode"
    - ☐ Verizon: "Account PIN"
    - ☐ T-Mobile: "Account PIN" + "Port Validation"
- ☐ **Enable port-out protection** (call your carrier to confirm it's active)
- ☐ **Require in-store ID verification** for SIM changes
- ☐ **Avoid phone support for account changes;** use online or in-store

> **What's a SIM swap?** A criminal calls your carrier, pretends to be you, and convinces them to transfer your phone number to a SIM card they control. Now they receive your calls and texts - including those two-factor codes. Port-out protection adds a PIN that the carrier must verify before moving your number, so a smooth-talking scammer can't just talk their way in.

Protect Your Tax Identity

Tax refund fraud is common and frustrating to resolve.

- ☐ **Enable an IRS IP PIN** at irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin
- ☐ **Store your IP PIN** in your password manager (renewed annually)

> **How does tax fraud work?** A criminal files a tax return in your name early in the season, claims a big refund, and gets the money. When you file your real return later, the IRS rejects it as a duplicate. Sorting this out can take months. The IP PIN is a six-digit code only you and the IRS know - without it, a return filed under your SSN gets rejected automatically.

Suggested Actions

These provide significant additional protection and are worth doing after the critical items.

Secure Your Social Security Account

If you don't create this account, an attacker could create one in your name.

- ☐ **Create a "my Social Security" account** at ssa.gov/myaccount
- ☐ **Enable MFA**
- ☐ **Verify contact information**
- ☐ **Review earnings history** for signs of SSN misuse

> **Why create an account if I don't need one yet?** The SSA only allows one online account per Social Security number. If you don't claim yours, a criminal can create one using your stolen info, then redirect your benefits, change your address, or lock you out. It's like squatting on a domain name - claim it before someone else does.

Harden Banking & Financial Accounts

- ☐ **Set a verbal PIN or passphrase** for phone/teller support (call your bank to add this)
- ☐ **Enable MFA** on all online banking (authenticator app preferred)
- ☐ **Disable SMS-only authentication** where better options exist
- ☐ **Enable transaction alerts** for large withdrawals or transfers
- ☐ **Review account recovery methods;** remove outdated contacts

> **What's a verbal PIN for?** Social engineering is when someone calls your bank pretending to be you and smooth-talks their way into your account. They might have your SSN, address, and mother's maiden name from a breach - enough to pass basic security questions. A verbal PIN is a secret word or code that the bank requires before making changes over the phone. It's not in any database for criminals to steal.

Secure Employer & Payroll Accounts

Payroll fraud redirects your paycheck to an attacker's account.

- ☐ **Enable MFA** on payroll portals (Workday, ADP, etc.)
- ☐ **Ask HR about secondary verification** for direct deposit changes
- ☐ **Monitor pay stubs** for unexpected changes

> **How does payroll fraud happen?** A criminal logs into your company's payroll portal (using credentials from a phishing email or breach), changes your direct deposit to their bank account, and waits for

> payday. You don't notice until your rent check bounces. By then, the money is gone. MFA and verification callbacks make this much harder.

Protect Healthcare Accounts

Medical identity theft creates false records and fraudulent bills.

- ☐ **Enable MFA** on health insurance portals
- ☐ **Monitor Explanation of Benefits (EOBs)** for unfamiliar claims
- ☐ **Review annual benefits statements**

> **Why is medical identity theft a big deal?** Someone uses your insurance to get prescriptions, treatments, or surgery. You get the bills - but worse, their medical history (blood type, allergies, conditions) gets mixed into your records. This can lead to dangerous medical errors later. Cleaning up medical records is much harder than fixing credit.

Secure HSA/FSA Accounts

These accounts are often overlooked and have weaker security.

- ☐ **Enable MFA** on HSA/FSA accounts
- ☐ **Monitor for unauthorized reimbursements**
- ☐ **Review linked bank accounts**

Optional Actions

Long-term hygiene for comprehensive protection. Do these when you have time.

Freeze Secondary Credit Bureaus

Beyond the big three, other agencies maintain reports used for specific purposes.

- ☐ **Innovis** - innovis.com/personal/securityFreeze
- ☐ **ChexSystems** (banking) - chexsystems.com/security-freeze/place-freeze
- ☐ **NCTUE** (utilities/telecom) - nctue.com/consumers
- ☐ **LexisNexis** - consumer.risk.lexisnexis.com/request

Opt Out of Data Brokers

Reducing your data broker footprint limits social engineering and identity correlation.

> **What are data brokers and why do they matter?** Data brokers collect and sell your personal information - addresses, phone numbers, relatives, jobs, property records, and more. Anyone can buy this data, including criminals. They use it to answer your security questions, impersonate you convincingly, or target you for scams. Opting out doesn't erase the past, but it reduces what's available going forward.

Manual opt-outs (time-intensive but free):

- ☐ Spokeo

- ☐ BeenVerified
- ☐ Whitepages
- ☐ Intelius
- ☐ PeopleFinder
- ☐ Radaris

Paid removal services (they handle opt-outs for you):

- ☐ joindeleteme.com
- ☐ privacyduck.com
- ☐ Optery
- ☐ Kanary

Review Third-Party App Access

- ☐ Review apps connected to your Google account: myaccount.google.com/permissions
- ☐ Review apps connected to Microsoft: account.microsoft.com/privacy
- ☐ Revoke access from apps you no longer use

What You Don't Need

Save your time and money:

Action	Why Skip It
SSN replacement	Extremely rare approval; doesn't stop existing exposure
Paid identity theft subscriptions	Free monitoring is sufficient; freezes are more effective
Multiple fraud alerts + freezes	Redundant; freeze already blocks new accounts
Panic account closures	Often unnecessary and complicates recovery
Multiple paid monitoring services	Diminishing returns; one free service is enough

---

Documentation & Incident Readiness

Keep records for disputes, insurance, or legal action.

- ☐ **Save breach notification letters** (scan or photograph)
- ☐ **Screenshot proof of credit freezes**
- ☐ **Document key dates and exposed data types**
- ☐ **Keep a log of suspicious activity**
- ☐ **Store securely** in your password manager or encrypted folder

---

Ongoing Monitoring

Free Monitoring

- ☐ **Enroll in breach-provided monitoring** if offered (don't enter payment info)

- ☐ **Set up free credit monitoring:**
  - ☐ annualcreditreport.com - free weekly reports
  - ☐ Credit Karma or Credit Sesame (free tier)

Regular Reviews

Quarterly:

- ☐ Review bank and credit card statements
- ☐ Check credit reports for unfamiliar accounts

Annually:

- ☐ Audit recovery methods on critical accounts
- ☐ Renew IRS IP PIN

Defensive Mindset

- ☐ **Treat unsolicited calls and emails as hostile by default**
- ☐ **Never confirm personal info to inbound callers**
- ☐ **Verify urgent requests** by calling official numbers from statements
- ☐ **Remember:** legitimate organizations won't pressure you for immediate action

---

Last updated: January 2026