Identity theft checklist

What to do if your identity is stolen. Work down the list in order and tick each step as you finish it. The full guide, with the reasons behind every step, is at confirmedstolen.com/identity-theft/.

Right away

- [ ] **Write down what you know: dates, accounts, charges and how you found out**
  A simple log of every call, letter and account number keeps the rest of the process organized and gives you a record if a dispute drags on.

- [ ] **Report the theft at IdentityTheft.gov**
  The FTC site walks you through a report and generates an FTC Identity Theft Report and a personal recovery plan. Save a copy; companies and credit bureaus may ask for it. IdentityTheft.gov (www.identitytheft.gov/)

- [ ] **Place a free fraud alert with one credit bureau**
  A fraud alert (a flag telling lenders to verify your identity before opening credit) placed with one of Equifax, Experian or TransUnion is passed to the other two. Ask the bureau how long the alert lasts and how to extend it.

- [ ] **Or place a free credit freeze with each bureau separately**
  A credit freeze (a block that stops most new lenders from seeing your report) is stronger than an alert, but you must request it from Equifax (www.equifax.com/), Experian and TransUnion individually. Keep any PIN or login each bureau gives you.

- [ ] **Call the fraud department of each company where fraud occurred**
  Use the number on your card, statement or the company's official website, not a number from an email or text. Ask them to close or freeze the account and to send written confirmation.

Within the first few days

- [ ] **Pull your credit reports from all three bureaus at AnnualCreditReport.com**
  AnnualCreditReport.com (www.annualcreditreport.com/) is the official free source. Look for accounts, inquiries and addresses you do not recognize.

- [ ] **Dispute every fraudulent account and inquiry with each bureau**
  File the dispute with the bureau that shows the item and attach or reference your FTC Identity Theft Report. Follow your IdentityTheft.gov recovery plan for the exact letters it recommends.

- [ ] **Change passwords on email, banking and any account that was touched**
  Start with your primary email account, because it resets every other password. Use a unique password for each account; a password manager makes that practical.

- [ ] **Turn on multi-factor authentication (MFA) everywhere it is offered**
  MFA requires a second proof, such as an authenticator app code or a security key, in addition to the password. App-based codes and security keys resist SIM swap attacks better than text messages. See SIM swap (confirmedstolen.com/sim-swap/).

- [ ] **Consider filing a police report**
  Some creditors, insurers or debt collectors ask for one, and it helps if the thief is known or a large loss is involved. Bring your FTC Identity Theft Report, ID and proof of address.

- [ ] **Sign out of other sessions and remove unknown devices from your accounts**
  Most email, banking and social platforms list active sessions and trusted devices in their security settings. Remove anything you do not recognize. See hacked accounts (confirmedstolen.com/hacked-accounts/).

If specific documents or records were misused

- [ ] **Tax-related identity theft: contact the IRS and ask about an Identity Protection PIN**
  If someone filed a return in your name or used your Social Security number for work, follow the IRS identity theft guidance. An Identity Protection PIN (a number that must accompany returns filed under your SSN) can block future fraudulent filings. Start at IRS.gov (www.irs.gov/) and check its current instructions.

- [ ] **Stolen Social Security card: request a replacement from the SSA**
  The Social Security Administration handles replacement cards. Check its current eligibility rules and options at SSA.gov (www.ssa.gov/).

- [ ] **Stolen driver's license: report it to your state DMV and request a replacement**
  Each state motor vehicle agency sets its own process. Ask whether it can flag the old license number. USA.gov (www.usa.gov/) links to state agencies.

- [ ] **Government benefits or unemployment fraud: report it to the paying agency**
  Benefits fraud was among the larger FTC identity theft categories in 2024. Contact the agency that issued the benefit directly, using contact details from its official website.

- [ ] **Online fraud with financial loss: consider a complaint to the FBI IC3**
  The FBI's Internet Crime Complaint Center collects cybercrime reports. File at IC3.gov (www.ic3.gov/) if the theft began with a hacked account, phishing or an online scam.

Recovery and the months that follow

- [ ] **Get written confirmation that each fraudulent account is closed and removed**
  Keep letters from creditors and bureaus confirming the debt is not yours. These documents settle later questions from collectors.

- [ ] **Recheck your credit reports on a regular schedule**
  New fraudulent accounts can appear after the first cleanup. A freeze makes that far less likely, but it is still worth looking.

- [ ] **Watch bank, card and benefits statements every month**
  Small test charges often come before larger fraud. Report anything unfamiliar to the company's fraud department at once.

- [ ] **Update your IdentityTheft.gov report if new problems appear**
  Adding new accounts to your existing report keeps your FTC Identity Theft Report complete and your recovery plan current.

Prevent it happening again

- [ ] **Keep your credit frozen unless you are applying for credit**
  Each bureau lets you lift a freeze temporarily and then restore it. A frozen file is the single strongest barrier against new-account fraud.
- [ ] **Treat breach notices as a prompt to act, not as noise**
  When a company says your data was exposed, change the affected password, confirm MFA is on, and check whether your credit is frozen.
- [ ] **Carry less: leave your Social Security card and spare cards at home**
  Fewer documents in a wallet means less to replace and less to misuse if it is lost or taken.

Your case record

FTC Identity Theft Report number

Fraud alert placed (bureau, date)

Credit freezes (date each)

Police report number

Companies contacted (and reference)

Notes

Version November 6, 2026. General information, not legal advice. Agencies change their procedures, so confirm each step with the organization named. Confirmed Stolen is an independent reference; it is not law enforcement and does not recover property. Free to print and share with attribution.