SIM swap checklist

What to do after a SIM swap or phone number port-out. 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/sim-swap/.

In the first hour

- [ ] **Confirm the outage is not an ordinary network problem**
  If your phone suddenly shows "No service" or "SOS only" while others nearby have signal, and a restart does not fix it, treat it as a possible SIM swap.
- [ ] **Call your carrier immediately from another phone**
  Use a family member's phone, a landline or a work line, and say you suspect a SIM swap or unauthorized port-out. Use the number on your bill or the carrier's official website.
- [ ] **Ask the carrier to restore the number and open a fraud case**
  For a SIM swap, the carrier can move service back to your SIM. For a port-out, ask how it will reclaim the number from the other carrier, and write down the case number.
- [ ] **Request a port-out freeze, number lock and new account PIN**
  Carriers use different names for these protections. Ask for every lock available and a new PIN that is not your birthday or part of your Social Security number.
- [ ] **Secure your primary email account from a trusted device**
  Change the password, remove recovery phone numbers you do not control, and delete forwarding rules you did not set. Our hijacked account guide (confirmedstolen.com/hacked-accounts/) covers each step.
- [ ] **Call your bank and card issuers on their official numbers**
  Use the number on the back of your card. Ask them to flag the account, block new payees and hold unusual outgoing transfers.

Within 24 hours

- [ ] **Move multi-factor authentication off SMS on key accounts**
  Switch email, banking, brokerage, cryptocurrency, password manager and registrar accounts to an authenticator app, hardware key or passkey.
- [ ] **Change passwords and sign out of all sessions**
  Start with email, then financial accounts, then social media. Use unique passwords from a password manager.
- [ ] **Review financial accounts for transfers and new payees**
  Check bank, card, payment app and investment statements for transactions, linked accounts or contact details you did not authorize.

- [ ] **Check cryptocurrency exchange and wallet accounts**
  Look for withdrawals, new withdrawal addresses and changed security settings, and contact the exchange's official support if anything moved.

- [ ] **Check domain registrar and web hosting accounts**
  SIM swaps are a common path to registrar account takeover. Confirm your domains, contacts and DNS are unchanged; see domain name theft (confirmedstolen.com/domain-name-theft/) if they are not.

This week

- [ ] **File a complaint with the FBI IC3**
  Report the SIM swap and any losses to the FBI Internet Crime Complaint Center (www.ic3.gov/) and keep the confirmation.

- [ ] **File a complaint with the FCC**
  Report the carrier incident through the FCC consumer center (www.fcc.gov/consumers), especially if the carrier was slow to respond or did not notify you.

- [ ] **Make a police report and keep the report number**
  Banks, carriers and insurers may ask for it when you dispute charges or reclaim accounts.

- [ ] **Report identity theft if new accounts were opened**
  If the attacker used your information to open accounts, create a recovery plan at IdentityTheft.gov (www.identitytheft.gov/).

- [ ] **Check your credit reports for accounts you did not open**
  Request your reports at AnnualCreditReport.com (www.annualcreditreport.com/) and consider a credit freeze with each bureau.

Prevent it happening again

- [ ] **Keep the port-out freeze and account PIN in place**
  Leave the locks on permanently and lift them only when you deliberately change carriers.

- [ ] **Remove your phone number as a recovery option where you can**
  Where a service allows it, rely on an authenticator app, passkey or backup codes rather than texts to your number.

- [ ] **Act on any SIM change or port-out notice you did not request**
  Carriers must notify customers of these requests under FCC rules. An unexpected notice is a signal to call the carrier at once.

- [ ] **Limit what you share publicly about your number and carrier**
  Attackers use birthdays, addresses and carrier details from social profiles and data breaches to impersonate you.

Your case record

Phone number

Carrier case number

Port-out lock or account PIN set (date)

FCC complaint number

IC3 complaint number

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.