Financial Account Breach

Your bank or credit card was compromised. Here's what to do.

Questions? Email hello@ohanasec.io

PHASE 1 — IMMEDIATE

Freeze or lock the affected account right now

1 Freeze or lock the affected account right nowMost banks have a card freeze in the app. Use it immediately. If unauthorized transfers occurred, call the fraud line — do not use a number from any email you received.Freeze card in mobile app (Chase, BofA, Wells Fargo, Citi — all have this)If online banking was accessed: change your password NOW from a trusted deviceEnable a session logout / "sign out of all devices" if available

2 Document everything before you change anythingBefore you start resetting things, take screenshots. You'll need these for the fraud claim and potentially for law enforcement.Screenshot all unfamiliar transactions with dates and amountsScreenshot any emails or texts related to the breachNote the exact time you first noticed something was wrong

3 Check if other accounts use the same passwordIf your bank login was compromised, any account with the same password is also at risk right now.Think of your top 5 most sensitive accounts — email, other banks, brokerage, PayPal/Venmo/ZelleLog into each and change the password if it matches (or is similar) to the breached one

PHASE 2 — ASSESS

Pull your full transaction history — go back 90 days

1 Pull your full transaction history — go back 90 daysAttackers often make small test charges days or weeks before larger ones. Look for:Charges under $1 (card testing)Unfamiliar merchant names — look up anything you don't recognizeRecurring charges you didn't authorizeTransfers to accounts you don't own (Zelle, ACH)

2 Check your credit report for new accounts or inquiriesIf someone accessed your banking credentials, they may have also applied for credit in your name.Pull your free report at AnnualCreditReport.com (the official government-mandated site)Look for accounts you didn't open or hard inquiries you didn't authorizeCheck all three bureaus: Equifax, Experian, TransUnionOfficial reporting linksAnnualCreditReport.com — free government-mandated report↗IdentityTheft.gov — FTC identity theft report and recovery plan↗

3 Determine how they got inUnderstanding the entry point matters for your fraud claim and for preventing recurrence.Phishing email/text— you were sent a fake login pageData breach— your credentials leaked from another service (check HaveIBeenPwned.com)Reused password— same password used on multiple sitesMalware— a keylogger or screen capture on your deviceSIM swap— attacker took over your phone number to intercept SMS codes

PHASE 3 — REPORT

File a formal fraud claim with your bank

1 File a formal fraud claim with your bankFederal law (Regulation E for bank accounts, Fair Credit Billing Act for credit cards) protects you — but only if you report promptly. Credit cards: generally 60 days. Debit cards: 2 days for full protection, 60 days maximum.Call the fraud department — ask for a case number and write it downRequest a written confirmation of the disputeAsk how long the investigation will take and when you'll receive provisional creditAsk for a new account number and card, not just a new card

2 Place a credit freeze at all three bureausA freeze stops anyone from opening new credit in your name — it's free and the single most effective thing you can do against identity theft.Freeze your credit — do all threeEquifax Credit Freeze↗Experian Credit Freeze↗TransUnion Credit Freeze↗FTC IdentityTheft.gov — personalized recovery plan↗

3 Report to the FTC and optionally local law enforcementAn FTC report (IdentityTheft.gov) creates a legal record and gives you an official document to show creditors. For losses over $500, a police report may help with reimbursement claims.File at IdentityTheft.gov — takes about 10 minutes, generates a personalized recovery planFor wire fraud or large losses, report to the FBI's IC3 at ic3.govIf you received a fraudulent text/email, forward it to 7726 (SPAM)

4 Rebuild trust with family members who may have been affectedIf shared accounts or family members' information was exposed, be direct with them. Silence creates more anxiety than honest communication.Tell affected family members what happened without over-explaining — "our bank account was accessed without permission, I've filed a fraud claim and our money is protected while they investigate"Let them know what you're doing about it (Phase 4)If a child's SSN or identity was involved, report separately at identitytheft.gov/child-identity-theft

PHASE 4 — PREVENT

Set up a password manager — all financial accounts get unique passwords

1 Set up a password manager — all financial accounts get unique passwordsThis is the single most impactful change you can make. A password manager generates and stores long, random, unique passwords — you only remember one master password.We recommendBitwarden — free, open source, best starting point1Password — excellent family plan option

2 Enable app-based two-factor authentication on every financial accountUse an authenticator app (Authy or Google Authenticator) — not SMS. SIM swap attacks can intercept text codes. Your bank, brokerage, PayPal, Venmo, and Zelle all support this.Setup guidesAuthy setup guideGoogle Authenticator setup guide

3 Set up account alerts for all transactionsEnable real-time push notifications for every transactionSet a threshold alert for any purchase over $50 (or your comfort level)Enable alerts for new payees added (for bank transfers)Review account login notifications — know every time someone logs in

4 Consider a credit monitoring serviceCredit freezes prevent new accounts but don't alert you to misuse of existing ones. Monitoring catches things freezes don't.Your bank may already offer free monitoring — check firstCredit Karma (free) monitors two of the three bureausExperian IdentityWorks offers all-three bureau monitoringSome homeowners/renters insurance policies include identity theft monitoring

Key Resources

Official links for reporting, recovery, and prevention.

FTC Identity Theft Report	https://identitytheft.gov
AnnualCreditReport.com	https://annualcreditreport.com
Equifax Credit Freeze	https://equifax.com/personal/credit-report-services/free-credit-freeze/
Experian Credit Freeze	https://experian.com/freeze/center.html
TransUnion Credit Freeze	https://transunion.com/credit-freeze

Need hands-on help?
OhanaSecure provides remote digital security sessions for families across the US. Email hello@ohanasec.io or visit ohanasec.io.