

6.3 Personal Data Incidents

Identity Theft

Signs of identity theft:

- Accounts or loans you didn't open appearing on credit report
- Calls or mail from debt collectors about debts you don't owe
- IRS notification of multiple tax returns filed in your name
- Medical bills for services you didn't receive
- Mail or email about accounts you didn't create
- Missing mail or bills
- Denied credit unexpectedly
- Unauthorized withdrawals from bank accounts

Step 1: Contain the Damage (IMMEDIATELY)

- Place fraud alert on credit reports (call ONE bureau, they notify the others)
 - Equifax: 1-888-766-0008
 - Experian: 1-888-397-3742
 - TransUnion: 1-800-680-7289
 - Fraud alert lasts 1 year, requires creditors to verify your identity
- File FTC Identity Theft Affidavit
 - Go to <https://www.identitytheft.gov>
 - Click "get started" – you'll be guided through a series of questions, have ready:
 - Personal information (name, address, SSN, DOB)
 - Details about the identity theft (what happened, when discovered)
 - Information about fraudulent accounts (account numbers, companies, amounts)
 - Any evidence you have (emails, bills, credit reports)
 - Review and submit
 - Download and print multiple copies (keep one safe as a backup)
 - This will be used for police reports and to legally contest any action taken against you on account of the identity theft
- Get your credit reports
 - Request from all three bureaus immediately
 - Go to annualcreditreport.com (or one of your financial accounts)
 - Or request from the bureau you called for fraud alert
 - Review for accounts and inquiries you don't recognize
- File police report

- Contact local police department
- Bring FTC Identity Theft Report
- Request a copy of the police report
- You'll need this for disputing fraudulent accounts

Step 2: Close Fraudulent Accounts (Within 24-48 Hours)

- For each fraudulent account found
 - Contact the fraud department of the company
 - Explain you're an identity theft victim
 - Provide your Identity Theft Report
 - Request the account be closed
 - Request fraudulent charges be removed
 - Ask for written confirmation
- For fraudulent credit cards or loans
 - Request investigation
 - Provide police report and FTC Identity Theft Report
 - Follow company's fraud dispute process

Step 3: Secure Your Legitimate Accounts (Within 48 Hours)

- Change passwords on all financial accounts
- Enable MFA on all accounts
- Review recent activity on all accounts
- Close accounts that were compromised

Step 4: Additional Actions

- Consider a credit freeze
 - More protective than fraud alert
 - Blocks new accounts from being opened
 - Free at all three bureaus
 - You can temporarily lift when applying for credit
- Ongoing monitoring (6-12 months)
 - Review credit reports every 3 months
 - Monitor bank and credit card statements weekly
 - Watch for new collection calls or letters
 - Keep detailed records of all actions taken
 - Follow up on dispute resolutions
- If tax fraud occurred
 - Contact IRS Identity Protection Specialized Unit: 1-800-908-4490
 - File Form 14039 (Identity Theft Affidavit)
- If medical identity theft
 - Contact your health insurance company
 - Request copies of medical records to review
 - Dispute incorrect information with providers

Lost or Stolen Wallet or Purse

What's at risk:

- Credit/debit cards
- Driver's license or ID
- Social Security card (if you carry it - you shouldn't)
- Insurance cards
- Other identification documents

Step 1: Immediate Containment (IMMEDIATELY)

- Cancel all cards:
 - Call fraud departments for all credit and debit cards in wallet
 - Request new cards with new numbers
 - Note the date/time you report each card
- Place fraud alert on credit reports (if ID was in wallet):
 - Call one credit bureau (see Identity Theft section above)
- Check accounts for unauthorized charges
 - Review all recent transactions
 - Report unauthorized charges immediately

Step 2: Replace Documents (Within 24-48 Hours)

- Driver's license/ID: Contact your state DMV to report and replace
- Social Security card: Contact SSA (don't carry SSN card in future)
- Insurance cards: Contact providers for replacements
- Other cards: Library, gym, membership cards - contact to cancel/replace

Step 3: Monitoring

- Monitor all financial accounts daily for 2 weeks
- Review credit reports monthly for 3 months
- Watch for fraudulent account openings
- Save all documentation of reported theft

Sent Money to a Scammer

Common scenarios:

- Wire transfer to scammer
- Gift cards purchased and codes given
- Cryptocurrency sent
- Payment app (Venmo, PayPal, Zelle) transfer

- Credit card payment to fake website

Step 1: Try to Stop the Payment (IMMEDIATELY)

Document everything:

- How scammer contacted you
- What they claimed
- Timeline of events
- Amount lost
- All communications

For wire transfers:

- Contact your bank (fraud department)
- Request wire transfer recall
- Most effective within 24 hours
- Provide details: amount, date, receiving bank

For credit/debit card charges:

- Contact card issuer fraud department
- Request transaction be blocked or reversed
- File dispute/chargeback
- Request new card number

For payment apps (Venmo, PayPal, Zelle):

- Contact app support
- Report unauthorized transaction
- Request cancellation/reversal
- Note: Zelle transfers are usually instant and irreversible

For gift cards:

- Contact gift card company (number on card)
- Provide card numbers and receipt
- Request freeze/cancellation
- Success rate is low but worth trying immediately

For cryptocurrency:

- Generally irreversible
- Report to exchange if applicable
- Document transaction details

Step 2: Report the Fraud (Within 24 Hours)

- File FTC report <https://reportfraud.ftc.gov>
 - Creates official record
 - Helps track scam patterns
- File police report:
 - Needed for most theft claims
 - Helps with bank/credit card disputes
 - Bring all documentation

Step 3: Protect Against Further Loss (Within 24 Hours)

- Place fraud alert on credit reports if you gave personal information
- Monitor accounts daily for additional unauthorized charges

Gave Out Personal Information

Follow this playbook if you gave out high risk, personal information via email or to a caller in a conversation you did not initiate.

High Risk Personal Information:

- Passwords or PINs
- Bank account numbers including any credit card data (number, CVV)
- Social Security number or date of birth
- Any answer you use in a security question

Step 1: Immediate Actions (Based on What You Shared)

- Passwords or PINs: Follow the appropriate account compromise playbook above
- Bank account numbers or any credit card data: Contact fraud department on back of card, or call banking institution to stop any unauthorized pending transactions and have new card or account issued
- Social security number or date of birth: Monitor credit report for any queries or new accounts and follow the Identity Theft playbook if anything shows up; consider a credit freeze regardless by calling one of the three credit bureaus (see Identity Theft playbook)
- Any answer you use in a security question: Change the security question in all sites where it was used

Step 2: Monitor accounts daily for 2 weeks

If you see anything unusual, follow the appropriate playbook

Clicked a Phishing Link or Opened Suspicious Attachment

Your next steps are based on what you did, based on risk.

Low Risk

- If you ONLY clicked the link and did not enter any information or download any files, close the browser and clear your browser cache.
- If you downloaded any files, and especially if you opened the file, delete the files and run a full virus scan (see Malware or Virus infection playbook below).

High Risk

- If you entered a password, follow the playbook for the appropriate type of compromised account above
- If you entered any other personal information, follow the playbook for Gave out Personal Information based on the type of data you entered

Received Notice of Data Breach

This is when a company notifies you your data was exposed.

Common notification sources:

- Email from company
- Letter in mail
- News article about breach
- Notification from HavelBeenPwned.com

Step 1: Verify Notification is Legitimate (IMMEDIATELY)

Beware of phishing! Don't click links in breach notification emails, instead, verify using one of the following:

- Go directly to company's website (type URL yourself)
- Look for official breach notification page
- Verify through news sources
- Call company using official phone number

Step 2: Understand What Was Exposed (Within 24 Hours)

Read the notification carefully:

- What specific data was compromised?
- When did the breach occur?
- What is the company doing?
- What services are they offering (credit monitoring, etc.)?

Step 3: Take Action Based on Data Exposed (Within 48 Hours)

If passwords were exposed: Follow the playbook for the type of compromised account above

If email address only: Not much you can do here, just understand you will likely start receiving a lot of spam and potentially phishing attempts, so be extra vigilant in the coming weeks and months.

If Social Security number or financial data:

- Place fraud alert on credit reports (see Identity Theft section)
- Consider a credit freeze
- Monitor credit reports monthly for 12 months
- Enroll in credit monitoring if offered (only California requires this be offered at the time of this writing, but many companies will offer anyway in a show of goodwill)
- Review financial statements going back to the date of the breach (US law requires you are notified, but the timeline for notification is somewhat of a gray area)

If medical information:

- Watch for fraudulent medical bills
- Contact health insurance if fraudulent claims appear
- Monitor credit reports monthly for 12 months

Step 4: Accept Company's Offer (If Valuable)

Many companies offer:

- Free credit monitoring (usually 1-2 years)
- Identity theft protection
- Credit freeze assistance

Evaluate the offer:

- Is credit monitoring included? (worth it)
- How long is coverage? (longer is better)
- Do you have to pay anything? (should be free)
- Read terms carefully before accepting

Step 5: Additional Actions

Document the breach:

- Save notification letter/email
- Screenshot relevant information
- Note what data was exposed

Monitor relevant accounts based on exposure and consider legal action if negligence was involved.

Ongoing monitoring:

- Check credit reports every 3 months for 1 year
- Monitor financial accounts for suspicious activity
- Watch for targeted phishing using your data
- Stay alert for identity theft signs

SIM Swap Attack

Signs of SIM swap:

- Phone suddenly has no service/signal
- Can't make calls or send texts (even after reboot)
- Notifications of password resets you didn't request
- Unusual account activity alerts stop arriving
- Carrier confirms your number was ported to new SIM

Step 1: Regain Control of Phone Number (IMMEDIATELY)

Contact your mobile carrier:

- Call from a different phone or use online chat
- Verify account activity and report unauthorized SIM swap if the agent determined your SIM card was ported
- Verify your identity (have account PIN ready)
- Request your number be restored to your SIM
- Ask them to lock your account with additional verification

Step 2: Secure Accounts That Use Phone for 2FA (Within 1 Hour)

Attackers may have targeted accounts using SMS for two-factor authentication. Verify recent logins to new devices in the following priority:

- Email accounts (especially recovery emails)
- Financial accounts (banks, investment, PayPal)
- Cryptocurrency exchanges
- Social media accounts
- Any other account using SMS for authentication

If there was an unauthorized login, for each account:

- Remove any new authorized devices that aren't yours
 - Change password (from trusted device)
 - Remove SMS as 2FA if possible and replace with authenticator app or hardware key
 - Check recent activity for and perform damage control (see relevant playbook in Account Compromise above)
 - Enable login alerts if not already enabled
-

Revision #1

Created 2026-07-12 22:23:24 UTC by Chris Landis

Updated 2026-07-12 22:28:22 UTC by Chris Landis