Wigington Security Group

Privacy consulting for individuals and families

⚠

Breach Response Playbook

What to do immediately after a data breach

You Got the Email. Now What?

This guide covers:

- First 24 hours: Critical actions you must take now
- Password reset prioritization framework
- Credit monitoring and freeze procedures
- Financial fraud prevention checklist
- Identity theft recovery steps
- How to prevent future breaches

Time-Sensitive Actions:

🔴 **First 1 Hour:** Change passwords on critical accounts
🟡 **First 24 Hours:** Enable 2FA, monitor accounts
🟢 **First Week:** Credit freeze, update security questions

February 2025 • 16 Pages • Free Download

wigingtonsecurity.com

Contents

1 Understanding Data Breaches

1.1 What Just Happened?

A data breach occurs when unauthorized parties access a company's database containing customer information. This could be:

- **Hacking:** Criminals exploit security vulnerabilities
- **Insider threat:** Employee or contractor steals data
- **Third-party compromise:** Vendor or partner gets breached
- **Misconfiguration:** Database left publicly accessible (happens more than you'd think)

1.2 What Information Was Exposed?

Breach notifications legally must tell you what data was compromised. Common categories:

Data Type	Risk Level
Email addresses	Medium — Used for phishing, spam
Passwords (hashed)	High — If weak hashing, can be cracked
Passwords (plaintext)	CRITICAL — Immediately usable
Security questions/answers	High — Used for account recovery attacks
Phone numbers	Medium — Enables SIM swapping, phishing
SSN / National ID	CRITICAL — Identity theft risk
Credit card numbers	High — Fraud risk (but cards can be replaced)
Date of birth	Medium — Used with other data for identity theft
Physical address	Medium — Privacy and physical security risk
Financial account data	CRITICAL — Direct fraud risk

1.3 Why This Matters Even If ”You Have Nothing to Hide”

⚠ Warning

Common dismissive reactions we hear:

- ”I don’t care if they have my email, I get spam anyway”
- ”My password was strong, so it’s fine”
- ”I don’t have money for criminals to steal”

Why you should still care:

1. **Credential stuffing:** 65% of people reuse passwords. Criminals will try your breached credentials on banking, email, and social media sites.
2. **Identity theft:** Even without SSN, combining email + DOB + address + phone enables synthetic identity fraud.
3. **Targeted phishing:** Breached data makes scam emails convincing—they’ll reference real details about you.
4. **Account takeover:** Losing access to your email means losing access to everything tied to that email.

1.4 How Did You Find Out?

Direct notification from company: You received an email or letter stating the breach. This is legally required in most jurisdictions.

Have I Been Pwned notification: You’re monitoring your email at https://haveibeenpwned.com (good practice).

News reports: You heard about it in the media before official notification (happens when companies delay disclosure).

Suspicious activity: You noticed unauthorized login attempts or weird account behavior.

Pro Tip

Use WigSec’s breach checker tool to see all known breaches affecting your email addresses:
https://wigingtonsecurity.com/tools/breach-check
This tool checks against Have I Been Pwned’s database and provides specific remediation steps for each breach.

2 Immediate Actions: First Hour

Time is critical. Follow this prioritized sequence.

CRITICAL ACTION

DO THIS NOW — Not after reading the entire guide
If the breach involved passwords, **stop reading** and complete Section 2.1 immediately. Then come back and read the rest.

2.1 Step 1: Identify What Was Breached

Look at the breach notification and identify:

Action Checklist

Which service was breached (website/company name)

What data was exposed (email, password, SSN, credit card, etc.)

Whether passwords were hashed or stored in plaintext

Date range of the breach (when did it happen vs. when discovered)

2.2 Step 2: Change Your Password on the Breached Service

Immediately reset your password on the affected service.

1. Go directly to the service's website (don't click email links—phishing risk)
2. Use password reset function
3. Create a **unique** password you've never used anywhere else
4. Minimum 16 characters, use a password manager to generate it

Warning

Don't reuse old passwords. Even if your old password was strong, it's now burned. Generate a completely new one.

2.3 Step 3: Identify Password Reuse

Critical question: Did you use that same password anywhere else?
If YES:

1. List every other account where you used that password
2. Prioritize by importance (see Section 2.4)
3. Change those passwords immediately

If NO (you used a unique password):

1. You're in good shape—the breach is contained to one service
2. Still follow remaining steps for that one account
3. Pat yourself on the back for using unique passwords

Pro Tip

Can't remember where you reused passwords?
If you use a password manager:

- 1Password: Security Watchtower shows reused passwords
- Bitwarden: Reports → Reused Passwords
- Dashlane: Password Health report

If you don't use a password manager: You need to assume you reused it and change passwords on all important accounts. Then start using a password manager (see our guide: *Password Manager Setup*).

2.4 Step 4: Prioritized Password Changes

You can't change 50 passwords at once. Use this priority framework:

Priority	Account Type	Timeline
P0	Email (Gmail, Outlook, etc.)	**NOW**
P1	Financial (bank, investment, PayPal, Venmo)	**Next 1hr**
P2	Password manager itself	**Next 1hr**
P2	Work accounts (email, VPN, corporate systems)	**Next 2hrs**
P3	Social media (Facebook, Instagram, Twitter, LinkedIn)	**Today**
P4	Shopping sites (Amazon, eBay, etc.)	**This week**
P5	Everything else	**This week**

Why email is P0: Your email account is the "keys to the kingdom." Anyone who controls your email can reset passwords on everything else.

Why financial is P1: Direct fraud risk. Criminals will try to transfer money or make purchases within hours of a breach.

2.5 Step 5: Enable Two-Factor Authentication (2FA)

On every account you just changed the password for, enable 2FA immediately.

Best 2FA methods (in order):

1. **Hardware security key** (YubiKey, Google Titan) — Most secure
2. **Authenticator app** (Authy, Google Authenticator, 1Password) — Very secure
3. **SMS to phone** — Better than nothing, but vulnerable to SIM swapping

Warning

Avoid SMS 2FA if possible. SIM swapping attacks let criminals receive your SMS codes. Use an authenticator app instead.

Action Checklist

2FA Setup Checklist:

Enable 2FA on primary email

Enable 2FA on all financial accounts

Enable 2FA on password manager

Save backup codes in secure location (not on your computer)

Enable 2FA on social media accounts

3 First 24 Hours: Containment

You’ve handled the critical passwords. Now expand your response.

3.1 Review Recent Account Activity

Check for unauthorized activity on affected accounts:

Action Checklist

On each affected account, review:

Recent login history (dates, times, locations, devices)

Recent password changes you didn’t make

New email addresses or phone numbers added to account

Recent purchases or transactions you didn’t authorize

Account recovery settings (backup emails, security questions)

Where to find login history:

- **Gmail:** `https://myaccount.google.com/security` → ”Your devices”
- **Facebook:** Settings → Security → Where You’re Logged In
- **Amazon:** Account → Login & Security → Secure Your Account
- **Banks:** Varies by institution; look for ”Security Center” or ”Activity Log”

CRITICAL ACTION

If you see unauthorized activity:

1. Screenshot everything (you may need evidence)
2. Log out all other sessions immediately
3. Change password again
4. Contact the company’s fraud department
5. File a police report (yes, really—you’ll need it for identity theft affidavits)

3.2 Monitor Financial Accounts

Even if the breach didn’t include financial data, criminals may try credential stuffing on banking sites.

☑ Action Checklist

Check your financial accounts:

Bank account transactions (last 30 days)

Credit card charges

PayPal, Venmo, Cash App activity

Investment account activity

Cryptocurrency exchange activity

Set up alerts:

- Enable transaction notifications for amounts over $1 (catches small test charges)
- Enable login alerts (notify you of any new login)
- Enable change alerts (notify you of address, phone, or email changes)

3.3 Update Security Questions

If the breach included personal information (DOB, address, mother's maiden name), your security question answers may now be public knowledge.

Pro Tip

Security questions are inherently insecure. The ”right” answers are often findable online.
Better approach: Treat security questions as secondary passwords:

- Question: ”What's your mother's maiden name?”
- Don't answer: ”Smith”
- Instead answer: Random string like ”9kF$mPqL2x”
- Store these ”answers” in your password manager

This way, even if someone knows your actual mother's maiden name, they can't use it.

3.4 Check for Phishing Attempts

After breaches, criminals send phishing emails that **reference the breach** to seem legitimate.

⚠ Warning

Watch for emails like:

- ”Urgent: Verify your account after the [Company] breach”
- ”You must update your information due to security incident”
- ”Click here to see if you were affected”

These are scams. Legitimate companies:

- Don’t send urgent action links via email
- Don’t ask for passwords or SSN via email
- Provide information at their official website, not via email links

How to verify legitimacy:

1. Don’t click links in emails
2. Go directly to the company’s website by typing URL
3. Look for official breach notification on their homepage
4. Call customer service using number from official website (not email)

4 First Week: Credit Protection

4.1 Place Fraud Alerts

A fraud alert requires creditors to verify your identity before opening new accounts in your name.

How to place fraud alert:

1. Contact **one** of the three major credit bureaus
2. They are required to notify the other two
3. Fraud alert lasts 1 year (renewable)

Contact information:

- **Equifax:** https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ or 1-800-525-6285
- **Experian:** https://www.experian.com/fraud/center.html or 1-888-397-3742
- **TransUnion:** https://www.transunion.com/fraud-alerts or 1-800-680-7289

4.2 Freeze Your Credit (Recommended)

Credit freeze vs. fraud alert:

	Fraud Alert	**Credit Freeze**
Protection	Creditors must verify identity	Blocks all new credit applications
Duration	1 year	Until you unfreeze
Cost	Free	Free (since 2018)
Applying for credit	Creditor does extra verification	You must unfreeze first
Recommendation	Minimum protection	**Best protection**

How to freeze your credit:
You must freeze with **all three bureaus** separately:

1. **Equifax:** https://www.equifax.com/personal/credit-report-services/credit-freeze/ or 1-800-349-9960
2. **Experian:** https://www.experian.com/freeze/center.html or 1-888-397-3742
3. **TransUnion:** https://www.transunion.com/credit-freeze or 1-888-909-8872

Process:

- Create online account with each bureau
- Click ”Freeze” or ”Security Freeze”
- Save your PIN/password for unfreezing
- Repeat for all three bureaus (20-30 minutes total)

Pro Tip

When you need to unfreeze:

- Applying for credit card, loan, or mortgage
- Renting apartment (landlord credit check)
- Some job applications (employer background check)

You can unfreeze temporarily (e.g., 1 week) or permanently. Freezing and unfreezing are both instant and free.

Action Checklist

Credit Freeze Checklist:

Freeze Equifax credit report

Freeze Experian credit report

Freeze TransUnion credit report

Save all PINs/passwords in password manager

Consider also freezing Innovis and ChexSystems (smaller bureaus)

4.3 Review Your Credit Reports

You're entitled to one free credit report per year from each bureau via https://www.annualcreditreport.com.

What to look for:

- Accounts you didn't open
- Hard inquiries you didn't authorize
- Incorrect personal information
- Addresses where you never lived

If you find fraudulent activity:

1. Dispute it immediately with the credit bureau
2. Contact the creditor's fraud department
3. File identity theft report at https://www.identitytheft.gov

4.4 Monitor Your Credit Going Forward

Free monitoring options:

- **Credit Karma:** Free credit score monitoring (TransUnion + Equifax)

- **Experian (free tier):** Monitor Experian report
- **Bank/credit card apps:** Many offer free FICO score tracking

Paid monitoring ($10-$30/month):

- All three bureaus monitored
- Dark web monitoring for your SSN/credentials
- Identity theft insurance (typically $1M coverage)
- Dedicated fraud resolution specialist

Our take: Paid monitoring is valuable if the breach included SSN or financial account data. Otherwise, free tools are sufficient.

5 Special Situations

5.1 If SSN Was Breached

! CRITICAL ACTION

Social Security Number breaches are the most serious. Take these additional steps:

1. **File identity theft report:** https://www.identitytheft.gov (creates FTC affidavit)
2. **Request IRS IP PIN:** Prevents tax fraud (https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin)
3. **Consider credit monitoring service:** Paid service with identity theft insurance
4. **Monitor SSA account:** Create account at https://www.ssa.gov/myaccount/ to prevent fraudulent benefit claims
5. **Alert employer:** Warn HR about potential unemployment fraud in your name

5.2 If Medical Records Were Breached

Medical identity theft is uniquely dangerous because fake medical records can lead to wrong treatment.

Actions:

1. Request copy of your medical records from all providers
2. Review for treatments/prescriptions you didn't receive
3. Place alert with Medical Information Bureau (MIB): 1-866-692-6901
4. Monitor health insurance Explanation of Benefits (EOBs)
5. Report fraudulent claims to insurance company immediately

5.3 If Children's Data Was Breached

Minors' identities are valuable to criminals because fraud often goes undetected for years.

Actions:

1. Check if your child has a credit file (they shouldn't unless they're 18+)
2. If file exists, it may indicate fraud—freeze it immediately
3. Request child identity theft report at https://www.identitytheft.gov
4. Consider freezing child's credit proactively (prevents file creation)

5.4 If Employer Data Was Breached

Work email and credentials compromise both personal and corporate security.

Actions:

1. Notify your IT/security team immediately (they may have incident response procedures)
2. Change work password and enable 2FA
3. Review access to corporate systems, files, and sensitive data
4. Watch for business email compromise (BEC) scams targeting you
5. Don't reuse work passwords for personal accounts (or vice versa)