Data Breach & Third-Party Exposure

Responding to A Third-Party Exposing Your Personal Data

A data breach or third-party exposure occurs when an organization you trusted, such as a company, school, healthcare provider, employer, or service, experiences a security incident that exposes your personal information.

You did not do anything wrong. These incidents happen outside your control, but how you respond next matters.

Breached data may include:

- Name, address, email, phone number
- Username/passwords (hashed or plain)
- Social Security number or government ID
- Financial or banking information
- Medical or insurance data
- Student records or education data

Breaches often lead to delayed scams, identity theft, or targeted impersonation attempts.

Data Breach – Do This First

Read the Breach Notice Carefully

Before taking action:

- Identify what data was exposed
- Note when the breach occurred
- Check what the organization is offering (credit monitoring, identity protection)
- Save the notice (email or letter)

Not all breaches carry the same risk, response should match exposure type.

Do Not Panic or Pay for "Emergency Fixes"

- Do not buy services pushed by unsolicited callers or emails
- Do not click links claiming to "secure your identity" unless verified
- Do not assume fraud has already occurred

Scammers frequently exploit breach announcements.

Preserve Documentation

Create a folder (digital or physical) and save:

- Breach notification letters or emails
- Dates you were notified
- Name of the affected organization
- Any reference or case numbers provided

This documentation supports disputes, reporting, and future protection.

Match Your Response to the Type of Data Exposed

If Login Credentials Were Exposed

- Change passwords for the affected service immediately
- Change passwords on any other accounts using the same or similar password
- Watch for login alerts or password reset emails

If Financial Information Was Exposed

- Monitor bank and credit card statements closely
- Contact financial institutions if suspicious activity appears
- Be alert for phishing pretending to be your bank

If Social Security Number or Government ID Was Exposed

- Strongly consider placing a credit freeze or fraud alert
- Monitor credit reports for new accounts or inquiries
- Changing an SSN is rare and only available in limited circumstances. Focus on credit freezes, fraud alerts, monitoring, and IdentityTheft.gov recovery planning.

If Medical or Insurance Data Was Exposed

- Review Explanation of Benefits (EOBs) carefully
- Watch for bills for services you did not receive
- Be alert for fake medical or insurance calls

If Student or Education Data Was Exposed

- Monitor for loans, accounts, or aid you did not apply for
- Secure school and education portals
- Consider credit protection for minors or young adults

Credit Protection Options

A credit freeze is free, reversible, and available to anyone. Fraud alerts are also free. You may choose one or both depending on exposure severity.

Fraud Alert

- Warns lenders to verify identity before opening new credit

- Typically lasts one year
- Useful when exposure risk is moderate

Credit Freeze

- Prevents new credit from being opened without your approval
- Strongest protection for SSN exposure
- Free and reversible

Watch for Follow-On Scams

After a breach, criminals may:

- Impersonate the breached organization
- Claim to offer “free recovery services”
- Send phishing referencing the breach
- Attempt account takeovers using leaked data
- Expect increased scam attempts for several months.

Report Problems If They Appear

If Fraud or Identity Misuse Occurs - Report It

- National Reporting
  - Federal Trade Commission (FTC)
    - Main federal agency for consumer and identity fraud
    - reportfraud.ftc.gov
    - https://www.identitytheft.gov
  - Health & Medicare Reporting
    - Medicare Fraud: 1-800-MEDICARE (1-800-633-4227)
    - https://www.medicare.gov
  - Internet Crime Complaint Center (IC3) – FBI
    - Tracks internet-based financial crimes and scams
    - ic3.gov
  - U.S. Postal Inspection Service
    - If the scam involved mailed checks, money orders, or parcels
    - uspis.gov/report
  - Secret Service Cleveland Field Office
    - Investigates certain cyber-enabled financial crimes; use FTC, IC3, or local law enforcement for routine consumer scam reporting
    - 216-750-2058
- Ohio Resources
  - Ohio Attorney General – Consumer Protection & Identity Theft
  - https://www.ohioattorneygeneral.gov
  - Consumer Protection Hotline: 800-282-0515
- Geauga County
  - Geauga County Sheriff’s Office

- https://www.geaugasheriff.org
- Local police non-emergency line for documentation
- Call 911 if threats, coercion, or immediate danger are involved

Law enforcement can document identity crimes and support recovery.

Recovery – Ongoing Protection

- Review accounts and credit reports regularly; free weekly credit reports are available through AnnualCreditReport.com
- Keep breach documentation long-term
- Expect breach-related scams to resurface periodically
- Avoid sharing personal information reactively
- A breach is not a one-day event, it's a monitoring phase.

How to Reduce Harm After a Breach

- Treat all unexpected contact as suspicious
- Verify organizations independently
- Do not rush decisions under pressure
- Keep records organized
- Ask for help if something feels off
- Add a trusted contact where your financial institution offers it