



## DATA BREACH RESPONSE CHECKLIST: COLLECTION OF INFORMATION REGARDING BREACH

*Privileged and Confidential Attorney-Client Communication. This document was prepared at the direction of counsel for the purpose of obtaining legal advice.*

Jennifer A. Puplava  
(616) 632-8050  
jpuplava@mikameyers.com

### 1. IMMEDIATE ACTION STEPS – Containment and Continuity.

- a. Engage response team.
  - i. Internal decision makers, subject matter experts, employees having best knowledge of facts.
  - ii. External service providers:
    - (1) Insurance carrier.
    - (2) IT/forensic experts.
    - (3) Attorney.
      - (a) preserve or obtain work product privilege
      - (b) communications regarding incident/response with attorney are protected under attorney-client privilege

- b. Do NOT delete, move or alter files, contact suspected perpetrators, or do forensic analysis (yet).
- c. Isolate affected systems to prevent further intrusion, loss or data or other damages.
- d. Preserve pertinent system logs.
- e. Make and secure backup copies of damaged or altered files.
- f. Identify where affected system resides in network.
- g. Identify all systems that connect to affected system.
- h. Identify all programs and processes that operate on affected system.
- i. Make arrangements for continuity of services.
- j. Use reasonably secure means to communicate – email traffic may be monitored.
- k. Activate auditing software (if not already activated).
- l. Consider whether to contact law enforcement (local, state, FBI, depending on circumstances), but keep intrusion details in confidence within response team until a decision is made to take further steps.
- m. Document all mitigation efforts for later analysis.

## 2. CONTINUING ACTIONS – Information gathering.

**Information is needed to determine next steps, such as notices. Document and describe incident-related events, including dates and times. Keeping records will help reduce possible future liability.**

- a. How was the data accessed? (breach through online connection, stolen laptop, etc.)
- b. Do you know (or do you suspect) who accessed the data?
- c. When did the intrusion(s) occur?
- d. When was the intrusion discovered?
- e. Who discovered the intrusion?
- f. How was the intrusion discovered?
- g. Have you been contacted with a ransom or similar demand? Who contacted you and what was your response? Who within your organization communicated with third parties regarding the ransom?
- h. Describe incident-related phone calls, emails, and other contacts (compile copies where appropriate).
- i. What other documentation do you have of the intrusion? (Keep all records!)
- j. Identify the systems, networks, and devices affected by the incident, and describe how affected.
  - i. Who had contact with the affected system? What did they do?
  - ii. Identify all hardware affected by or lost in the breach.
  - iii. Identify all data lost in the breach (i.e., data that is not inaccessible).
  - iv. Have you preserved log files and other information

- associated with the misappropriation?
- v. Identify all personnel who will be necessary to analyze and address the breach.
  - vi. Have you stopped additional data loss? How? (e.g., changing security access or passwords, disconnect affected system, etc.)
  - vii. Is any physical evidence in the possession of a third party (e.g., cloud providers)?
- k. Identify all data affected by the incident, and describe how affected (e.g.: data accessed, data lost, etc.) For all affected data, also describe:
- i. Is the data yours, owned by you, or licensed by you?
    - (1) If the data is owned or licensed by someone else, who is it owned or licensed by? (e.g.: are you a vendor doing work for a third party, and the data relates to that third party's employees?)
    - (2) An entity that owns/licenses the data has different notification requirements than an entity that maintains or works with the data but does not own/license it.
  - ii. If you possess, work with, or maintain the data for another organization, describe that organization (e.g., healthcare

- provider, financial institution, or other regulated entity or handler of sensitive information).
- iii. Who are the data subjects for the affected data (e.g., employees, customers, students, patients, etc.)
  - iv. Specify whether affected data is personally identifiable (name, address, telephone number, financial information).
  - v. Specify whether the affected data includes Protected Health Information under HIPAA (individually identifiable health information)
  - vi. Specify whether the affected data includes Nonpublic Personal Information under the Graham Leach Bliley Act (i.e., personally identifiable financial information provided by a consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer, or otherwise obtained by a financial institution.)
  - vii. Does the affected data consist of information about students of an educational institution?
  - viii. Does any part of the affected data consist of social security numbers?
  - ix. Does any part of the affected data pertain to children under the age of 13?

- x. Does any part of the affected data pertain to one or more citizens of any member state of the European Union?
- xi. Do you have any indication that the affected information has been used or distributed by the intruder? If so, describe how and to whom.

1. Geographical information

- i. Of what other states or jurisdictions are the data subjects residents/citizens?  
Many states have their own data breach notification statutes, so it will be important to identify the number of affected residents in each state.
- ii. Are you a private or a governmental entity?
- iii. In what state or other jurisdiction are you organized?
- iv. In what states are you qualified to do business (e.g., by government filing)?
- v. In what states do you do business?

**3. CONTINUING ACTIONS – Assess reporting obligations.**

- a. Assess reporting obligations under applicable law(s) with your attorney.
  - i. reporting to data owners
  - ii. reporting to data licensors/licensees

- iii. reporting to governmental entities
  - iv. reporting to third parties (e.g., consumer reporting agencies, etc.)
- b. Is there any reason to delay notification to affected individuals? (e.g., law enforcement, prejudice to ongoing investigation, risk to data subjects, etc.)
  - c. Have you notified law enforcement or similar personnel about the breach? If so, when, and who has been notified?
  - d. Do you have a privacy policy that addresses data breaches? If so, what does it say?
  - e. Do you have contractual obligations (with clients, vendors, other third parties, etc.) that address data breaches? If so, what do they say?
  - f. Does your insurance cover data breaches, and if so, have you contacted your insurer?
  - g. Do you have a PR firm or otherwise identified a spokesperson?
  - h. Determine whether to provide credit monitoring or identity theft protection services to affected individuals.
4. **CONTINUING ACTIONS -- Coordinate drafting of notifications with response team.**
5. **CONTINUING ACTIONS – Update information security plan to both mitigate past breaches and reduce future vulnerabilities.**