Security Incident Response Timeline & Considerations

Summary

This Security Incident Response Timeline & Considerations ("Timeline") provides guidance on the recommended procedures and actions in the event a company suspects a data Security Incident or Security Breach involving personal other proprietary data. This Timeline may also be used to evaluate a suspected Incident or Breach and determine whether the Incident or Breach triggers notification to customers, individuals, regulators, and/or consumer reporting agencies ("CRA"). Please note that each incident will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks and data involved as the basis for deciding what actions to take next, given the circumstances. A company may have varying obligations based on whether the Incident or Breach involves the company's own data or the company's customer data.

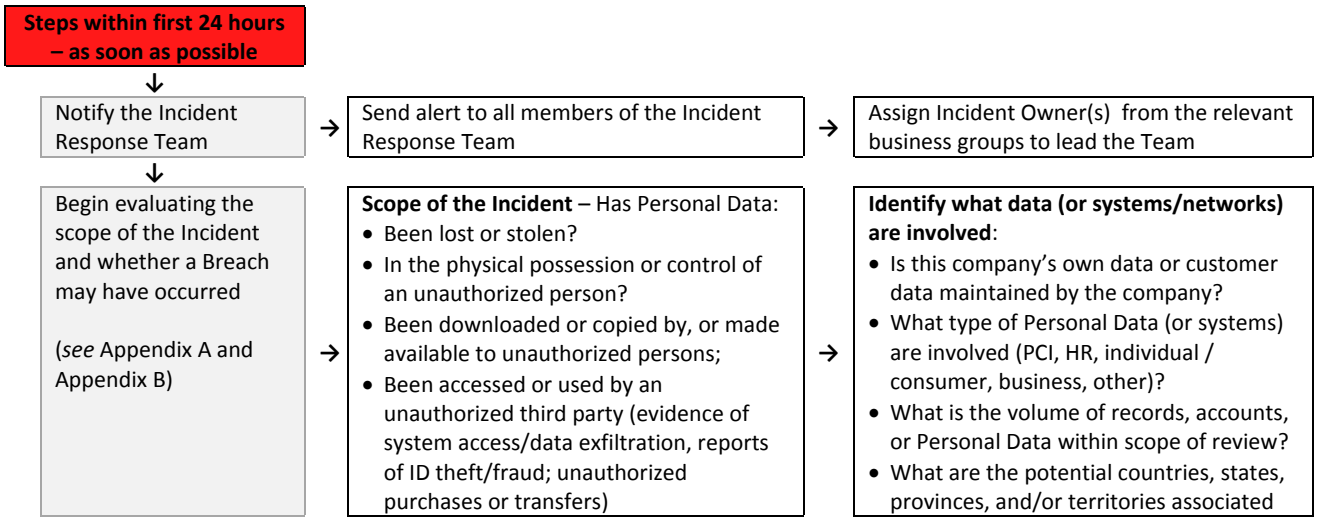
Relevant Definitions

1. **Personal Data**: Information relating to an identified or identifiable individual. The definition of Personal Data may vary based on the geographic location and legal requirements. See Appendix A for additional guidance.

2. **Security Incident** (or "**Incident**"): The attempted or successful *unauthorized* (a) access to or acquisition of a company's confidential information or the company's customer data, including financial account credentials, (b) modification to a network, interference with system operations in an information system, and/or (c) denial of services / network resources. Upon investigation, an Incident may be elevated to be a Breach.

3. **Security Breach** (or "**Breach**"): An actual or reasonably-suspected theft, loss, or unauthorized acquisition, access to, or disclosure of (a) Personal Data,(b) the company's confidential information or the company's customer information – maintained or controlled by, or on behalf of, the company that may compromise the security, confidentiality, or integrity of such information. This includes corporate or individual account takeover situations or other use of confidential information to transfer or divert funds to the culprit or related accomplices. Determination of whether an Incident is a Breach is a legal determination to be made by the company's counsel in consultation with the group of company employees designated to respond to cybersecurity events ("Incident Response Team"). The Incident Response Team should be a predetermined and include stakeholders from the company's relevant business and compliance functions.

Procedure when an Incident or Breach is Suspected



Have systems/networks been accessed or compromised such that unauthorized access to Personal Data or customer data is reasonably expected or cannot be disproven?

with such records (e.g., state of residency, place of business)?
- Is a vendor or customer involved? If so, who?

↓

Take immediate actions to start containing the Incident/Breach and recover stolen funds if possible

↓

Does it involve a Critical Incident? [1]
- **If YES**: Consult company management and legal counsel immediately for guidance.

↓

Notify outside counsel

Steps within first 24-48 hours

↓

Convene the Core Incident Response Team

→

Meet and discuss what the Team has been able to determine so far, including:
- Scope of Incident;
- Type(s) of data involved;
- What steps have been taken to contain the Incident;
- What type of harm to the individuals may result from the Incident;
- What steps have been take to reduce/eliminate the harm to the individuals;
- Whether to hire a third-party forensic vendor to assist in investigation/verification of containment; and
- Whether to notify law enforcement.

↓

Determine whether customer, individual, regulator, and/or CRA notification is required, and whether online credentials should be reset and for whom

(*see also* Appendix C)

→

The Legal Team should work in conjunction with outside counsel to determine:
- Whether an Incident and/or Breach may have occurred;
- If the Incident / Breach involves online credentials, whether a prompt credential reset should occur urgently;
- Whether customer, individual, regulator, and/or CRA notification is required in the applicable jurisdictions or pursuant to contract;
- Whether there is a contractual obligation to notify (*e.g.*, insurance carrier; vendors; payment card brands / processors); and
- Whether the company will provide free ID theft/credit monitoring services;
- Whether a litigation hold should be issued at the company to preserve records and pause any automatic destruction of documents under a documentation retention program.

↓

Notify law enforcement, if applicable

→

If the company reasonably believes that a Breach has occurred, determine whether to report the Breach to appropriate law enforcement agencies (separate from any regulator notice requirement). Considerations for notifying law enforcement include:
- If a physical intrusion is involved;
- Attack involves known actor (rogue employee / known third party) and the company may bring legal action;
- Type of attack / forensic evidence indicates presence of a nation/state attack; or
- Type of attack / forensic evidence indicates presence of sophisticated criminal activity.

Document such communications. Decision to notify law enforcement may extend beyond initial 48 hours as facts of the Breach develop.

Steps within first 48-72 hours

↓

[1] "Critical Incidents" include any (1) probable or realized data loss of restrictive or confidential data; (2) negative (safety, experience) impact to greater than 50% of the company in the ability for employees to do their work; or (3) negative impact to greater than 50% of customers.

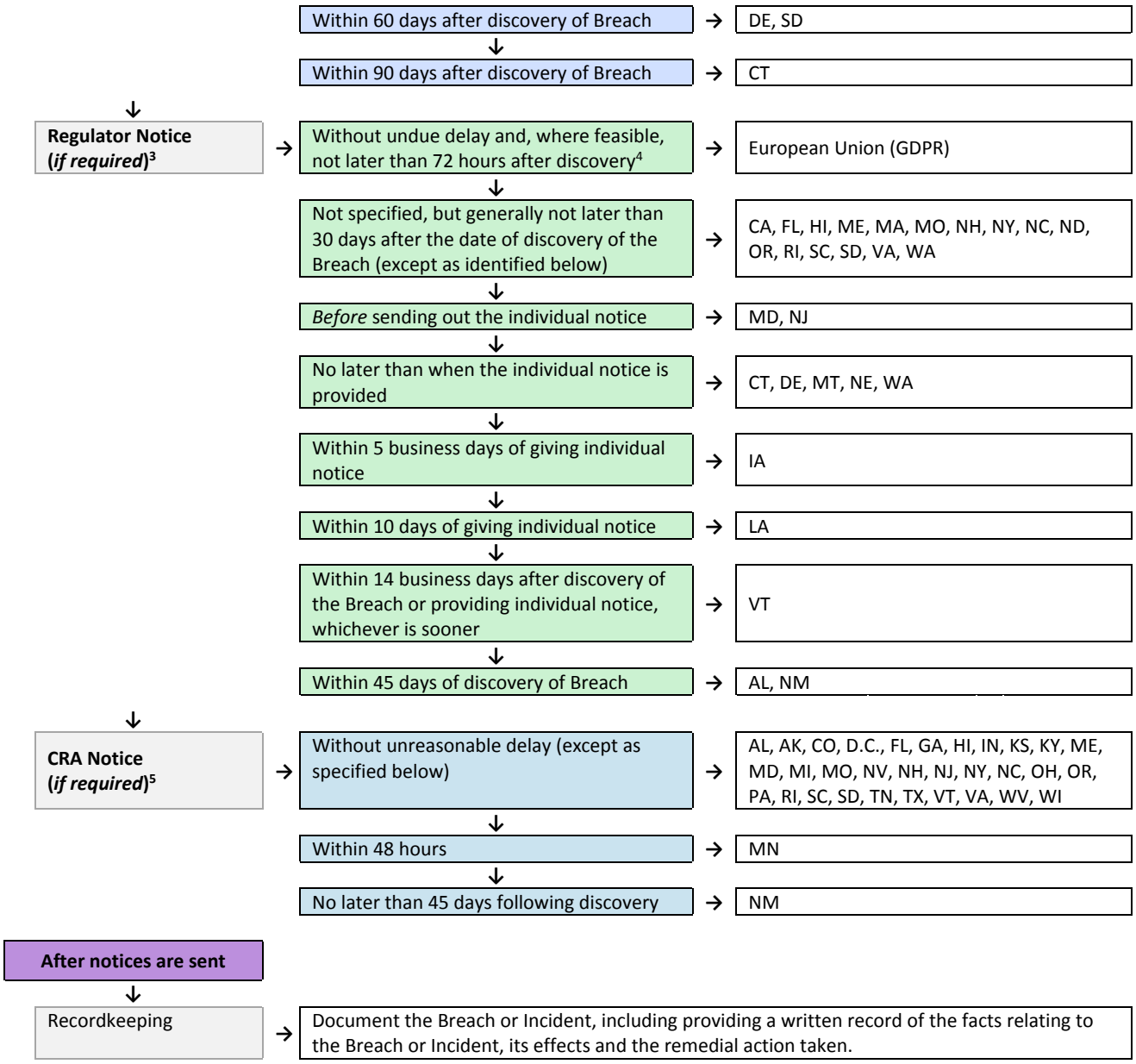
Contact insurance company (if applicable)	Determine whether an existing insurance policy may provide coverage for the Incident / Breach. Insurance policies may require notice within a specified period of time (even if the facts of the Incident / Breach are still developing) in order to make a claim. Provide only the information required to put the insurance carrier on notice of a potential claim.
Contact applicable business partners	This may include, as applicable: • Vendors to support incident response (call center, PR, ID Theft/Monitoring); • Impacted customer(s); • Merchant/Acquiring Bank; • Payment processor/gateway; • Payment card brands (often through bank/processor). Notification obligations may vary depending on contract obligations and customer relationships.
Consider whether to contact PR/crisis management firm	Depending on the number of individuals affected and the type of Personal Data (or customer data) at issue, the company may consider hiring a PR/crisis management firm to assist

Over the following week

Draft notice documents	If there are obligations to notify affected individuals, regulators, and/or CRAs, the company may, with outside counsel support and (if applicable) the PR/crisis management firm, draft the following documents required by law: • Individual notice; • Regulator notice (if applicable); • CRA notice (if applicable); • Customer or insurance carrier written notice (initial/supplemental).
Draft other public Documents	Consider whether it is necessary to draft other documents including any individual FAQs, website statement, media FAQs, holding and reactive statements, and/or business partner/vendor FAQs.
Order ID Theft/credit monitoring package	Whether ID Theft/credit monitoring is necessary will depend on the type of Personal Information subject to the Breach.
Establish call center support	Even if the company does not need to hire external call support, it should provide internal/external training regardless to handle calls concerning the Incident/Breach, and to document appropriately number of/escalation/resolution of such calls.

Send Notices	**Timeframe for sending notices**	
Individual Notice (*if required*)	Without undue delay[2]	European Union (GDPR)
	Most expedient time possible and/or without unreasonable delay; as soon/quickly as possible (except as specified below)	AK, AZ, AR, CA, CO, D.C., GA, HI, ID, IL, IN, IA, KS, KY, LA, ME, MA, MI, MN, MS, MO, MT, NE, NV, NH, NJ, NY, NC, ND, OK, PA, RI, SC, TN, TX, UT, VT, VA, WA, WV, WY NOTE: CA and NC guidance recommend notifying within 10 business days
	Within 30 days of determination of Breach	FL, NM
	Within 45 days after discovery of Breach	AL, MD, OH, OR, RI, TN, WA, WI

[2] If Breach results in *high risk* to the rights and freedoms of individuals.



Appendix A: Types of Personal Data Triggering a Breach

What constitutes Personal Data that triggers data breach notification varies by jurisdiction and changes from time to time. Therefore, please confirm the exact definition of Personal Data to be applied for notice obligations in consultation with the company's legal team.

In the United States, all 50 states, the District of Columbia, Guam, Puerto Rico, and US Virgin Islands have data breach notification laws. The definition of Personal Data varies between the states. Below is a list of data types that amount to Personal Data in one or more U.S. states:

[3] Regulator notice is *not* required in the following US states: AK, AZ, AR, CO, DC, GA, ID, IL, IN, KS, KY, MI, MN, MS, NV, OH, OK, PA, TN, TX, UT, WV, WI, and WY.

[4] Regulator notice is required unless Breach is unlikely to result in risk to the rights and freedoms of individuals.

[5] CRA notice is *not* required in the following states: AZ, AR, CA, CT, DE, ID, IL, IA, LA, MS, NE, ND, OK, UT, WA, and WY. In MA and MT, CRA notice is required only in certain circumstances.

- An individual's first name or first initial and last name in combination with: (a) Social Security number or employer taxpayer ID number, (b) Driver's license, state, or tribal identification card number; (c) full date of birth; (d) passport number; (e) financial account number or credit or debit card number; (f) passwords, PINs, or other access codes for financial accounts; (g) medical information, or (h) health insurance information.
- A user name or email address in combination with a password or security question and answer that would permit access to an online account

In the European Union, Personal Data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Appendix B - Data Breach Examples

Type of Event	Examples
Unauthorized third party access	Personal information related to individuals were intentionally accessed by a third party hacker.
Online credential stuffing	An unauthorized third party uses online login credentials (email or username plus passcode) obtained from another source to log in to customer accounts.
Unauthorized internal access	Accessing or disclosing personal information outside the requirements or authorization of the employee's role that do not appear in good faith
Unintentional disclosure	Sending Personal Information to an unauthorized email or physical address, or disclosing data to an unauthorized recipient (*e.g.*, sending an unencrypted file with customer personal information to an unintended recipient).
Records not securely destroyed	Improper disposal of Personal Information (*i.e.*, hard disk, storage media or paper documents containing Personal Information sold or discarded before data is properly deleted).
Loss of computer or device	Loss of an employee laptop, mobile device, or data storage device (e.g., USB, CD) containing personal information

Appendix C: Decision to Notify

When it is determined that a Breach has occurred, the company's obligation to notify will vary based on whether the company is the data owner (i.e., it is the company's own data) or a the company customer is the data owner (i.e., the company maintains the data because the company is providing services to the customer).

When the company is the Data Owner

When the company is the data owner, the company must provide written notice informing individuals of a Breach affecting their Personal Data and including certain minimum details regarding the Breach, as required by applicable law. The applicable U.S. state law(s) depend on the individuals' locations of residence. Note that some states also permit email or telephonic notice, in lieu of a written letter.

- **State Regulatory Authorities**: Certain U.S. states and other jurisdictions require notification to regulatory authorities, depending on the number of potentially affected individuals in that state.
- **Consumer Reporting Agencies** ("CRA"): Certain U.S. states require notification to consumer reporting agencies, depending on the number of potentially affected individuals.

For Personal Data of individuals in the European Union, the company will need to provide notice as required by the GDPR and country-specific law(s) based on the company's locations in the EU and the individuals' location of residence. Consult the company's legal team.

If a decision has been made to notify the affected individuals, the following points must be considered:

- **Timing to notify**. The timing of notice to individuals, regulators, and/or CRAs depends on the jurisdiction. If a notification is required/recommended by local law, it must take place within the prescribed time. Otherwise, a notification should be made as soon as possible. Note, however, that the laws in this area continue to change, so consult with the legal team.
- **Who should notify**: The notification should be carried out by the legal team, in consultation with outside counsel.
- **How to notify**. The potentially affected individuals should be directly notified by email or letter, or other means as permitted by applicable law. The content of the notice to individuals, regulators, and CRAs depends on the U.S. state(s) or other jurisdiction where the individual is located. If for some reason the potentially affected individuals' contact information is not available, a notification should be considered either via a relevant the company's website or local media outlet, consistent with requirements under applicable law.
- **What to include in the notification**. The content of the notification will vary depending on the Breach and type of information involved. However, in all cases, the information will need to include details to assist the individual with reducing or preventing harm that could be caused by the data security incident and whom to contact for further information, as well as any other information required under applicable law.

When a Customer is the Data Owner

When a customer is the data owner (i.e., the company maintains the data because the company is providing services to the customer), and the company has determined that (a) there was a Breach under applicable law, or (b) the company has an obligation to notify the customer under the terms of the customer contract, the company must provide notice to the customer informing the customer of a Breach (or Incident) affecting the Personal Data (or other contractually designated data) maintained by the company on behalf of the customer. The notice should be provided in writing (for recordkeeping purposes). Consult the company's legal team for determination of obligations under applicable law and the customer contract, including obligations regarding timing and content of notice.

###