Security Incident Response Procedure Guide for Companies

May 2024

Payments Innovation Alliance®

Nacha®

Table of Contents

1.0 Introduction

Data breaches commonly involve financial information like credit card or bank account details, protected health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property.

When a data security breach or incident is discovered, the systems have likely been compromised for some time. According to the "IBM Cost of a Data Breach Report 2023," the overall mean time to identify and contain a security breach is 277 days or just over nine months.[1] While this figure has remained relatively consistent over the past few years, IBM reported the average cost of a data breach reached an all-time high in 2023 of $4.45 million. This represents a 2.3% increase from the 2022 cost of $4.35 million. This is a continuing trend; the 2023 average cost has increased 15.3% from the average cost of $3.86 million cited in the 2020 report.

Compromised companies need to respond quickly to minimize damage. The impact of an incident or breach on a company can be reputational damage, misuse or sale of intellectual property and confidential data, operational downtime and disruption, and lawsuits and fines. Customers, clients, business partners and other third parties may also be impacted. Share prices of breached companies hit a low point approximately 14 market days following a breach. Share prices fall 7.27% on average, and underperform the NASDAQ by minus 4.18%.[2]

Cybersecurity experts say that it is a question of "when, not if" a company will face a cybersecurity incident. It is therefore important for organizations to have a Cybersecurity Incident Response Plan. As discussed below, this "Security Incident Response Procedure Guide" ("Guide") is a starting point for discussions within an organization. It should be customized, however, in consultation with information technology, compliance and legal advisors, to fit your organizational structure and industry(s).

Disclaimer

This Guide does not constitute legal advice and is provided for general informational purposes only. Readers should contact their attorney to obtain advice with respect to any particular legal matter. No reader should act or refrain from acting on the basis of information in this Guide without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation.

The views expressed at, or through, this site are those of the individual authors writing in their individual capacities only – not those of their respective employers, Nacha, or the Payments Innovation Alliance. All liability with respect to actions taken or not taken based on the contents of this Guide is hereby expressly disclaimed. The Guide's content is provided "as is;" no representations are made that the content is error-free. Use of, and access to, this Guide or any of the links or resources contained within the site do not create an attorney-client relationship between the reader and the Guide's authors, contributors, or contributing law firms.

---

[1] https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=437000777238225555&p5=p&&msclkid=6967e0cf6d1d1b58f0fd857eebefea76&gclid=6967e0cf6d1d1b58f0fd857eebefea76&gclsrc=3p.ds

[2] https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/

2.0 Purpose/Scope

The Guide provides guidance on the recommended procedures and actions in the event a company reasonably suspects a Security Incident or Security Breach (as those terms are defined below) involving personal or other proprietary data.

The Guide may also be used to evaluate a suspected Incident or Breach and determine whether the Incident or Breach triggers notification to customers, individuals, regulators, credit card brands, the media, and/or consumer reporting agencies (CRA). Each incident will need to be assessed on a case-by-case basis, with consideration of the specific circumstances including the risks and data involved. A company may also have contractual obligations if the Incident or Breach involves the company's customer data.

3.0 Definitions

3.1 **Core Incident Response Team (**or "**Team**"**)**: The group of individuals responsible for responding to cybersecurity incidents. In addition to information technology specialists, it should include experts and leaders who can guide the organization in areas such as external communications, regulatory requirements and business continuity and recovery.

3.2 **Personal Data**: Information relating to an identified or identifiable individual, or similar definition under an applicable privacy law that requires notification in the event of a Breach of Personal Data. The definition of Personal Data may vary based on jurisdiction and legal requirements. See Appendix A for additional guidance.

3.3 **Security Incident (**or "**Incident**"**)**: The attempted or successful (a) unauthorized access to or acquisition of a company's confidential information or the company's customer data; (b) modification to the 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.

3.4 **Security Breach** (or "**Breach**"): An actual or reasonably-suspected theft, loss, unauthorized acquisition, disclosure of, or access to (a) personal data; (b) the company's confidential information; or (c) customer information – maintained or controlled by, or on behalf of, the company that may compromise the security, confidentiality, or integrity of such information. **Whether an Incident is a Breach is a legal determination to be made by the company's Legal Team in consultation with the Core Incident Response Team.** All communications referencing a security event should refer to that event as an Incident until instructed otherwise by the company's Legal Team.

4.0 Procedure when an Incident or Breach is Suspected

Time is of the essence to effectively respond to a suspected Incident or Breach. The types of data lost or stolen, the extent of the data loss, and the governing federal and state laws are key considerations for a company's response. This Guide provides suggested actions based on time sensitivity.

Steps within first 24 hours – ASAP

- Notify the Core Incident Response Team → Send alert to: <email address/slack channel/text/phone> → Assign Incident Owner(s) from the relevant business groups to lead the Team
- Begin evaluating the scope of the Incident and whether a Breach may have occurred (see Appendix A and Appendix B)

Scope of the Incident:

- Has Personal Data:
  - Been lost or stolen?
  - Been in the physical possession or control of an unauthorized person?
  - Been downloaded or copied by, or made available to unauthorized persons?
  - Been accessed or used by an unauthorized third party (evidence of system access/data exfiltration, reports of ID theft/fraud; unauthorized purchases)?
- Have systems/networks been accessed or compromised such that unauthorized access to Personal Data or customer data is reasonably expected or cannot be disproven?

Identify what data (or systems/networks) are involved:

- Is this the company's own data or customer data maintained by the company?
- What type of Personal Data (or systems) are involved (PCI, HR, individual/consumer, business, other)?
- What is the volume of records, accounts, or Personal Data within scope of review?
- What are the potential countries, states, provinces, and/or territories associated 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
- Notify outside counsel
- Does it involve a Critical Incident? [3]

[3] "Critical Incident" is defined based on the organization's business criteria. For example, an organization may define a "Critical Incident" to 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 OR negative impact to greater than 50% of cloud or hybrid-based customers. The definition, however, may be more general. The NIST definition is, "A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery."

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 taken to reduce/eliminate the harm to the individuals. • Whether to hire a third-party forensic vendor to assist in investigation/verification of containment. • 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). • 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 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

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. • Correspondent banks and credit unions. • 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.[4]	[If Applicable] European Union/United Kingdom (GDPR).
	Most expedient time possible and/or without unreasonable delay; as soon/quickly as possible (except as specified below).	AK, AR, CA, CO, DC, GA, HI, ID, IL, IA, KS, KY, MA, MI, MN, MS, MO, MT, NE, NV, NH, NJ, NY, NC, ND, OK, PA, SC, TX, UT, VA, WV, WY. NOTE: CA and NC guidance recommend notifying within 10 business days.
	Within 30 days of determination of Breach.	FL, ME, WA.
	Within 45 days after discovery of Breach.	AL, AZ, IN, MD, NM, OH, OR, RI, TN, VT, WI.
	Without unreasonable delay, and in no case later than/within 60 days after discovery of Breach.	CT, DE, LA, SD, TX. FTC - Health Breach Notification Rule. HIPAA - Breach Notification Rule.
Regulator Notice (if required)[5]	The most expedient time possible without undue delay.	UT.
	Without undue delay and, where feasible, not later than 72 hours after discovery.[6]	European Union (GDPR). Without undue delay: MA, MO, NC, ND, RI, SC, VA.
SEC	Within four days of the company's determination that the Incident is material or will result in material changes for investors, and updates without undue delay.	SEC Disclosure Requirements (Form 8-K).
	Not specified, but generally not later than 30 days after the date of discovery of the Breach (except as identified below).[7]	CA, DC*, HI*, ME, NH, NY, SD.
	Before sending out the individual notice.	MD, NJ.
	No later than when the individual notice is provided.	CT, DE, MT.
	Within 5 business days of giving individual notice.	IA.

[4] If Breach results in high risk to the rights and freedoms of individuals.
[5] Regulator notice is not required in the following U.S. states: AK, GA, ID, KS, KY, MI, MN, MS, NV, OH, OK, PA, TN, WV, WI and WY.
[6] Regulator notice is required unless Breach is unlikely to result in risk to the rights and freedoms of individuals.
[7] Asterisk* denotes that regulator notice is required to be provided in most expedient time.

SEC	Annually.	SEC: Form 10-K disclosure regarding risk strategy, separate disclosures regarding data governance.
FTC	Within 10 days of discovering an incident involving 500+ individuals.	FTC: Health Breach Notification Rule events involving 500+ individuals.
	Within 10 days of giving individual notice.	LA.
	Within 14 business days after discovery of the Breach or providing individual notice, whichever is sooner.	VT.
	As soon as possible and no later than 30 days after discovery of Breach.	FTC – GLBA Safeguards Rule (16 C.F.R. 314.4).
	Within 30 days after Breach.	CO, FL, WA.
	Within 45 days of discovery of Breach.	AL, AR, AZ, NM, OR.
HHS Secretary	Without unreasonable delay but in no case later than 60 days following discovery of Breach.	HIPAA Breach Notification Rule. Note: Must also provide notice to prominent media outlets if Breach affects 500+ individuals.
FTC; HHS Secretary	Within 60 calendar days following calendar year.	FTC: Health Breach Notification Rule events involving <500 individuals. HIPPA, HHS Secretary notice for Breaches affecting <500 individuals.
CRA Notice (if required)[8]	Without unreasonable delay (except as specified below).	AL, AK, CO, D.C., FL, GA, HI, IN, KS, KY, ME, MD, MI, MO, NV, NH, NJ, NY, NC, OH, OR, PA, RI, SC, SD, TN, TX, UT, VT, VA, WV, WI.
	Within 48 hours.	MN.
	No later than 45 days following discovery.	AZ, NM.

After notices are sent

Recordkeeping	Document the Breach or Incident, including providing a written record of the facts relating to the Breach or Incident, its effects and the remedial action taken.

[8] CRA notice is not required in the following states: AZ, AR, CA, CT, DE, ID, IL, IA, LA, MS, NE, ND, OK, WA and WY. In MA and MT, CRA notice is required only in certain circumstances such as thresholds of affected residents.

5.0 Forward Looking

Companies bear the responsibility for protecting customer data, and mitigating Incidents and Breaches. Companies should have comprehensive disaster recovery and incident response plans in place, conduct periodic employee training and testing, audit and review their systems as appropriate and employ threat detection and response technologies.

Reducing the breach lifecycle can translate into significant cost reductions. On average, the cost difference between breaches that took less than 200 days to find and resolve was 23% lower – or $1.02 million – than breaches that took more than 200 days to find and resolve.

Security artificial intelligence (AI) and automation tools may be used to reduce the time to identify and contain a breach. The "IBM Cost of a Data Breach Report 2023," revealed that responding organizations that extensively used extensive security AI and automation reduced the time to identify and contain a breach by more than 100 days.[9]

[9] https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700077723822555&p5=p&&msclkid=6967e0cf6d1d1b58f0f-d857eebefea76&gclid=6967e0cf6d1d1b58f0fd857eebefea76&gclsrc=3p.ds

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 U.S. Virgin Islands have data breach notification laws. The definition of Personal Data varies between jurisdictions. Below is a list of data types that amount to Personal Data in one or more U.S. states:

- 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 username or email address in combination with a password or security question and answer that would permit access to an online account.

Federal privacy laws are sector specific and have varying definitions of the class of data that the statutes are meant to protect, or that trigger a notification obligation in the event of an Incident or Breach. The definitions of data that trigger a notification obligation include:

- Health Insurance Portability and Accountability Act (HIPAA): A breach occurs where a healthcare entity, known as a covered entity or business associate, experiences the unauthorized disclosure of unsecured protected health information (PHI). PHI is any information in an individual's medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a healthcare service such as diagnosis or treatment. This includes payment information.
- Graham-Leach-Bliley Act (GLBA): This law and the related Safeguards Rule applies to "financial institutions" and has breach reporting obligations triggered by the unauthorized acquisition of unencrypted, personally identifiable, nonpublic financial information (NPI). NPI includes any information that a consumer provides to a financial institution to obtain a financial product or service or that the financial institution otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.
- Health Breach Notification Rule: Promulgated and enforced by the Federal Trade Commission (FTC), this rule has reporting obligations triggered by the unauthorized access of Personal Health Records (PHR). PHR is an electronic health record that can be "drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."

Companies that process financial transactions using payment card information are also subject to the self-regulatory standards maintained by the Payment Card Industry (PCI) Security Standards Council, which is comprised of the credit card brands American Express, Discover, JCB, Mastercard, and Visa. The PCI Data Security Standards (DSS) set security safeguards for systems processing customer financial data. Where that information is Breached, impacted companies need to assess their reporting obligations to individuals and regulators, but also to the card brands.

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	A third-party hacker intentionally accessed personal information. Note that the update Safeguards Rule and Health Breach Notification Rule cover instances where a company exceeds a consumer's authorization when sharing Personal Data with even a "friendly" third party.
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).
Ransomware	Unauthorized threat actor access to Personal Data causing the loss of integrity of that data, or in some cases, the acquisition of Personal Data.
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 the company's 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, it 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, sometimes depending on the number of potentially affected individuals in that state.
- Federal Regulatory Authorities: Federal sectoral privacy laws and regulations such as the Graham-Leach-Bliley Act (GLBA) and Safeguards Rule, the Health Insurance Portability and Accountability Act (HIPAA) and Breach Notification Rule, and the Health Breach Notification Rule promulgated by the FTC, require notice to individuals, and where a certain number of individuals are affected, notice to regulators. The number of affected individuals may determine whether the company has an affirmative duty to notify a regulator, or it may determine the timing of the notification.
- Media Outlets: State data breach notification laws permit substitute notice where a company may not be able to establish the identity of the affected individuals. This may include notifying prominent media outlets and advertising the fact of the Incident or Breach. Other laws and regulations, such as the HIPAA Breach Notification Rule, require notice to the media when a particular threshold of affected individuals is met.
- 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. The GDPR requires notification of the lead supervisory Data Protection Authority within 72 hours, and notification to individuals based on a risk-based standard.

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 company 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 it has determined that (a) there was a Breach under applicable law; or (b) it 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 it 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.

Acknowledgements & Additional Resources

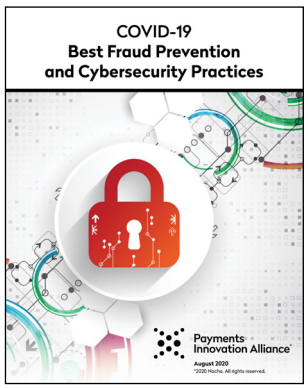
Payments Innovation Alliance – Cybersecurity & Payments AI Project Team

The Guide was developed by the Cybersecurity & Payments AI Project Team of Nacha's Payments Innovation Alliance, with special recognition to Matt Luzadder and Elliott Siebers with Kelley Drye & Warren LLP.

The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions. The Alliance established the Cybersecurity & Payments AI Project Team to help organizations understand and respond to evolving threats related to potential cyberattacks. Visit Cybersecurity & Payments AI Project Team to see more resources developed by the team, including:

Cybersecurity Tabletop Exercise for Small to Medium-Sized Businesses

COVID-19 Best Fraud Protection and Cybersecurity Practices



These resources may be downloaded and shared with employees, colleagues, and clients as appropriate. If you'd like more information on the Payments Innovation Alliance, including the work we have done and how your organization can get involved, please visit nacha.org/payments-innovation-alliance.