Not All Data Breaches Are Equal

Understanding Sensitivity and Consequences

Our colleagues at FTI Consulting investigate cybersecurity incidents on a daily basis, including determining the post-incident impact, discerning whether reasonable measures were taken by the organization, and assisting with client's regulatory obligations that are triggered by the incident. In this article, we unpack the different types of data, the risks and threat landscape associated, the regulatory environment and the real-world threats and regulatory actions that we have seen arise from incidents, and we take a forward-looking view at how organizations can best prioritize their risk management strategies for protecting data. For the purposes of this discussion, a cybersecurity incident is any event that threatens systems or data, while a data breach is the subset of incidents where sensitive information is actually accessed or exposed without prior authorization.

In our digital, interconnected economy, cybersecurity incidents have become everyday occurrences. The most mature cybersecurity programs can reduce the risk of an incident, but nothing short of closing up shop altogether can completely eliminate the risk. Indeed, incidents are so commonplace, the exposure of personal and sensitive information has also become the norm. Breach notification letters are delivered with such frequency that consumers have become numb to them.

Not all data breaches are the same, however, and the type of data, volume and nature of the exposure all contribute to the risk posed to the individuals affected. An exposed email address, government identifier, credit card number or crypto wallet address all contribute to different levels of risk and provide malicious actors different vectors for conducting nefarious activities.

Understanding the Confidentiality, Integrity, and Availability Risks to Data

Data breach risks vary widely based on the type of sensitivity of the information involved, requiring analysis across multiple dimensions:

Confidentiality Risks and Real-World Impact: Personally Identifiable Information (PII) presents a spectrum of risks that can vary widely - combinations of name, email and address are usually considered low risk, while these elements combined with the Social Security numbers (SSN), drivers' licenses or financial account numbers increase identity theft potential. Payment card data presents significant financial risks, enabling immediate fraud and requiring robust protection under the nationwide Payment Card Industry Data Security Standard (PCI-DSS) framework. Government identification data creates identity theft risks that can persist for years, potentially affecting victims' ability to obtain credit, employment or housing. Lastly, the loss of confidentiality of some information may lead to more direct threats, such as the revelation of crypto assets or attributable wallet information or the revelation of confidential employment information.

Integrity and Availability Considerations: Beyond initial exposures, compromised data integrity can lead to corrupted records affecting medical treatment decisions or financial transactions. System availability disruptions can halt critical services, from healthcare delivery to financial transactions, with cascading effects on public trust and organizational reputations. While these incidents may not include the public disclosure of personal sensitive information, they pose their own unique risks to the safe delivery of these services.

Understanding these nuanced dimensions is essential when evaluating breach severity, determining proper responses and implementing preventative measures across different data categories.

Data Under Regulation and Regulatory Protection Frameworks

Not all data carries the same risk or can lead to the same level of threat when exposed. Moreover, different regulations apply different definitions to common data types across the environment in which they are processed and stored.

For our purposes, we break down data into the following key types, which includes regulatory definitions and illustrative examples, as shown in Table 1:

Table 1 – Data Types and Examples

Type of Data	Definition	Examples of Data
Sensitive Data	According to the Code of Federal Regulations,[1] sensitive data is: • Defined as any type of information that can result in harm or adverse consequences to individuals that the data pertains to, if this information is accessed or disclosed without authorization.[2]	• Financial information • Credential data • Customer information • Human Resources (HR) records • Network security map
Confidential/ Privileged Data	According to the Privacy Act of 1974,[3] Confidential/Privileged data is: • Defined as any information that is not intended for public viewing or access.[4] • Privileged data is any information that uniquely provides special access or control to a system or an account.[5]	• Patent applications • Trade secrets • Company documents • Special user access

Personal Information (PI) or Personally Identifiable Information (PII)	According to the patchwork of state laws[6] governing PII in data breaches, like the California Dat Breach Notification Law:[7] • PII is typically defined to include an individual's first name (or first initial) and last name combined with a driver's license, Social Security Number, or financial account numbers (bank account information, payment cards, etc.). • Many states broaden the definition of PII to include login credentials, health information, biometric information, and genetic information.Includes indirect identifiers, that when used in combination, can identify or be linked back to an individual. Many regulations focus on the linkability of PII (i.e., a name combined with a state issued ID number as opposed to a name in isolation).	Certain combinations of: • Birth date • SSNs • Passport number • Driver's license number • Credit card number • Biometric data • Login credentials • Health information
Protected Health Information (PHI)	According to Health Insurance Portability and Accountability Act (HIPPA):[8] • Is related to an individual's past, present, or future physical/mental health or healthcare. • Must be secured to protect a patient's healthcare privacy.[9]	• Health/Medical Records • Treatment records • Health insurance beneficiary numbers • Payment Information
Payment Card Industry (PCI)	According to the Payment Card Industry Security Standards Council, PCI is:[10] • Provided through an electronic card payment and is used to authenticate a card transaction.[11]	• Card Holder Name • Card Number • Card Expiration Date • Card Code Verification (CCV) number • Magnetic stripe data
Biometric Data	According to the Federal Trade Commission (FTC), biometric data is: • Defined as data that depicts or describes physical, biological or behavioral traits, characteristics or measurements of or relating to an identified or identifiable person's body.[12]	• Facial features • Iris or retina • Finger or handprints • Voice • Genetics • Characteristic movements or gestures (e.g., gait or typing pattern)

In the United States, data protection works through a fragmented system of federal and state laws that regulate different data types with varying levels of stringency. These regulations typically align with the associated risk level of the data with federal laws applying based on industry sector (such as healthcare or financial services) rather than following a single comprehensive framework. Outside these industry-specific federal regulations, general consumer data protection falls primarily under state authority, creating a complex patchwork of requirements.

Table 2 shows the different laws and regulations applied to various data types that organizations store and process in the U.S.:

Table 2 – Industry Regulations

Industry	Key Regulations
Health[13] / PHI	• HIPAA • Health Information Technology for Economic and Clinical Health Act (HITECH Act)
Financial / PCI	• Gramm Leach Bliley Act (GLBA)[14] • Fair Credit Reporting Act (FCRA) • Fair and Accurate Credit Transactions Act (FACTA)[15] • PCI DSS[16]
Biometric[17]	• Illinois Biometric Information Privacy Act (BIPA) • Texas Capture or Use of Biometric Identifier Act (CUBI) • Washington Biometric Identifiers Law
Consumer PII	• FTC Act • State Data Breach Notification Laws, like California's Data Breach Notification Law and New York's Information Security breach and Notification Act (NYS Data Breach Notification Law)
Children/Teen Data	• Children's Online Privacy Protection Act (COPPA)

While our focus here is the United States regulatory landscape, beyond the U.S., international data protection laws, such as EU's GDPR, China's Personal Information Protection Law (PIPL), Brazil's Lei Geral de Proteção de Dados (LGPD) and India's Digital Personal Data Protection (DPDP) Acts, govern how organizations collect, process and protect personal data. These frameworks can result in investigations, processing restrictions, remediation mandates, specific fines and in some cases criminal penalties, with highly sensitive sectors like healthcare and finance facing more frequent audits, deletion orders and escalating sanctions.

Regulatory Consequences Without Corporate Collapse

Enforcement severity depends heavily on data sensitivity. Breaches involving low-sensitivity data often lead to corrective actions from federal or state regulators, while incidents involving highly sensitive data, such as biometric or health information, can trigger stricter penalties, statutory damages and class actions. Regulatory

enforcement is generally driven by two factors: (1) the sensitivity and volume of data exposed (i.e., a lower volume of records that includes only name and email address compared to a higher volume of records that also includes government-issued identifiers); and (2) whether the victimized and impacted organization took reasonable measures to prevent, detect and disclose the incident (i.e., threat vectors such as unknown zero-day exploits or insider threats compared to system vulnerabilities with vendor-supplied patches or misconfigurations).

The threat landscape is constantly evolving, leaving organizations in a continual uphill battle to ensure proper protections for data they store and process. U.S. regulatory enforcement is designed not to punish organizations affected by breaches, but to strengthen cybersecurity practices through accountability, guidance and continuous improvement. Moreover, enforcement most often remains in the purview of regulatory bodies, with criminal sanctions focused on the perpetrators of the incidents rather than the victim organizations. There is one known case where an executive from a victim organization was criminally prosecuted, but the case involved unique circumstances, and the individual was charged with obstruction of justice, not a failure that resulted in the breach.

Table 3 shows notable organizations that were breached, underwent regulatory enforcement, and yet remain leaders in their industries:

Table 3 – Notable Data Breaches and Enforcements

Breach	Approx. Records Affected	Data Types Exposed	Risk to Users	Enforcement Outcomes
Target (2013)[18]	~40M customers(payment cards); ~70M customers (personal information)	Payment card data, names, and personal information (addresses, phone numbers, emails)	Card fraud, purchase scams	~$18.5M multi-state Attorney General (AG) settlement; card brand/PCI penalties; major investment in security[19]
Neiman Marcus (2013[20] & 2020[21] & 2024)	~370k cards (2013); ~4.6M customers (2020); ~3.1M customers (2024)	Names, card numbers/exp dates (2013); contact info, payment/gift cards, usernames/passwords (2020)	Card fraud and account takeover risk	$1.5M multistate settlement (2013, 43 AG + DC); notifications/monitoring (2020)
eBay (2014)[22]	~145M users	Names, encrypted passwords, emails, addresses, phone numbers, date of births (DOBs)	Account compromise and takeover	Regulatory investigations in U.S./EU; no mega-fine but significant remediation and monitoring
Home Depot (2014)[23]	~56M cards, 53M emails	Payment card data (card numbers, expiration), customer email addresses	Unauthorized charges (financial fraud)	~$25M settlement with card networks; ~$17.5M AG settlement; security and PCI remediation
Anthem (2014–2015)[24]	~78.8M people	Names, SSNs, DOBs, health plan IDs, addresses, employment info (no medical diagnosis)	Insurance fraud, identity theft	~$115M+ class-action settlement; ~48M settlement with state AGs; $16M OCR HIPAA settlement; mandated security improvements
Google (2015–2018 disclosed 2018)[25]	~500k then ~52.5M users	Names, emails, occupations, genders	Social engineering scams and targeted phishing	Led to accelerated shutdown of Google+ consumer product; scrutiny of disclosure timing

Equifax (2017)[26]	~147M individuals	Names, SSNs, DOBs, addresses, driver's license numbers, limited credit card data	Full identity theft, new account fraud, credit damage	~$575M+ settlement with FTC + Consumer Financial Protection Bureau (CFPB) + 50 states; long-term security program and third-party audits[27]
MyFitnessPal (2018)[28]	~150M accounts	Usernames, email addresses, hashed passwords, limited IP-related info	Account takeover, credential stuffing on other sites using breached credentials	User notifications and forced password resets; no large public regulatory fine reported
Canva (2019)[29]	~137M users	Names, usernames, email addresses, city/country, salted/hashed passwords	Loss of account access, intellectual property theft	Notifications, password resets; regulatory interest but no headline mega-fine reported
Coinbase (2025)	~69,461 users[30]	Names, addresses, phone numbers, emails, masked SSNs/bank info, govt ID images, transaction history[31]	Crypto theft, financial fraud, identity theft and account takeovers	DOJ investigation; class action lawsuits; $20M reward offered by Coinbase for the identity of the threat actor (ransom refused)[32]

This sampling of breaches offers valuable lessons in resilience and response. Although these incidents disrupted operations and exposed sensitive data affecting millions of consumers, each organization persevered. Even though each breach involved exposure of sensitive consumer information, the severity of regulatory enforcement varied across each case, reflecting differences in oversight, sector-specific obligations and the varying risks.

Common threads observed across these and other breaches include regulatory actions and settlements focused on cybersecurity improvements aimed at strengthening controls, and fines that, in some cases, were significant but were not a threat to the organization's financial health.

Conclusion

Not all incidents are breaches, and not all data breaches are created equal. The exposure of certain sensitive data leads to far higher risk of fraud, identity theft or greater. The exposure of less sensitive data, while still opening the door for misuse, may pose much less risk of harm to individuals.

For organizations, they must consider both the data breach risk and the regulatory landscape when evaluating impacted information and should make clear to their customers the types of data and associated risks so that they can take appropriate action.

For consumers, while it is easy to dismiss the next breach letter, individuals should evaluate the change in their risk landscape with the information now out in the wild.

Endnotes

1 https://www.ecfr.gov/current/title-31/subtitle-B/chapter-VIII/part-800/subpart-B/section-800.241

2 https://www.paloaltonetworks.com/cyberpedia/sensitive-data#:~:text=Sensitive%20data%2C%20also%20known%20as,to%20whom%20the%20data%20pertains

3 https://www.justice.gov/opcl/privacy-act-1974

4 https://www.it.tum.de/en/it/it-security/for-employees/confidential-data/definition-confidential-data /

5 https://safecomputing.umich.edu/protect-the-u/protect-your-unit/access-authorization-authentication/managing-privileged-accounts

6 https://perkinscoie.com/insights/publication/security-breach-notification-chart

7 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.82&lawCode=CIV

8 https://www.hhs.gov/answers/hipaa/what-is-phi/index.html#:~:text=PHI%20stands%20for%20Protected%20Health,hipaa/understanding/index.html

9 https://www.paloaltonetworks.com/cyberpedia/protected-health-information-phi

10 https://www.pcisecuritystandards.org/standards/

11 https://controller.ucsf.edu/how-to-guides/accounts-receivable-banking-services/understanding-payment-card-industry-data-security#:~:text=The%20Payment%20Card%20Industry%20Data%20Security%20Standard,updating%20software%2C%20security%20systems%2C%20and%20antivirus%20tools**

12 https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf

13 https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

14 https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

15 https://www.ftc.gov/legal-library/browse/statutes/fair-accurate-credit-transactions-act-2003

16 https://www.pcisecuritystandards.org/standards/pci-dss/

17 https://www.bakerdonelson.com/webfiles/Publications/Global-Biometrics-Laws-Chart.pdf

18 https://redriver.com/security/target-data-breach

19 https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

20 https://www.mass.gov/news/ag-healey-joins-15-million-multistate-settlement-with-neiman-marcus-over-2013-data-breach

21 https://constella.ai/neiman-marcus-data-breach-analysis-and-example-of-how-criminals-exploit-data-using-ai/

22 https://www.upguard.com/blog/biggest-data-breaches-us

23 https://www.upguard.com/blog/biggest-data-breaches-us

24 https://www.upguard.com/blog/biggest-data-breaches-us

25 https://www.huntress.com/blog/biggest-data-breaches

26 https://www.huntress.com/threat-library/data-breach/equifax-data-breach

27 https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

28 https://www.huntress.com/blog/biggest-data-breaches

29 https://www.huntress.com/blog/biggest-data-breaches

30 https://www.claimdepot.com/data-breach/coinbase

31 https://www.pkware.com/blog/data-breach-report-may-2025

32 https://milberg.com/news/coinbase-data-breach-class-action-lawsuit/