Cyber Incident Notification and Reporting Requirements for Financial Institutions

The financial services sector is one of the few critical infrastructure sectors that has had mandatory cybersecurity and incident reporting requirements in law and regulation for over 20 years. In 2022, Congress established a uniform reporting standard that applies to every major sector of the economy and outlines expectations for how the private sector and its government partners should share information following a cyber incident. Regulators are now working to implement the legislation and it is important to ensure that any new expectations are harmonized and align with existing requirements for financial firms; this helps to avoid disruptions that may negatively affect a financial institutions' ability to respond to an incident and reduces the risk of developing new rules that either duplicate or conflict with existing regulations.

In addition to reporting from the private sector, it is critical that federal agencies and independent regulators also report incidents when they experience a breach that affects the sensitive information of businesses or consumers.

To help guide implementation efforts, the following is a snapshot of some of the existing requirements that apply to financial institutions.

U.S. Federal Requirements and Proposals

1. **Cyber Incident Reporting for Critical Infrastructure Act (2022)**
   Requires critical infrastructure companies to report significant cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours. It also requires firms to report a ransomware payment within 24 hours. CISA is required to issue a proposed rule to implement these requirements no later than March 2024.
   - **Reporting Timeline** – 72 hours after determining a cyber incident has occurred.
   - **Definitions** – Significant cyber incidents are defined as an incident or group of incidents that are likely to result in demonstrable harm to national security interests, foreign relations, or the economy, or to public confidence, civil liberties, or public health and safety. Other key definitions for types of entities required to report and specific information required will be determined through a rulemaking process.
   - **Scope of Reporting** – A "covered cybersecurity incident" to be defined through the rulemaking process.
   - **Reporting Mechanism** – Reports to be provided to CISA according to requirements set through the final rule.

2. **Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (2022)**
   Under the final rule issued jointly by the Office of the Comptroller of the Currency, Federal Reserve Board, and the Federal Deposit Insurance Corporation, incident notification is triggered to the banking organization's primary federal regulator upon determination that a computer-security incident has occurred that has caused, or is reasonably likely to cause actual harm to the institution's operations and ability to deliver products and services to a significant portion of its customers, or could pose a risk to the financial stability of the United States.
   - **Reporting Timeline –** as soon as possible but no later than 36 hours from the determination by the banking organization that an event has crossed the notification incident materiality threshold.
   - **Definitions –** A computer security incident is defined as an occurrence that jeopardizes confidentiality, integrity or availability of an information system or the information a system processes, stores, or transmits[1]; a *notification incident* is defined as a significant computer security incident that has, or is

[1] This definition is taken from NIST which states a computer security incident is "an occurrence that results in actual or potential jeopardy to the

reasonably likely to jeopardize the viability of the operations of a financial institution, prevent customers from accessing their deposit and other accounts, or impact the stability of the financial sector.

- **Scope of Reporting –** covers nonpublic customer information and information technology systems[2].
- **Reporting Mechanism –** Notification to be provided to the primary federal regulator; intended to provideearly awareness of emerging threats to individual institutions and potentially the broader financial system.

3. SEC Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (2022)

On March 9, 2022, the SEC released a notice of proposed rulemaking to enhance disclosure requirements for registered public companies. Among several requirements designed to provide investors with information about cybersecurity risk management, governance, and strategy, the proposal requires public companies experiencing a material cybersecurity incident to disclose certain non-technical information in an 8-K filing within four business days of the materiality determination. It further requires additional details to be provided on 10-Q and 10-K filings. Additionally, incidents that are immaterial but could become material in the aggregate are required to be reported as an element of the 10-K filing.

- **Reporting Timeline –** Within four business days following determination that a material incident has occurred.
- **Definitions –** Materiality is defined within the established SEC standard for public company disclosures.
- **Scope of Reporting** – Covers all material cybersecurity incidents within the four-day period, and immaterial incidents that become material in the aggregate for the annual reporting period.
- **Reporting Mechanism –** Reporting and disclosures provided through investor disclosures (8-K, 10-Q, and 10K).

4. SEC Proposed Rule on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (2022)

- **Reporting Timeline –** Promptly, but within 48 hours after having a reasonable basis to conclude that a significant incident has occurred or is occurring.
- **Definitions –** A significant incident is defined as a single or combination of cyber incidents that significantly disrupt or degrade an adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations.
- **Scope of Reporting** – Covers significant incidents as defined by the proposed rule, as well as certain unauthorized access or use of adviser information resulting in substantial harm to the adviser, client, or an investor in the private fund whose information was accessed.
- **Reporting Mechanism –** New proposed form that includes general and specific questions related to the significant cybersecurity incident (e.g., nature and scope and whether disclosure has been made to clients and/or advisers).

5. Securities & Exchange Commission (SEC) Guidance on Public Company Cybersecurity 10-Q, 10-K and 8-K Disclosures (2018)

On Feb. 26, 2018, the SEC released a clarification to earlier 2011 general disclosure guidance that warned public companies that cyber incidents may have to be reported through public disclosures. The clarification guidance puts public companies on more stringent notice with regard to breach notification practices and requires reporting of material cyber incidents and their *potential security risks* within quarterly,yearly and, if needed, current filings.

- **Reporting Timeline –** Dependent on the materiality of a given incident in relation to the timing of the preparation and release of a periodic disclosure filing, but states that it is critical that

confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." See NIST, Computer Security Resource Center, Glossary https://csrc.nist.gov/glossary/term/Computer_Security_Incident

[2] The NPR does not define information technology systems.

public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion.

- **Scope of Reporting –** Covers material cybersecurity incidents and associated potential security risks.
- **Reporting Mechanism –** Reporting/disclosure provided through investor disclosures (10-Q, 10-K and 8-K ifnecessary).

6. Gramm-Leach-Bliley Act (1999)

Under the GLBA and its implementing regulations[3], cyber incident reporting is triggered when a financial institution becomes aware of unauthorized access to sensitive customer information that is, or is likely to be, a misuse of the customer's information. To ensure adherence to these requirements, regulators conduct ongoing and rigorous reviews of institutions' operating and governance processes, including data security anddata handling processes and third-party risk management measures. Failure to report incidents and adhere tothese requirements could result in serious enforcement measures including mandatory corrective action directives, restrictions on activities and fines.

- **Reporting Timeline –** as soon as possible once the institution determines unauthorized access occurred.
- **Definitions –** A *cyber incident* is defined as unauthorized access to sensitive customer information.
- **Scope of Reporting –** Covers nonpublic customer information such as personally identifiable financialinformation, financial transaction information, income and credit rating data, etc.
- **Reporting Mechanism –** Report provided to regulators; information becomes part of ongoing regulatoryoversight/examinations.

European Union Requirements

7. European Union General Data Protection Regulation (GDPR)

GDPR sets specific privacy parameters for use, data security and handling of consumer data.

- **Reporting Timeline –** not later than 72 hours after becoming aware of the breach
- **Definitions –** A "data breach" is defined as "the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
- **Scope of Reporting** – Personal data[4]
- **Reporting Mechanism –** Entities report to the agency designated by each Member state, which thennotifies other Member states as needed.

8. European Union NIS Directive 1.0.

In 2016, the EU mandated cyber incident reporting for all sectors defined under the term Essential Services which is like the U.S. term of Critical Infrastructure. However, the EU has both mandatory security mandates on Digital Service Providers and stricter reporting requirements on DSPs[5]. The EU is in the midst of updating the NIS Directive 2.0 where notification must occur with any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible, via network and information systems.

- **Reporting Timeline –** 24 hours from when an entity is aware of an incident, and then a report 30 dayslater.
- **Definitions –** An *incident* means any event having an actual adverse effect on the security of network andinformation systems.[6]

[3] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. See https://www.federalregister.gov/documents/2005/03/29/05-5980/interagency-guidance-on-response-programs-for-unauthorized-access-to-customer-information-and

[4] Personal data is under GDPR here: https://gdpr-info.eu/art-4-gdpr/

[5] Essential Services are defined by the EU in the NIS Directive and were implemented in 2016. See: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[6] For definition of "incident," see https://eur-lex.europa.eu/eli/dir/2016/1148/oj

- **Scope of Reporting –** The Directive does not define the threshold of what is a significant incident requiring notification to the relevant EU Member state national authority and defines three parametersfor reporting: number of users affected; duration of incident; geographic spread. DSPs have five requirements that are broader.
- **Reporting Mechanism** –Entities report to the agency designated by each Member state.

Insurance Industry Requirements and Model Legislation

9. National Association of Insurance Commissioners (NAIC) Model Law

Insurance is a state-regulated business model overseen by the insurance commissioners of the 50 states. Financial institutions with insurance subsidiaries must operate within these 50 jurisdictions under the rules ofthe several states in which they provide insurance products. The National Association of Insurance Commissioners (NAIC) developed a cybersecurity framework model law that guides states in adopting their own statutes on cyber incident notification. The model law is not binding until adopted by an individual state;states are free to modify or decline to adopt any aspect or provision of the model law through their state legislative process. As of July 2021, less than 20 states have adopted the model law in whole or part, but its framework is under active consideration in many more.

- **Reporting Timelines –** Under the language of the model law, notification is to be made as promptly aspossible but in no event later than 72 hours from a determination that a cybersecurity event has occurred. However, adopting states are free to, and do, vary their reporting timelines.
- **Definitions –** A cybersecurity event means an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such an Information System. An InformationSystem means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well asany specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.
- **Scope of Reporting –** Under the language of the Model Law, covers information systems andinformation stored on information systems.
- **Reporting Mechanisms –** Under the language of the Model Law, notification is made to the state insurance commissioner and affected consumers as directed by the adopting state's data breach notification law.

State Requirements

10. New York Department of Financial Services (NYDFS) Cybersecurity Regulation

The NYDFS regulations[7] became effective on March 1, 2017, and add another layer of mandatory cybersecurity reporting requirements for financial services companies. A financial institution must notify NYDFS when a cyber event triggers reporting to any other government body, regulatory or self-regulatory agency. Notification is also triggered if there is a reasonable likelihood of material harm to the institution'soperations.

- **Reporting Timeline –** 72 hours from the determination that a cyber event has occurred.
- **Definitions –** A *cyber event* is defined as any act or attempt to gain unauthorized access to, disrupt, ormisuse an information system or information stored on an information system.
- **Scope of Reporting –** Covers nonpublic customer information and information technology systems[8]
- **Reporting Mechanism –** Report provided to NYDFS; information becomes part of ongoing regulatoryoversight

[7] See New York Codes, Rules and Regulations (23 NYCRR 500). https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)

[8] Defined as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems."

11. State Data Breach Notification Requirements

All 50 states have codified a version of a consumer data breach notification statute[9], which contains provisions intended to protect against unauthorized access of computerized data and personal information. The statutes generally also require notification to affected residents of the state whose personal informationwas or is reasonably believed to have been compromised. In most cases, the statute also requires notice in varying combinations to the state's Attorney General, state law enforcement and credit reporting agencies. Although in many states financial institutions are statutorily exempted or deemed in compliance due to theirexisting compliance with federal standards like GLBA, federal banking regulatory guidance, or in some cases,by operation of their supervision by a federal entity, the exemption provides little relief. Still, many financial institutions purposefully do not avail themselves of the state exemption and notify the relevant state authority to avoid being penalized for inadvertent nondisclosure.

- **Reporting Timelines –** Varies by state, ranging from "within the most expedient time possible and without unreasonable delay…" to "72 hours from the determination that a cyber event has occurred…"
- **Definitions –** Varies by state.
- **Scope of Reporting –** Varies by state but generally covers unauthorized access of personal information.
- **Reporting Mechanisms –** Varies by state, but nearly always requires notice to affected residents of the state, and generally some combination of the state Attorney General, state law enforcement, and credit reporting agencies. It can also occasionally require notice to subordinate state regulatoryoffices as directed by the state legislature or state executive.

Key Definitions

Systemically Important Financial Institutions

Congress is also considering creating a new definition for critical infrastructure, "Systemically Important Critical Infrastructure (SICI)," modeled after the financial designation of Systemically Important Financial Institutions (SIFI). Under Section 113 of the Dodd-Frank Act, a financial institution may be named a SIFI if the nature, scope, size, scale, concentration, interconnectedness, or mix of its activities could pose a threat to U.S. financial stability. The designation is made by the Financial Stability Oversight Council[10] and subjects institutions to enhanced regulatory standards.

Information Technology Systems

NIST defines an information technology system as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems."[11]

[9] *See* "Sample of Cyber-Incident Notification Requirements"

[10] For more information on FSOC see https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/about-fsoc

[11] See https://csrc.nist.gov/glossary/term/information_system.

Examples: Cyber Incident Notification and Reporting Requirements

US Federal Banking / SEC Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
Federal	Gramm-Leach-Bliley Act	CFPB	as soon as possible
Federal	Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers	FDIC/FRB/OCC	36 hours after determination that a certain threshold of incident has occurred, based on an institution's good faith belief
SEC	2018 Guidance on Public Company Cybersecurity Disclosures	SEC	take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion

European Union Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
EU	NIS Directive	EU member state agency	24 hours from awareness of the incident, followed by a report within 30 days
EU	General Data Protection Regulation (GDPR)	EU member state agency, followed by other EU member states	not later than 72 hours after becoming aware of the breach

State Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
Alabama	Ala Code 8-38	Attorney General	as expeditiously as possible and without unreasonable delay, taking into account the time necessary to conduct an investigation, and within 45 days of discovering that a breach has occurred and is reasonably likely to cause substantial harm to affected individuals.
Alaska	AS 45.48.010	Private Right of Action	shall be made in the most expeditious time possible and without unreasonable delay consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the information system.
Arizona	Ariz. Rev. Stat. 44-7501	Attorney General	shall be made within 45 days after the Entity's determination that there has been a security breach
Arkansas	Ark. Code 4-110-101	Attorney General	shall be made in the most expedient time and manner possible and without unreasonable delay, subject to any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.
California	Cal. Civ. Code 1798.29; 1798.82	Private Right of Action	shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
Colorado	Colo. Rev. Stat. 6-1-716	Attorney General	shall be made in the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determination that the breach occurred, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
Connecticut	Conn. Gen. Stat. 36a-701b	Attorney General/Insurance Department for insurance companies	shall be made without unreasonable delay, but not later than 90 days after the discovery of such breach, unless a shorter time is required under federal law, consistent with any measures necessary to determine the nature and scope of the breach, to identify individuals affected, or to restore the reasonable integrity of the data system.

State Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
Delaware	Del. Code Ann. Tit. 6, 12B-101	Attorney General	must be made without unreasonable delay but not later than 60 days after determination of the breach of security, unless a shorter time is required by federal law. If the entity could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of this State was included in a breach of security, the entity must provide notice as soon as practicable after the determination that the breach of security included the personal information of such residents, unless the Entity provided substitute notice.
District of Columbia	D.C. Code 28-3851	Private Right of Action/Attorney General	shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
Florida	Fla. Stat. 501.171	Department of Legal Services	as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the Entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reasons to believe a breach occurred. Entity may receive 15 additional days to provide notice to Affected Individuals if good cause for delay is provided in writing to the Department within 30 days after determination of the breach or reason to believe a breach occurred.
Georgia	Ga. Code. 10-1-910	N/A	shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.
Hawaii	H.R.S. 487N-1	Attorney General	shall be made without unreasonable delay, consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system.

State Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
Idaho	Idaho Code 28-51-104	Primary State Regulator	must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.
Illinois	815 Ill. Comp. Stat. 530/5, 530/10, 530/12, 530/15, 530/20, and 530/25	Attorney General	shall be made in the most expedient time possible and without unreasonable delay, but in no event later than when the data collector provides notice to consumers pursuant to this Section.
Indiana	Ind. Code 4-1-11; 24-4.9-1	Attorney General	shall be made without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and restore the integrity of the system.
Iowa	Iowa Code 715C.1-2	Attorney General	shall be made in the most expeditious manner possible and without unreasonable delay, consistent with any measures necessary to sufficiently determine contact information for the affected IA residents, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.
Kansas	Kan. Stat. 50-7a01	Attorney General	must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
Kentucky	KY Rev. Stat. 365-732	N/A for KY residents; non-affiliated third parties of KY state and municipal governments must notify the attorney general	should occur in the most expedient time possible and without unreasonable delay, subject to the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system; non-affiliated third parties of state and municipal governments must notify the attorney general in the most expedient time possible and without unreasonable delay, within 72 hours of determining that a breach occurred.

State Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
Louisiana	La. Rev. Stat. 51:3071	Private Right of Action/Attorney General Consumer Protection Section	shall be made in the most expedient time possible and without unreasonable delay, but not later than 60 days from discovery of the breach, consistent with any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.
Maine	10 Me. Rev. Stat. 1346	Attorney General/"appropriate state regulators within the Dept. of Professional and Financial Regulation"	must be made no more than 30 days after becoming aware of the breach and identifying its scope. The notices must be made as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data in the system. Notification may be delayed for no longer than 7 business days after a law enforcement agency determines that the notification will not compromise a criminal investigation. If notification is not delayed due to law enforcement investigation, notification must be made no more than 30 days after becoming aware of a breach of security and identifying its scope.
Maryland	Md. Code Com. Law 14-3501	Attorney General	shall be given as soon as reasonably practicable, but no later than 45 days after the business concludes the investigation, consistent with measures necessary to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system
Massachusetts	Mass. Gen. Laws 93H 1	Attorney General/Director of Consumer Affairs and Business Regulation	shall be given as soon as practicable and without unreasonable delay following discovery of the breach. Entities cannot delay notification "on the grounds that the total number of residents affected is not yet ascertained"
Michigan	Mich Comp. Laws 445.63, 72	Attorney General	shall be given without unreasonable delay following discovery of the breach, consistent with measures necessary to determine the scope of the breach of the security of a system or restore the integrity of the system.

State Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
Minnesota	Minn. Stat. 325E.61, 325E.64	Attorney General	must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.
Mississippi	Miss. Code 75-24-29	Attorney General	shall be provided without unreasonable delay subject to the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the system.
Missouri	Mo. Rev. Stat. 407.1501	Attorney General	shall be made without unreasonable delay and consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.
Montana	Mont. Code 2-6-1501, 30-14-1704, 33-19-321	Attorney General/Insurance Commissioner	is to be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
Nebraska	Neb. Rev. Stat. 87-801	Attorney General	shall be made as soon as possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.
Nevada	Nev. Rev. Stat. 603A.010, 242.183	Attorney General/Breached Data Collector Right of Action	shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.
New Hampshire	N.H. Rev. Stat. 359-C:19	Attorney General/Private Right of Action	shall notify the affected individuals as soon as possible.
New Jersey	N.J. Stat. 56:8-163	Division of State Police, Dept. of Law and Public Safety, with potential dissemination or referral to other appropriate law enforcement agencies	shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

State Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
New Mexico	N.M. Stat. 57-12C-1	Attorney General	shall be made in the most expedient time possible, but not later than 45 calendar days following discovery of the security breach. Notification may be delayed as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.
New York	N.Y. Gen. Bus. Law 899-aa	Attorney General, Department of State Consumer Protection, and Division of State Police	shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
	Part 500	NYDFS	72 hours from determination that a cyber event has occurred
North Carolina	N.C. Gen. Stat. 75-61, 75-65	Attorney General, AG Consumer Protection Division	shall be made without unreasonable delay, consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.
North Dakota	N.D. Cent. Code 51-30-01	Attorney General	must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the data system.
Ohio	Ohio Rev. Code 1347.12, 1349.19, 1349.191, 1349.192	Attorney General	shall be made in the most expedient time possible but not later than 45 days following discovery or notification of the breach in the security of the system, consistent with any measures necessary to determine the scope of the breach, including which residents' PI was accessed and acquired, and to restore the reasonable integrity of the data system.
Oklahoma	24 Okla. Stat. 161	Attorney General	shall be made without unreasonable delay consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.

State Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
Oregon	Or. Rev. Stat. 646A.600, 646A.602, 646A.604, 646A.624, 646A.626	Attorney General	shall be made in the most expedient manner possible and without unreasonable delay, but not later than 45 days after discovering or receiving notice of the breach. In providing the notice, the Entity shall take reasonable measures necessary to determine sufficient contact information for the individuals, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the PI.
Pennsylvania	73 Pa. Stat. 2301	Attorney General	Except in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay.
Puerto Rico	10 L.P.R.A. St 4051	Department of Consumer Affairs	as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security.
Rhode Island	R.I. Gen. Laws 11-49.2-1	Attorney General	shall be made in the most expedient time possible but no later than 45 calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements and shall be consistent with the legitimate needs of law enforcement.
South Carolina	S.C. Code 39-1-90	Attorney General/Consumer Protection Division of the Department of Consumer Affairs/Private Right of Action	must be made in the most expedient time possible and without unreasonable delay, consistent with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
South Dakota	S.D. Codified Laws 22-40-19	Attorney General	must be given no later than 60 days from when the Information Holder discovers or is notified of a breach.
Tennessee	Tenn. Code 47-18-2107	Private Right of Action	shall be made immediately, but no later than 45 days from the discovery or notification of the breach, unless a longer period of time is required due to the legitimate needs of law enforcement.

State Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
Texas	Tex. Bus. & Com. Code 521.002, 521.053	Attorney General	without unreasonable delay and [effective January 1, 2020] in each case not later than the 60th day after the date on which the person determines that the breach occurred, consistent with the legitimate needs of law enforcement, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
Utah	Utah Code 13-44-101, 13-44-202, 13-44-301	Attorney General	shall be provided in the most expedient time possible without unreasonable delay, after determining the scope of the breach of system security and after restoring the reasonable integrity of the system.
Vermont	9 V.S.A. 2430, 2435	Attorney General	shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery of the breach, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.
Virginia	Va. Code 18.2-186.6, 32.1-127.1:05	Attorney General	shall be made without unreasonable delay. Notice may be reasonably delayed to allow individual or entity to determine scope of the breach of security and restore the reasonable integrity of the system.
Washington	Wash. Rev. Code 19.255.010, 42.56.590	Attorney General/Private Right of Action	shall be made in the most expedient time possible and without unreasonable delay, no more than 30 calendar days after the breach was discovered, unless the delay is at the request of law enforcement or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
West Virginia	W.VA. Code 46A-2A-101	Attorney General	Except in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the notice shall be made without unreasonable delay.

State Requirements			
Jurisdiction	**Statute or Regulation (et. seq.)**	**Principal Notification or Enforcement Entity Beyond Affected Residents or Individuals**	**Disclosure Timeline**
Wisconsin	Wis. Stat. 134.98	N/A	within a reasonable time, not to exceed 45 days after the Entity learns of the acquisition of PI. A determination as to reasonableness shall include consideration of the number of notices that an Entity must provide and the methods of communication available to the Entity.
Wyoming	Wyo. Stat. 40-12-501	Attorney General	shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

NAIC Model Law Adopting States (States that have adopted, in whole or part, the NAIC Insurance Data Security Model Law)			
US Federal Banking / SEC Requirements	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**
N/A	NAIC Model Law	Insurance Commissioner	as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred
Alabama	Ala. Code 27-62-1	Insurance Commissioner	as promptly as possible, but in no event later than three business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred

NAIC Model Law Adopting States (States that have adopted, in whole or part, the NAIC Insurance Data Security Model Law)			
US Federal Banking / SEC Requirements	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**
Connecticut	Conn. Gen. Stat. 697-38a-38	Insurance Commissioner	as promptly as possible but in no event later than three business days after the date of the cybersecurity event
Delaware	Del. Code. 18-8601	Insurance Commissioner	as promptly as possible but in no event later than 3 business days from the licensee's determination that a cybersecurity event has occurred
Hawaii	Haw. Rev. Stat. 431	Insurance Commissioner	as promptly as possible, but in no event later than three business days from a determination that a cybersecurity event impacting two hundred fifty or more consumers has occurred
Indiana	Ind. Code 27-2-27-1	Insurance Commissioner	within three (3) business days after making the determination that a cybersecurity event has occurred
Iowa (Effective 1/1/2022)	Iowa Code XXX	Insurance Commissioner	no later than three business days from the date of the licensee's confirmation of a cybersecurity event
Louisiana	La. R.S. 22:2501	Insurance Commissioner	without unreasonable delay but in no event later than three business days

NAIC Model Law Adopting States (States that have adopted, in whole or part, the NAIC Insurance Data Security Model Law)			
US Federal Banking / SEC Requirements	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**
Maine	Me. Stat. 24-B-2261	Insurance Superintendent	as promptly as possible but in no event later than 3 business days from a determination that a cybersecurity event has occurred
Michigan	Mich. Comp. Laws 500.559	Director of the Department of Insurance and Financial Services	as promptly as possible but not later than 10 business days after a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred
Minnesota	Minn. Stat. 60A.985	Commissioner of Commerce; Commissioner of Health (whichever regulates the entity)	without unreasonable delay but in no event later than five business days from a determination that a cybersecurity event has occurred
Mississippi	Insurance Department Bulletin 2019-4	Insurance Commissioner	as promptly as possible, but in no event later than three (3) business days from a determination that a cybersecurity event involving nonpublic information has occurred
New Hampshire	Insurance Department Bulletin INS 20-001-AB	Insurance Commissioner	within three (3) days, pursuant to RSA 420-P:6

NAIC Model Law Adopting States (States that have adopted, in whole or part, the NAIC Insurance Data Security Model Law)			
US Federal Banking / SEC Requirements	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**
North Dakota	N.D.C.C. 26.1-02.2	Insurance Commissioner	as promptly as possible, but no later than three business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred
Ohio	Ohio Rev. Code 3965	Insurance Superintendent	as promptly as possible after a determination that a cybersecurity event involving nonpublic information in the possession of the licensee has occurred, but in no event later than three business days after that determination
South Carolina	S.C. Code Ann. 38-99	Director of the Department of Insurance	no later than seventy-two hours after determining that a cybersecurity event has occurred
Tennessee	Tenn. Code Ann. 56-2-10	Insurance Commissioner	as soon as practicable, and in no event more than three (3) business days, following a determination that a cybersecurity event has occurred
Virginia	Va. Code Ann. 38.2-6-2	Insurance Commissioner	in accordance with requirements prescribed by the Commission, as promptly as possible but in no event later than three business days from such determination

NAIC Model Law Adopting States (States that have adopted, in whole or part, the NAIC Insurance Data Security Model Law)			
US Federal Banking / SEC Requirements	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**	**US Federal Banking / SEC Requirements**
Wisconsin (Effective 11/1/21)	Wis. Stat. 601.954	Insurance Commissioner	shall provide the notification under par. (a) in electronic form and as promptly as possible, but no later than 3 business days from the determination that the cybersecurity event occurred