

The Sedona Conference Draft Commentary on Proposed Model Data Breach Notification Law (April 2022)



The Sedona Conference Draft Commentary on Proposed Model Data Breach Notification Law (April 2022)

Drafting Team Members:

Matt Meade (Drafting Team Leader)

Kamal Ghali

Amy Keller

Ryan Kriger

Daryl Osuch

Ruth Promislow

David Sella-Villa

Martin Tully

Hon. Tom Vanaskie (ret.)

Larry Wescott

Al Saikali (Steering Committee Liaison)

The Sedona Conference

WG11 Draft Commentary on Proposed Model Data Breach Notification Law

SECTION I. INTRODUCTION

In 2002, California became the first U.S. state to adopt a data breach notification law, which became effective on July 1, 2003.¹ Since then, a patchwork system of inconsistent data breach notification laws was gradually enacted in other states, with all fifty U.S. states now having enacted some form of notification law. Generally speaking, data breach notification laws require those affected by a data breach (or unauthorized access to data) to notify individuals, customers, and other parties about the breach, as well as to take specific steps to remedy the situation based on directives of the state legislature.

Data breach notification laws are typically viewed as having two main goals. The first is to timely notify individuals whose data was involved in a breach in order to give them the chance to mitigate damage and risks caused by the data breach. The second is to increase accountability of organizations and encourage them to strengthen data security. But the laws, as they are written, do not necessarily accomplish those goals for two chief reasons.

First, there is the issue of uniformity. There are important differences among the measures adopted by different states. Differences in data breach notification laws include varying definitions of personally identifiable information (“PII”) with corresponding variations of notice obligations to impacted individuals, law enforcement and consumer credit agencies. Other differences include varying penalties for non-compliance. This lack of uniformity makes it challenging for breached entities to understand their obligations and makes it more complicated and expensive to comply with the law. This is a particular issue for smaller organizations which do not have the resources to retain external privacy counsel.

Second, most notification letters do little to help consumers. When a data breach occurs, individuals whose data was involved in the breach will likely receive a standardized letter that vaguely explains what happened, why they should not be panicked, and a general discussion of the type of data that was involved in the breach. Typically, the notification does little to inform the consumer of how to protect themselves through certain, mitigating measures—such as freezing their credit, or enrolling in a credit monitoring service. The vague nature of the notices, combined with the fact that consumers are receiving more and more notices, can lead to fatigue and, eventually data security apathy.

This Commentary is intended to assist federal and state lawmakers to update or enact data breach notification laws that: (i) enable the individuals to protect themselves against the risk of data breaches; and (ii) provide concise, clear and consistent direction to PII Controllers (defined below) responding to data security incidents. This Commentary was prepared by a cross-section of

¹ SB 1386, Cal. Civ. Code 1798.82 and 1798.29.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than May 27, 2022.

experienced privacy lawyers, technology experts, and regulatory authorities who seek to reduce conflict between and lack of clarity within the various state data breach notification laws.

The Commentary addresses the above two, chief problems with present data beach notification statutes, and suggests eight areas where the current iterations of state data breach notification laws can be improved by greater uniformity and clarity: (1) definition of security breach; (2) definition of PII; (3) definition of risk of harm; (4) encryption, de-identification and similar technologies; (5) method and form of notification; (6) timeline for notification; (7) credit monitoring; and (8) notifying law enforcement and regulatory authorities.

For ease of reference, we have compiled the proposed model language for each of the eight areas identified above in their entirety in Section IV of this Commentary. Because of the interplay among them, it is essential to the formulation and subsequent use of this proposed language that the eight sections be considered as a whole. The Drafting Team recognizes that there are other significant topics addressed in state data breach notification laws that are not covered within the eight areas, *e.g.*, private right of action, notification to consumer reporting agencies, definitions of records, covered entities, substitute notice, law enforcement delay, form of regulator notice, etc. We focused principally on these eight areas because, based upon our collective experience, these areas would benefit the most from the uniformity and clarity of a Model Data Breach Notification Law.

This Commentary is intended to inform policy decisions at the federal or state levels as data breach statutes evolve. Even if a legislature declines to adopt all of the recommendations made herein, it may benefit from our analysis as to specific elements of such a law.

SECTION II. BACKGROUND

Security breach notification laws can impose obligations on any PII Controller², regardless of its size, sophistication, or industry. Similarly, all organizations are vulnerable to security breaches, regardless of how mindful they are of data security. PII Controllers frequently experience security incidents that may give rise to breach notice obligations.³

The Drafting Team notes that the number of data breaches and data security incidents continues to rise; however, requiring that *all* security incidents be reported, and notice sent would not be good policy. This would lead to notice fatigue among notice recipients, who would likely start ignoring notices, even ones of critical importance. Professor Rui Chen of Iowa State University has described a trend which he calls “data breach fatigue” where people do not appear to be concerned

² “PII Controller” means any for-profit or non-profit entity, or government entity, that collects, receives, maintains, possesses, controls, or has custody of PII. See Section IV. A.

³ For purposes of this document, a “security incident” refers to an occurrence that actually or potentially jeopardizes the 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. National Institute of Standards and Technology, Computer Security Resource Center, “Security Incident,” located at https://csrc.nist.gov/glossary/term/security_incident (last visited May 12, 2019). All security breaches begin with a security incident, while not all security incidents turn out to be security breaches.

about their data security, despite recent major data breaches.⁴ Professor Chen observed, “[w]hen an incident happens, when a data breach incident goes to the media, people read that news and they start to lose interest... They take it as a new normal in today’s society.”⁵ As a result, individuals may not take steps to protect themselves from further loss and injuries or may not understand what steps they may take to do so. This potential notice fatigue may mean that consumers will not engage in routine, common-sense measures to mitigate their losses—such as taking the time to freeze their credit, monitor their credit reports (or purchase credit monitoring services to do that for them), or routinely monitor already-open credit files.

Further, requiring overly broad notice may impose an unnecessary burden on the business community. As discussed in more detail in Section IV, a Model Data Breach Notification Law should be tailored to require that only certain incidents be considered reportable security breaches.

The analysis of whether a given security incident triggers a notice obligation can be time consuming and costly. If the media affected includes email, file systems, backup tapes, or paper records, search algorithms might not suffice, and entities seeking to ascertain if a notice obligation exists might be required to pore over terabytes of data by hand. Often forensic investigators must be retained by the entity to determine exactly what happened and, working with counsel, to determine whether an incident triggers a notice obligation. In addition to expense, these activities take time, during which individuals who may be vulnerable to fraud and identity theft by reason of the security incident are not being made aware of their exposure. These activities are also expensive for PII Controllers and their insurers. Thus, a Model Data Breach Notification Law should be drafted to make it as clear as possible what constitutes a notification-triggering security incident requiring such investigation and should be drafted with the complexities and costs of compliance in mind.

While a Model Data Breach Notification Law must be narrowly tailored to be manageable by PII Controllers, it must remain broad enough to ensure that individuals are notified of a security incident when circumstances warrant notification—such as when such incidents put them at increased risk of identity theft, or when they might experience reputational harm—among other things. Any consideration of what should or should not be included in such a law must be guided by the fundamental need to inform individuals of such a security event so that they may take steps to mitigate against further loss.

It is critical that a Model Data Breach Notification Law should be drafted with these principles in mind.

⁴ Grayson Schmidt, “Expert Warns of the Risks Posed by Data Breach Fatigue,” *Government Technology*, Jan. 31, 2018, located at <https://www.govtech.com/security/Expert-Warns-of-the-Risks-Posed-by-Data-Breach-Fatigue.html> (last visited May 12, 2019).

⁵ *Id.*

SECTION III. ANALYSIS AND DISCUSSION OF CURRENT STATE DATA BREACH NOTIFICATION LAWS AND PROPOSED MODEL DATA BREACH NOTIFICATION LAW

Set forth below is the Drafting Team’s analysis of the eight areas of current state data breach notification laws followed in each case by the Drafting Team’s proposed model language as to the area in question and the Drafting Team’s explanation for proposing that language.

A. Is PII Involved in the Incident?

The first step in determining whether an entity would need to send notice pursuant to the proposed model statute is determining whether PII was involved in the incident. PII is information that, when used alone or with other data, can identify an individual. An entity that does not collect PII need not worry about having to provide notice to individuals of data security incidents, and entities that do collect PII can take steps to segment such data or focus their data protection efforts on such data in order to minimize their risk of suffering a notice-triggering incident.

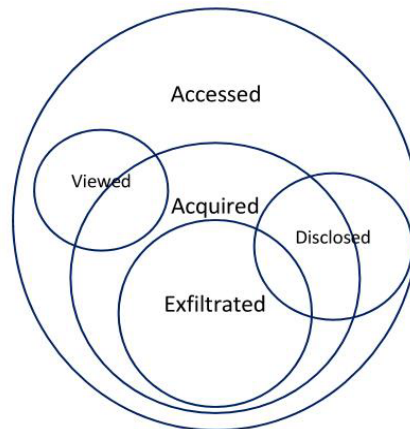
B. If the Incident Involves PII, Is it a Security Breach?

1. Inconsistencies in Current State Law on What Should Constitute a Notifiable Data Breach

After determining that PII was affected by a security incident, the next step in determining whether notification is required is to assess whether the incident constitutes a data breach.⁶ If PII was involved, the next question is whether the unauthorized user interacted with the data in a manner that may necessitate notice. The terms most often used by state notification statutes in defining what must have happened to the data in question for the statute to apply include *accessed*, *viewed*, *disclosed*, *acquired*, and *exfiltrated*.

These different terms are subject to interpretation and debate—the Venn diagram below provides one such interpretation:

⁶ See *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 2d. 333, 339 (W.D.N.Y. 2018) (“plaintiffs had standing to bring data breach claims when the breached database contained personal information such as ‘names, dates of birth, marital statuses, genders, occupations, employers, Social Security Numbers, and Driver’s license numbers.’”), citing *Whalen v. Michaels Stores, Inc.*, 689 Fed. Appx. 89, 91 (2d. Cir. 2017). Virtually every state data breach notification law covers personal information.



Access is considered the broadest definition. For example, in the context of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et. seq.*, a defendant was found to have “accessed” America Online’s computers by sending email through them: “For purposes of the CFAA, when someone sends an email message from his or her own computer, and the message then is transmitted through a number of other computers until it reaches its destination, the sender is making use of all of those computers and is therefore ‘accessing’ them.”⁷

A minority of states use the “access” approach.⁸ “Acquisition” is considered a narrower definition and has been adopted by the vast majority of states.⁹ However, the trend may be beginning to move

⁷ *America Online, Inc. v. National Health Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000).

⁸ See, e.g., Fla. Stat. Ann. § 501.171(1)(a) (“‘Breach of security’ or ‘breach’ means unauthorized access of data in electronic form containing personal information.”); N.J. Stat. Ann. § 56:8-163(a) (“Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.”); Conn. Gen. Stat. Ann. § 36a-701b(a) (“‘breach of security’ means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.”); R.I. Gen. Laws Ann. § 11-49.3-3(a)(1) (“‘Breach of the security of the system’ means unauthorized access or acquisition of unencrypted, computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency, or person.”); P.R. Laws Ann. tit. 10 § 4051(c) (“Violation of the security system. — Means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised...”).

⁹ See, e.g., Colo. Rev. Stat. Ann. § 6-1-706(h) (“‘Security breach’ means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.”); Minn. Stat. Ann. § 325E.61(1)(d) (“‘breach of the security of the system’ means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.”); Utah Code Ann. § 13-44-102(1)(a)

in the other direction. New York recently moved from acquisition to access.¹⁰

Some states have recognized that it is difficult to determine absolutely that access took place due to insufficient logging or log retention, sophisticated attackers, or intervening circumstances. These states require that a PII Controller report a breach if it has a *reasonable belief* of access without providing any examples of what constitutes a reasonable belief.¹¹

Due to the potential for difficulty in distinguishing whether a threat actor has acquired data because of the sophistication of the threat actor or insufficient logging by the breached entity, the Drafting Team believes a broad definition of “Security Breach” is appropriate. The Commentary’s proposed Model Data Breach Notification Law hinges the definition on unauthorized access to PII, rather than unauthorized acquisition, disclosure, or theft, for example. This approach simplifies the analysis necessary to determine whether notice should be provided and can help avoid incentivizing businesses to collect *less* logging information in order to be able to claim an inability to establish acquisition.

While a broader definition of “Security Breach” could include access to data or a circumstance which would lead a reasonable PII Controller to believe that an unauthorized access to unencrypted data has occurred, whether that access compromises the security, confidentiality, or integrity of an individual’s PII maintained by that PII Controller—this definition would be so broad that it would include certain security incidents that would have very little likelihood of harm to individuals whose PII was accessed. Excluding those incidents would have the benefit of encouraging PII Controllers to adopt best practices. One such exclusion would be for unauthorized access to encrypted or sufficiently de-identified data.¹² Where the accessed data is encrypted with sufficient security measures or de-identified in a way that prevents a threat actor from accessing the data, it should be unusable by bad actors. For this reason, access to encrypted or de-identified data should

(“‘Breach of system security’ means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.”).

¹⁰ N.Y. S.B. 5575

¹¹ See, e.g., Alaska Stat. § 45.48.090(1) (“breach of the security” means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector....”). The concept of reasonable belief is also sometimes applied to a risk of harm analysis, though for purposes of this analysis we are limiting its use to the access or acquisition of data. See Ky. Rev. Stat. Ann. §365.732(1)(a) (“‘Breach of the security of the system’ means unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky.”).

¹² Many states include the issue of encryption in the definition of PII instead of the definition of security breach. We believe it is more appropriately addressed in another section of the proposed model statute. This is because if a business collects social security numbers, for example, it may be encrypted at rest but at some point it may be available in an unencrypted form. If the data is acquired while unencrypted, it is a breach. If PII is defined as “unencrypted data,” then whether a business holds PII can change based on the state or use of the data.

not be considered a security incident potentially worthy of requiring notice, unless the bad actor also possesses the encryption key or is otherwise likely able to re-identify the data.¹³ Additionally, there are several different encryption techniques and algorithms, some of which are no longer effective. Thus, encryption should be separately defined to mean, “a technology for securing computerized data in such a manner that it is rendered unusable, unreadable, or indecipherable in its original format without the use of a decryption process or key and in accordance with generally accepted industry standards.” While an exclusion for encrypted data could be built into the definition of “Security Breach” or the definition of “PII,” the Drafting Team believes the clearest way to create such an exclusion is by a separate statutory provision. *See* the further discussion of encryption, de-identification and related technologies in Section III.E, *infra*.

Another situation in which there is a low likelihood of injury to the individual(s) in question exists where data is accessed by someone without authorization, but the access was made in good faith by an internal employee, or an agent, for authorized business purposes. Thus, an exception from the definition of Security Breach should be made for this situation, as is already common in many data breach laws.¹⁴ The Drafting Team proposes to build that exclusion directly into the definition of “Security Breach.”

2. *Challenges Created by Current Laws*

As the means of data interaction for triggering a potential notice obligation, the use of the term “acquisition” is not only less consumer-friendly, but also may create difficulties in the cloud computing context. Threat actors may still “access” information in cloud computing environments without “acquiring” it, leading to a significant risk of harm to the individuals whose data was housed in the cloud. State statutes which use the term “acquisition” without a corresponding “risk of harm” analysis (as discussed below) significantly disadvantage individuals whose data was

¹³ *See, e.g.,* Tex. Bus. & Com. Code § 521.053(a) (“In this section, ‘breach of system security’ means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.”); Cal. Civ. Code § 1798.29(a) (“Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.”)

¹⁴ *See* Iowa Code § 715C.1(1) (“Good faith acquisition of personal information by a person or that person’s employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.”).

impacted by a security incident. This can also lead to further confusion among PII Controllers, who will need to implement different notice thresholds in different states.

Finally, because security incidents are often very specific and listing all possible variations of a “harmless” breach would be futile, it would be worthwhile to insert a “catch all” provision for access to data that is unlikely to lead to harm (*see* Risk of Harm discussion, below). This determination, however, should be made by a data collector in consultation with the appropriate regulator, as otherwise the incentive would be too great for a PII Controller to rationalize why any individual breach is unlikely to lead to harm.

C. The Type of PII Involved Determines Whether Notification Is Necessary

Currently, state data breach notice laws vary significantly in their definitions of what sorts of PII can trigger a notice obligation. Most states contain a laundry list of data elements that are amended from time to time in order to keep up with advances in technology. These lists can and do vary widely from state to state.

Further, the nature of data breaches has evolved to include an increased scope of PII. Previously, data breaches typically involved financial or other information that could be used to commit identify theft. Now, threat actors are increasingly focused on acquiring a much broader scope of personal information including private information and then commoditizing that information for purposes beyond financial fraud e.g., identity theft. For these reasons, the Commentary’s two-tiered approach to defining PII means that harm beyond economic loss such as bodily harm, psychological distress, damage to reputation or relationships, or loss of employment, business, or professional opportunities may require notice.

1. Current State Data Breach Notification Laws

In the United States, there are varying definitions of PII among the states. Each state’s data breach notification law specifies the particular information that is defined to be “personal,” such that a compromise of that kind of information may amount to a reportable breach. The definition of PII in these state breach notification laws is therefore static. That is, there is no flexibility in the statute to interpret the definition of PII to include a category of information that is not already expressly identified.

This static approach to defining PII does not account for the evolving cyber threat landscape where new types of information associated with individuals are compromised, and which can cause the same or greater level of harm as the compromise of traditionally recognized categories of PII. For example, categories of personal information that are increasingly compromised include a data subject’s contact list, geolocation data, and employment information. As more of our business and personal lives are conducted online, and as PII continues to be commoditized through behavioral and targeted advertising, the ability of threat actors to monetize increasing categories of personal information continues to expand. A static definition of PII fails to account for this evolving threat.

This threat to an expanding number of categories of personal information can also be attributed to the increasing digitization of records by businesses of all sizes and across all industries. This move

toward a digital economy contributes to the expansion of information associated with individuals that is subject to compromise in a security incident.

Additionally, a static definition of PII does not account for new categories of personal information that may be at risk as technologies emerge, such as biometrics (which is included in the definition of PII in some state breach notification laws) and information captured by voice assistants or connected vehicles.

A static approach to defining PII requires legislative reform as new categories of PII are revealed to be at risk that may give rise to harm when subjected to unauthorized access.

2. Current Compliance Challenges

The practical problem that a PII Controller faces in the event of a security incident is the conflicting state regimes with which it must comply. What may constitute a reportable incident in one state is not necessarily so in another.

The fact that a state breach notification law has included a particular category of information in the definition of PII implies that a compromise of such data could give rise to harm. Likewise, the absence of a particular category of information from the specific list of PII in the state breach notification law suggests that a compromise of such information would not give rise to harm in that jurisdiction. For that reason, notice to impacted individuals involving that omitted category of information is not required. But data is not different depending on jurisdiction, and state-by-state definitions of PII have created more complications than benefits to governments, entities, and individuals. Based on those categories of information identified in the definition of PII, a PII Controller may develop a data protection strategy that focuses on protecting listed categories of information. In this way, the state breach notification laws indirectly incentivize PII Controllers to implement reasonable safeguards for the categories of information included in the definition of PII. The varying and conflicting definitions of PII in the state breach notification laws therefore create inconsistent incentives for organizations in developing their data protection strategy.

The following types of information associated with individuals have been included in various states' definitions of PII:

- Social Security number;
- motor vehicle operator's license number or non-driver identification card number;
- financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
- account passwords or personal identification numbers or other access codes for a financial account;
- biometric information, including a fingerprint, retinal scan, and facial recognition data;
- genetic information;
- health information;

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than May 27, 2022.

- health insurance policy number or health insurance identification number and any unique identifier used by a health insurer to identify an individual;
- login credentials, including a username or password; and
- passport number.

Specific examples of the discrepancies with respect to the definition of PII are as follows:

Biometric data is included in the definition of PII in several states including California, Colorado, Delaware, Louisiana, Maryland, Nebraska, New Mexico, Vermont and Texas,¹⁵ but not in others such as Alabama, Arkansas, California, Florida, Indiana, Kansas, Massachusetts, and Nevada.¹⁶

Passport number is included in the definition of PII in states such as Alabama, Colorado, Delaware, Florida, Louisiana, Maryland and Vermont,¹⁷ but not in others such as Arkansas, California, Indiana, Massachusetts, Minnesota, Nebraska, New Mexico, Nevada, and Rhode Island.¹⁸

A broad definition of PII serves to clarify the obligations on PII Controllers with respect to their obligations in protecting PII.

3. *Guidance Regarding the Scope of PII*

A potential criticism of a broad PII definition is that PII Controllers will not have advance notice of the specific types of PII that could trigger a notice obligation if accessed without authorization and that PII Controllers may be penalized for failing to provide notice based on unauthorized access to data that they did not consider to be PII. However, the proposed definition, while broad, is clear and straightforward: it covers factual or subjective information about, pertaining to, or traceable to, an identifiable individual.

Guidance is provided on the scope of PII as follows:

- Information will pertain to, be traceable to, or be about an identifiable individual, even where the information does not itself identify that individual, where it is more likely than not that an individual could be identified through the use of that information, either alone or in combination with other information.

¹⁵ Cal. Civ. Code Ann. § 1798.29(g); Colo. Rev. Stat. Ann. § 6-1-716(g); Del. Code. Ann. tit 6 §12B-101(7); La. Rev. Stat. §51:3073(4)(a); Md. Com. Law. Code Ann. §14-3501(e); Neb. Rev. Stat. §87-802(5); N.M. Stat. Ann. §57-12C-2(C); N.M. Stat. Ann. §57-12C-2(C); Vt. Stat. Ann. tit. 9 § 2430 (10) .

¹⁶ Code of Ala. §8-38-2(6); Ark. Code. Ann. § 4-110-103(7); Fla. Stat. Ann. §501.171(1)(g); Ind. Code. Ann. §24-4.9-2-10 ; Kan. Stat. Ann. §50-7a01(g); Mass. Gen. Laws Ann. ch. 93H, §1(a); Nev. Rev. Stat. Ann. §603A.040(1).

¹⁷ Code of Ala. §8-38-2(6); Colo. Rev. Stat. Ann. § 6-1-716(1)(g); Del. Code. Ann. tit 6 §12B-101(7); Fla. Stat. Ann. §501.171(1)(g) ; La. Rev. Stat. §51:3073(4)(a); Md. Com. Law. Code Ann. §14-3501(e); Vt. Stat. Ann. tit. 9 § 2430 (10).

¹⁸ *See id*; Minn. Stat. Ann. §325E.61(1)(e); R.I. Gen. Laws §11-49.3-3(a)(8).

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than May 27, 2022.

- Information can meet the definition of PII regardless of how or from whom its acquisition occurred, including information voluntarily provided, , or observed, derived, or inferred from non-confidential source material.

The following is an illustrative, but non-exhaustive, list of classes of PII (either by itself or in connection with other PII) to aid in current understanding and future analysis:

- Name (including full name);
- Government-issued numbers or other unique identifiers (social security numbers, passport numbers, motor vehicle operator’s license numbers, state identification card numbers, etc.);
- Dates pertaining to an individual (birth date, wedding date, graduation date, death date, military enlistment or discharge date, etc.);
- Financial account numbers—real or virtual (any bank account numbers, credit card numbers, investment or retirement account numbers, virtual currency account numbers, etc.);
- Any login credentials (email address, username, password or other access code such as a personal identification number (“pin” or “pin number”), or security question or password recovery answers);
- Biometric data (more specifically, an individual’s physiological, biological or behavioral characteristics, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity);
- Insurance information (identification numbers, insurance policy numbers or any other unique identifying number);
- Health information (health history, information about illnesses, information or observations about a patient, etc.);
- Employee personnel files or similar evaluations or personal commentary (subjective or objective employee performance metrics, any kind of personal analysis, goals that might be about an identifiable individual, etc.);
- Physical asset information that consistently links an item to an individual (MAC address, IP address, car license plate number, home address);
- Geolocation data (such as data used on ride-sharing apps, shopping or discount apps, augmented reality apps or games);
- Customer loyalty or affinity account numbers;
- Physical asset or software usage data (browser history, cookies, software tokens, usage metadata, etc.); or
- Any other unique number-based code or characteristic that is about an identifiable individual (phone number, an organizational anonymized code for an individual, etc.).

4. *International Trends Regarding PII*

Smart phones and devices—and, therefore, applications which collect, maintain, and control PII—are used by individuals domestically and internationally. Accordingly, there is value in moving

toward a definition of PII that more closely aligns with the international approach. Increasingly, PII Controllers conduct business in multiple jurisdictions and are required to comply with varying, conflicting regulatory regimes. Incentivizing PII Controllers to take privacy seriously and to incorporate privacy by design is supported by moving toward the more broad approach to defining PII globally.

The General Data Protection Regulation (GDPR), a law which imposes obligations and regulations on entities which target or collect data related to individuals in the European Union, uses a broad definition of PII. “Personal data” is defined as “any information relating to an identified or identifiable natural person (‘data subject’); 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.”¹⁹

Likewise, the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) uses a broad definition of PII. Under PIPEDA, personal information is defined as “information about an identifiable individual.”²⁰ In guidelines issued by the Office of the Privacy Commissioner (“OPC”) (which oversees the administration of PIPEDA), PII is further explained to be “any factual or subjective information, recorded or not, about an identifiable individual,” and examples of PII are provided.²¹

For the reasons discussed herein, the Drafting Team proposes a two-tiered definition of PII that will provide clarity to PII Controllers so that determinations of notification obligations can be more easily made. Category I PII includes among other things as listed in the draft of the Model Law, Social Security numbers, driver’s license numbers, and sensitive health information; financial information; and account and login credentials. If there is a Security Breach (as defined below) involving Category I PII, then such breach automatically triggers reporting obligations on the basis of presumed harm. Category II PII means PII where the PII Controller must evaluate the possibility of the PII impacted by the Security Breach causing harm to the PII Subject(s), because unauthorized access to the PII may, depending on context, cause harm to the PII Subject. Examples of Category II PII include but are not limited to date of birth; maiden name of the individual’s mother; digitized or other electronic signature; insurance information (identification numbers, insurance policy numbers or any other unique identifying number); health information that is not sensitive diagnosis information (health history, information about illnesses, information or observations about a patient, etc.).

¹⁹ General Data Protection Regulation, art. 4 (1), located at <https://gdpr-info.eu/art-4-gdpr/> (last visited May 24, 2019).

²⁰ S.C. 2000, c.5, §2(1).

²¹ Office of the Privacy Commissioner of Canada, “PIPEDA in brief”, located at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ (last visited May 24, 2019).

D. What Role Should Risk of Harm Analysis Play in Data Breach Notification?

Because the nature of data breaches has evolved to include an increased scope of PII, the scope of harm has likewise evolved. Accordingly, the next step in determining whether notification of a security incident is required involves performing a “risk of harm” analysis. Put in the simplest of terms: if an individual is likely not to experience harm as a result of a Security Breach, then providing notice to that individual is unnecessary.²² The vast majority of state data breach notification laws require some analysis by the impacted PII Controller of the risk of harm to the individual associated with the PII in question by reason of the event in question before a notification requirement is triggered. The standard for determining whether a sufficient risk of harm exists to require notification varies across those states, however, and uniformity is necessary to eliminate confusion.

1. The Variation in Risk of Harm Standards and Definitions Is Problematic

For most states, the statutory formulations require *some* degree of likelihood of *some* sort of harm to the individual associated with the PII in question in order to trigger a notice obligation to the individual affected. The statutory formulations vary widely, however, in regard to *what* sort of harm and to *what* degree of likelihood that harm must exist for notice to be required. For example, in New Jersey, notification is not required if the business or public entity establishes that misuse of the information is not reasonably possible.²³ In North Carolina, notification is not required if a breach does not result in illegal use of PII, is not reasonably likely to result in illegal use, or there is no material risk of harm to a consumer.²⁴ In Massachusetts, notification is required where the breach creates a “substantial risk of identity theft or fraud against a resident of the Commonwealth,” or when the person or agency knows or has reason to know that the PII of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.²⁵ In Indiana, notification is required “if the database owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting the Indiana resident.”²⁶ Under other frameworks, there is a presumption of harm (and thus a requirement to give notice) unless it is “reasonable” to conclude otherwise.²⁷

²² This statutory “risk of harm” analysis for breach notification is related to but very distinct from the question of whether “concrete, particularized harm” or “intangible” injury exists—including the “risk” of injury—that is central to whether plaintiffs have standing to sue over a data breach and whether their claims are viable. The “risk of harm” analysis for statutory data breach notification purposes presents different concerns from the “injury” requirement for Article III standing. Accordingly, this commentary refers only to “risk of harm” in statutory construction and is not intended to provide any analysis concerning venue or jurisdiction in litigation.

²³ N.J. Stat. Ann. § 56:8-163(a).

²⁴ N.C. Gen. Stat. § 75-61(14).

²⁵ See *supra* note 16.

²⁶ Ind. Code Ann. § 24-4.9-3.1(a).

²⁷ Looking to Europe, the GDPR requires personal notifications when the personal data breach is likely to result in a “high risk to the rights and freedoms of natural persons,” unless certain conditions are met. See *generally* GDPR, article 35.

The Drafting Team considers the current statutory formulations of the risk of harm standard to be problematic for two reasons. First, the differences between the formulations create the distinct possibility of identical facts triggering a notice obligation in one jurisdiction but not in another. Second, the vagueness of those formulations arguably denies PII Collectors fair notice of what the formulations require, and that vagueness at a minimum creates an undesirable range of differing, but reasonable, interpretations of those requirements. For example, by using subjective terms like “low,” “high,” “significant,” “material,” “reasonably,” and “substantial” to define how likely the harm in question must be for a notice obligation to exist, the current statutory formulations leave the question of whether a notice obligation has been triggered very much in the eye of the beholder. And this problem is exacerbated by those statutory formulations that, rather than following the example of states like Indiana (which as noted defines the relevant “harm” as “identity deception, identity theft, or fraud”), provide no definition at all of what constitutes “harm” for purposes of the statute, and thus leave that core issue wholly open to interpretation and subjective judgment. The likely result? Breached entities will likely conclude that no risk of harm resulted at all.

A requirement that the acquisition/access is “reasonably likely to cause injury or identity theft or fraud” leaves the determination solely in the hands of the data collector or owner. Some PII Controllers may underestimate or misunderstand the potential risk of harm and inadvertently default to finding that the likelihood of injury is low and therefore not be incentivized to provide notice to individuals. Others may be incentivized to find that no harm exists given the cost of sending notice. Under other frameworks, there is a presumption of harm (and thus a requirement to give notice) unless reasonable to conclude otherwise. In tacit recognition of the interpretive problems created by the current statutory formulations of the risk of harm standard, some state statutes inject the relevant regulator into the process by which PII Collectors apply the risk of harm standard. Vermont, for example, has a “negative option” harm trigger which states that if a data PII Controller believes misuse of personal information is not reasonably possible, and they inform the Attorney General, they need not notify potentially affected persons.²⁸ Florida requires that the risk of harm analysis be conducted in consultation with relevant federal, state, or local law enforcement agencies.²⁹ Alaska similarly requires the giving of notice to the state Attorney General as a condition of determining that no reasonable likelihood of harm exists.³⁰ Presumably, statutory provisions like these are premised on a concern that because the statute’s risk of harm standard is vague and subjective, if the statute leaves the risk of harm determination solely in the hands of the PII Collector, breach notification that the relevant regulator believes should be given will not be given. Whatever the merit may be of such statutory provisions and the policy concerns on which they presumably are premised, the Drafting Team views these “run it by the regulator” provisions as corroboratory of the highly problematic vagueness and subjectivity built into the current statutory formulations of the risk of harm standard.

2. Considerations to Address Issues Created by Various Risk of Harm Standards

²⁸ Vt. Stat. Ann. tit. 9 § 2435(d).

²⁹ Fla. Stat. Ann. § 501.171(4)(c).

³⁰ Alaska Stat. Ann. § 45.48.101(c).

The statutory framework for HIPAA provides a helpful analysis in determining when notification of a Security Breach is necessary. Under that statute, the “acquisition, access, use, or disclosure of protected health information in a manner not permitted” under the statute is presumed to be a breach “unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment” constituting four factors.³¹ Following those factors provides guidance and a framework for assessing risk of harm in other data contexts.

i. The Nature and Extent of the Information Involved

Consider the nature and extent of the PII involved. Is it sensitive information? Is it financial? What type of information was inappropriately disclosed or used? Would the unauthorized access, unavailability or modification of the PII likely harm the data subject? See discussion of what constitutes PII in Section IV.A, *supra*.

ii. The Recipient of the PII

Consider the unauthorized person who accessed the PII. This analysis is different from any analysis that would be performed to determine if a Security Breach has occurred. Is the recipient a criminal actor? Also, consider whether this person has legal obligations to protect the information—for example, is the person or entity required to comply with confidentiality or non-disclosure obligations or applicable privacy laws? If so, there may be a lower probability that the PII has been compromised. Also, consider if the unauthorized person has the ability to re-identify the information.

iii. Whether the PII Was Actually Acquired, Used or Viewed

In other instances, it may be possible to determine that the PII accessed as a result of the security incident has not, in fact, been viewed or used in a manner that likely caused or is likely to cause the requisite harm.³² For example, this would be the case if a laptop containing PII is stolen but soon after tracked to a pawnshop where it is determined that the laptop was never actually accessed or forensically imaged/copied by an unauthorized individual. Accordingly, there is little to no risk of harm, and therefore notice need not be provided.

iv. Mitigation of the Risk Following Unauthorized Disclosure

Consider the extent to which the risk of harm from unauthorized access to the PII in question has been mitigated by the entity that suffered the security incident (as compared to mitigation efforts the affected individuals might employ). For example, consider whether the PII Collector has obtained the recipient’s assurances that the PII will not be further used or disclosed (through a confidentiality agreement or similar means), has been completely returned, or has been/will be

³¹ CFR § 164.402(2).

³² Some security incidents may fall into another type of safe harbor because the PII was encrypted, de-identified, anonymized, or otherwise rendered inaccessible, and therefore not reasonably likely to ever be used or viewed. But this consideration, while important, goes to whether or not a Security Breach even occurred.

destroyed. This factor, when considered in combination with the factor regarding the nature of the unauthorized recipient, may lead to a determination that the requisite the risk of harm has not been established. For example, an entity may be able to obtain and rely on the assurances of an employee, affiliated entity, or vendor that they destroyed the information in order to make such a determination. However, such assurances from other third parties may not be sufficient to overcome other indicia that the requisite risk of harm exists.

3. Advantages of the Two-Tiered PII Approach Discussed in Section IV. A

The flexible approach to defining PII encourages PII Controllers to address the risk of harm in a proactive way. They can consider what forms of PII they are responsible for safeguarding, assess whether a compromise of that information could conceivably give rise to a risk of harm, and then make decisions as to the appropriate levels of safeguards to protect that PII.

Some PII is sensitive in nature (such as health data), such that it is automatically deemed to give rise to a risk of harm, and therefore classified as Category I PII. However, whether other PII (such as subscription to a magazine or membership to an organization) is sufficiently sensitive depends on contextual considerations, such as the nature of the magazine, or the PII Controller and the nature of the PII. For example, a membership list for Alcoholics Anonymous may be sufficiently sensitive, whereas a membership list for a “dog lovers” organization may not be. The potential risk of harm from unauthorized access to information showing the names of members of Alcoholics Anonymous is evident.

This context-specific analysis may incentive PII Controllers to engage in PII analysis prior to a breach. Such analysis promotes consideration of privacy issues in a preventive manner, rather than a reactive one, and informs the PII Controller’s assessment of the required safeguards.³³

E. Elaboration on the Effect of Encryption and De-identification

Existing breach notification statutes recognize that some data security incidents may have no practical consequences because the accessed data is either not accessible to or usable by anyone other than its owner, or it is not likely to be capable of being associated with an individual or household. In effect, this means that no data breach affecting PII has occurred in the first instance, much less is any harm to an individual likely. Thus, if the data that was disclosed without authorization is encrypted, de-identified or otherwise rendered inaccessible or not attributable to any individual, there is no reasonable likelihood of harm, and the incident is not a breach requiring notification. Differing treatments of encrypted and de-identified information create confusion and inconsistent outcomes when it comes to data breach notification.

1. Encryption Is Already a Recognized Safe Harbor but Not Well-Defined

³³ The Drafting Team notes that there is disagreement within the team regarding: (1) requiring notification to regulators in this situation; and (2) a proposal that the regulator must agree with the determination. For this reason, the Drafting Team seeks input from WG 11 on the most effective approach.

As discussed above, “Encryption” for purposes of the Model Data Breach Notification Law proposed in this Commentary broadly means: “a technology for securing computerized data in such a manner that it is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key, which is not accessible by unauthorized persons, and in accordance with generally accepted industry standards.” More specifically, encryption is the process of using an algorithm to transform information to make it unreadable in its original format for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key. Symmetric-key and asymmetric-key are the two primary types of encryption.

Most states’ data breach notification statutes provide for an exception to the requirement to notify individuals of a data breach involving their PII if the data exposed to unauthorized access was encrypted. California, for example, provides for this exception in requiring notification to residents:

(1) whose unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that PII readable or useable.³⁴

The data breach notification statutes of other states, like Illinois, simply remove encrypted data from the definition of “PII” altogether, the consequence of which is that unauthorized access to encrypted data does not constitute a data breach in the first place:

“Personal information” means either of the following: “(1) An individual’s first name or first initial and last name in combination with any one or more of [several listed] data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security; ... [or] (2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or

³⁴ Cal. Civ. Code § 1798.29(a).

otherwise read the data elements have been obtained through the breach of security.”³⁵

The Drafting Team believes an exclusion from breach notification requirements for Encryption-protected PII is appropriate, and it further believes the clearest mechanism for implementing such an exclusion is by means of a separate statutory provision rather than by building such an exclusion into the definition of “PII” or “Security Breach.” Accordingly, the Model Data Breach Notification Law proposed in this Commentary includes a separate provision in order to implement an exclusion from breach notification requirements for PII that is protected by Encryption.

2. *Many Existing Data Breach Laws Do Not Account for De-identification*

The intent of information sanitization, e.g., data anonymization and pseudonymization, is privacy protection by de-identification. It is the process of either encrypting or removing PII from data sets, so that the people whom the data describe remain anonymous and are not reasonably capable of being identified. The GDPR strongly suggests that, where possible, stored data on people in the EU undergo either an anonymization or a pseudonymization process. Similarly, section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information.³⁶ Under this standard, health information is not individually identifiable if it does not identify an individual, and if the covered entity has no reasonable basis to believe it can be used to identify an individual.

Pseudonymization is a data management and de-identification procedure by which PII fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. A single pseudonym for each replaced field or collection of replaced fields makes the data record less identifiable while remaining suitable for data analysis and data processing. The process of obscuring data with the ability to re-identify it later is also called pseudonymization and is one-way companies can store data in a way that is HIPAA compliant. Note that the GDPR recitals point out that pseudonymized data is still personal data because as long as the key exists and has not been destroyed, there is always the chance that the data could be compromised.

The Drafting Team believes an exclusion from breach notification requirements for PII that is protected by De-Identification is appropriate—provided that the breached entity can confirm that the threat actor does not have access to the key, and the Drafting Team further believes the clearest mechanism for implementing such an exclusion is by means of a separate statutory provision, rather than by building such an exclusion into the definition of “PII” or “Security Breach.” Accordingly, the Model Data Breach Notification Law proposed in this Commentary includes an exclusion for PII protected by De-identification as part of the separate provision being proposed in order to implement an exclusion from breach notification requirements for PII that is protected by Encryption.

³⁵ 105 ILCS §530/5.

³⁶ 45 C.F.R. § 164.514.

F. How Should Notice Be Provided; Who Should Provide It; and What Should It Look Like?

1. Current Data Breach Notification Laws Provide the Following Regarding what Constitutes Acceptable Notice

The U.S. state data breach notification laws vary in terms of appropriate methods of notification, but all states give written notice via U.S. mail as at least one option. Often, written notice is framed as the first option in combination with other possible options (such as telephonic notice or electronic notice). Most states have an option for substitute notice, which is triggered by: (i) the cost of notification exceeding a certain threshold, (ii) the number of individuals affected exceeding a certain threshold, or (iii) the company lacking appropriate contact information. Electronic or email notification is usually a form of substitute notice under most state statutes. Substitute notice often requires more actions than standard notice, as it generally requires, in addition to notice by email, posting to the company website, and notification to statewide media.

If email is given as an option for notice, it is often limited in the following ways:

- Electronic notice, for those persons for whom it has a valid email address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001;³⁷ or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001;³⁸ or
- Email notice, if a prior business relationship exists and the person or entity has a valid email address for the individual.³⁹

2. Compliance with the Current Methods of Notification Can Be Problematic

Providing written notice via U.S. mail can be very costly, particularly for small and mid-size organizations. Most state laws have substitute notice provisions, which should provide a cheaper alternative to written U.S. mail notice. However, the available substitute notice provisions are often triggered by individual thresholds so high that they are not accessible to most organizations. In addition, though substitute notice may seem less costly on the surface, a closer look at most states' provisions reveals a surprising lack of cost-savings. Substitute notice allows a cheaper notification method (such as email), but only in conjunction with relatively expensive notification methods (such as statewide media notification). Since data breaches will likely affect most PII Controllers of varying levels of sophistication and size, it is problematic to make notice expensive or difficult. Complicated and costly methods of notification will not accomplish the

³⁷ See, e.g., Conn. Gen. Stat. § 35a-701b(e); Miss. Code Ann. § 75-25-29(6); Mo. Rev. Stat. § 407.1500(2)(6)(b).

³⁸ Vt. Code Ann. tit 9 § 2435(b)(6)(A)(ii)(II).

³⁹ Ala. Code Ann. § 8-38-5(d).

broadest goal of data breach notification, which is to alert individuals to enable them to protect themselves.

3. *Considerations to Address Issues with Notification Methods*

The overarching purpose of state data breach notification laws is to provide prompt notice to individuals to permit them to take action to protect themselves against whatever harm they have been exposed to by the event in question. As such, a model method of notification should be simple and low-cost, which will allow PII Controllers to accomplish this task quickly.

To that end, the Drafting Team believes, and the Commentary's proposed Model Data Breach Notification Law accordingly provides, that PII Controllers should be able to provide notice through traditional U.S. mail or email—provided that the PII Controller already communicates with the individual through email. Email is the primary mode of communication for most individuals today, and one that most individuals can be relied upon to check regularly. Many PII Controllers will have current email addresses of their customers. If PII Controllers already communicate with individuals via email, or if the customer has given their email address through the course of their business relationship, communicating through email gives notice to individuals quickly and effectively.

The Drafting Team further believes, and the Commentary's proposed Model Data Breach Notification Law accordingly further provides, that if a PII Controller does not have access to the U.S. mail or email of each PII Subject, the PII Controller should post notification of the Security Breach for at least 60 days on the PII Controller's website if the PII Controller maintains one. This post should consist of a link to the notice on the home page or first significant page after entering the website that is in larger type or contrasting type, font or color to surrounding text of the same size or set off from other text by symbols or marks that call attention to the link.

4. *Who Should Send Notice?*

The Drafting Team believes, and the Commentary's proposed Model Data Breach Notification Law accordingly provides, that if a PII Controller experiences a Security Breach, conducts an investigation in accordance with Section IV.B of the Commentary's proposal, and determines that the Security Breach likely caused or is likely to cause harm to one or more of the PII Subjects associated with the PII in question, then the PII Controller should provide notice of the Security Breach to each PII Subject as to whom the PII Controller made such determination.

Where an obligation to provide notice of a Security Breach to a PII Subject exists under this Section IV.D of the Commentary's proposal, the Drafting Team believes, and the Commentary's proposed Model Data Breach Notification Law accordingly provides, that such notice should be provided either by the PII Controller or by another party that has an agreement with the PII Controller that allows the PII Controller to require the party to provide such notice.⁴⁰ It is common for PII Controllers to share information related to PII Subjects with service providers and other

⁴⁰ There are, of course, some exceptions—such as if the PII Controller was required to provide such notice under an agreement, but the relationship between the PII Controller and the other party terminated, and the PII Controller no longer has access to the data to provide such notice.

contract partners. For example, a business may provide human resources data relating to its employees to its benefits provider, or a customer facing business may provide customer preferences to a market research company. When a Security Breach occurs in this type of situation, the Drafting Team believes that the parties should “have the flexibility to set forth specific obligations for each party, such as who will provide notice to individuals . . . , following a breach . . . , so long as all required notifications are provided.”⁴¹ The parties could set forth in their underlying agreement who is responsible for providing notice to impacted PII Subjects. In addition, the parties should determine which entity is in the best position to provide notice to the individual, by considering among other things: (1) which functions the service provider or contract partner performs on behalf of the entity; (2) which entity has the relationship with the individual; and (3) which entity has access to information to provide such notice.⁴² Parties should take steps to ensure that the individual does not receive notifications from both the PII Controller and the service provider about the same breach, which may create confusion.⁴³ The PII Controller remains responsible for ensuring that notice of the Security Breach is provided, either by itself or by its service provider or contract partner.

G. What Should Be the Timeline for Notification?

1. General Issues Affecting the Timing of Data Breach Notification to Individuals

Not all threats to data security result in the unauthorized access to PII held by an PII Controller, and therefore are not security breaches as defined by statute. The legal determination of a Security Breach can only occur after gathering and analyzing relevant facts. It may take time to understand the underlying events and arrive at the legal conclusion of a Security Breach. Accordingly, the affected individuals could have been suffering harm for some time before they receive notice of the event that is causing such harm.

Several factors⁴⁴ contribute to the amount of harm affected individuals may suffer from a security breach, including, (a) whether the underlying security breach is ongoing, (b) what steps the PII Controller that suffered the security breach can take to mitigate harm to affected individuals, and (c) what steps affected individuals themselves can take to mitigate harm from the Security Breach, in spite of timing issues resulting from the investigation of any Security Breach, or the failure to detect the Security Breach. Reducing harm through each of these factors reveals an inherent

⁴¹ Federal Register, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules (Jan. 25, 2013), *available at* <https://www.federalregister.gov/documents/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the>.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ Other relevant factors include, the sensitivity of the breached data, the value of the breached data on the black market, and whether the PII qualifies for special statutory protections. Discussion of these factors and how they impact the harm suffered by affected individuals is beyond the scope of these guidelines.

tension between the costs and benefits of however much time elapses between the occurrence of the Security Breach and the provision of notice about the Security Breach. On the one hand, with more information about the Security Breach, the PII Collector and the individuals whose PII was accessed in the Security Breach can respond more precisely and thoroughly to the specific threat posed by the Security Breach. On the other hand, gathering all the relevant information about a Security Breach takes time, and during that time, individuals whose PII was accessed in the Security Breach could suffer increasing harm. The more harm individuals suffer, the greater an PII Controller's potential legal liability for that harm.

2. *Current Data Breach Notice Timing Requirements*

State breach notice statutes generally employ one of three different approaches to balancing the timing of security breach notifications with the information content of security breach notifications to affected individuals:

- i. Notification to impacted individuals must be made without unreasonable delay or in the most expedient time possible

The timing for notification in this approach emphasizes promptness but allows for the time necessary to gather relevant information. For example, prompt notice to affected individuals may allow them to take steps on their own to mitigate the harm from a Security Breach, but the PII Controller may not have had time to determine whether the Security Breach is still ongoing. By contrast, waiting to provide notification to affected individuals until the breach has been stopped and a tailored risk mitigation plan has been implemented may only marginally reduce the potential harm to affected individuals.

Depending on the specific nature of the breach, the best way to minimize the harm to the affected individuals (and accordingly the potential liability to the PII Controller) may be provide to notifications as soon as the breach is discovered. For example, if a rogue employee gained unauthorized access to PII, once the employee can no longer gain access to the PII, the risk of harm is effectively eliminated. In the case of mass exploits like the Heartbleed Bug,⁴⁵ the individual's and PII Controller's harm mitigation efforts would likely have little effect until the underlying issues in the software are patched. Accordingly, notifications to affected individuals would make most sense once the underlying security threat has been addressed thoroughly.

With this timing of notification standard, the specific facts of the security breach dictate whether the PII Controller provided notifications promptly enough. Barring a statutory liability for notification delays, the affected individuals would likely need to realize harms from the security breach or the delay in notification in order for the PII Controller to incur liability. This timing of notification standard generally leaves the courts in the best position to quantify harms and

⁴⁵ The Heartbleed Bug, <http://heartbleed.com/> (last accessed Sept. 22, 2021).

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than May 27, 2022.

apportion liability. Some states with this timing standard include California,⁴⁶ New York,⁴⁷ Texas,⁴⁸ and Illinois.⁴⁹

It appears that without a set deadline, many PII Controllers argue that as long as a good faith investigation into the breach is ongoing, such PII Controllers do not need to provide notice to affected individuals. Though this approach might match the letter of the law, it defeats the spirit of the law that aims to help individuals protect themselves.

ii. Same as (i) *and* specify a deadline for notice

This approach largely uses the same standard described in approach (i). However, this approach adds the caveat that no more than a specified number of days can pass between the date a security breach is discovered and the date affected individuals receive notification of the breach. In Colorado, for example, the notification requirement reads as follows:

Notice 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 the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.⁵⁰

Like approach (i), the specific facts of a security breach can generally dictate whether expediency or details about the information involved in the breach should be prioritized in the notification to affected individuals. Assuming the PII Controller is working diligently, though, there may be occasions when all the necessary information about the security breach is not yet available, but notifications need to be made. Accordingly, the notification's ability to help prevent further harm to the affected individuals would be diminished. The deadline for notice under such circumstances could appear arbitrary.

If a PII Controller does not work diligently in response to a security breach, the deadline could act as a "safe harbor." PII Controllers may respond to security breaches in such a manner that they meet the statutory deadline, even if the circumstances of the security breach merit a speedier notification. In such cases, affected individuals could realize increased harm for which the PII Controller might not be held liable because it met the statutory deadline.

This approach sets a standard for what constitutes timely notice. Therefore, it takes an important step in protecting affected individuals, even if PII Controllers suffering a breach have to operate with incomplete information at the time of the notification.

⁴⁶ Cal. Civ. Code § 1798.29(a).

⁴⁷ N.Y. Gen. Bus. Law § 899-aa(2).

⁴⁸ Tex. Bus. Com. Code § 521.053(b).

⁴⁹ Ill. Comp. Stat. Ann. ch. 815 §530/10(a).

⁵⁰ Colo. Rev. Stat. Ann. § 6-1-716(2).

The facts of security breaches can be difficult to ascertain. Quantifying the harms realized by affected individuals has proved challenging and apportioning the associated liability has stretched the abilities of the courts. This time of notification standard could shift some liability away from PII Controllers that need to provide notice of security breaches at the expense of affected individuals.

iii. Simply specify a deadline for notice

This standard for the timing of security breach notification simply states that no more than a set number of days can pass between the date a security breach is discovered and the date affected individuals receive notification of the breach. PII Controllers working diligently in response to a breach will work to provide the right information to affected individuals as quickly as possible. However, like approach (ii), when PII Controllers are not prepared to provide an appropriate notification by the deadline, the deadline can seem arbitrary. South Dakota is an example of this, mandating a sixty-day deadline.⁵¹

Unlike approach (ii), this timing of notification standard does not require PII Controllers to provide notifications without unreasonable delay (or as quickly as possible). By setting a hard deadline, though, PII Controllers are required to act in what is deemed a timely manner. The breach notice statute effectively treats all security breaches the same for the purpose of timing of notifications. Even when the facts of security breach merit a very speedy notice to affected individuals, PII Controllers have no disincentive to provide notifications any time sooner than the deadline.

This timing of notification standard can also help promote judicial efficiency. The question of whether the PII Controller's timing of breach notification contributed to an individual's harm would not have much traction under such a statutory construction. Accordingly, this timing of notification standard could shift liability away from PII Controllers that need to provide notice of security breaches at the expense of affected individuals.

All three timing of security breach notification standards have their advantages and disadvantages. A uniform standard should allow for the greatest flexibility in the timing of security breach notifications, while incentivizing diligent responses from PII Controllers.⁵²

Drafting Team notes that creating a 60-day notice requirement generated significant discussion within the Team and seeks guidance from WG11 on the efficacy of this approach and alternative approaches. We also note that the subject of when “the clock starts running” for breach notification purposes is worthy of panel discussion. The Model Data Breach Notification Statute as written does provide some guidance on this issue.

⁵¹ S.D. Stat. Ann § 22-40-20.

⁵² The Drafting Team notes that creating a 60-day notice requirement generated significant discussion within the Team and seeks guidance from WG11 on the efficacy of this approach and alternative approaches. We also note that the subject of when “the clock starts running” for breach notification purposes is worthy of panel discussion. This section as written does provide some guidance on this issue.

H. Under What Circumstances Should Credit Monitoring Be Offered?

Credit monitoring “tracks activity on your credit reports” and “*only* warns you about activity that shows up on your credit report.”⁵³ Credit monitoring alerts you *after* someone has applied for or opened new credit in your name. “Credit monitoring can be helpful in the case of a Social Security number breach,” but “[i]t does not alert you to fraudulent activity on your existing credit or debit card account.”⁵⁴ The timing of the alerts received in connection with credit monitoring is problematic as well. An individual learns *after the fact* of unauthorized use of PII with credit monitoring. As one industry expert stated, “by the time you get the alert, it’s too late, the damage has been done. It just shortens the time to detection so you may have a slightly improved chance of cleaning up damage faster.”⁵⁵

Importantly, however, many consumer finance experts recommend that individuals both freeze their credit and regularly check their credit reports after any data breach to determine if any fraudulent activity has occurred so that it can be quickly remediated.⁵⁶ While credit monitoring has some weaknesses, its service provides consumers with alerts when their credit files have changed, which is consistent with advice from agencies advising consumers to regularly check their credit files.

1. Credit Monitoring and State Breach Notification Laws

Despite some of the inherent weaknesses with credit monitoring, four states⁵⁷ have credit monitoring requirements in connection with their state data breach notification laws. In 2014, California amended its breach notification law as follows:

If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have

⁵³ Identity Theft Protection Services, Fed. Trade Comm’n, <https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services> (last visited Feb. 27, 2017) (emphasis in original).

⁵⁴ *Breach Help: Consumer Tips from the California Attorney General*, CAL. DEP’T JUSTICE CONSUMER INFO. SHEET 17, Oct. 2014, at 1, *available at* <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf>.

⁵⁵ *Are Credit Monitoring Services Worth It?*, KREBS ON SECURITY <http://krebsonsecurity.com/2013/03/are-credit-monitoring-services-worth-it> (quoting Avivah Litan, a fraud analyst with Gartner Inc.).

⁵⁶ This same guidance is recommended by the Federal Trade Commission. *See* Federal Trade Commission, Data Breach Response: A Guide for Business https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf; When Information Is Lost or Exposed, Federal Trade Commission, <https://www.identitytheft.gov/#/Info-Lost-or-Stolen> (last accessed Sept. 22, 2021).

⁵⁷ *See supra* at notes 58 - 63.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than May 27, 2022.

exposed PII defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).⁵⁸

California's law states that identity theft protection services should be used for breaches involving Social Security numbers, driver's license numbers, or California identification card numbers. Noticeably excluded from the types of PII where identity theft protection should be offered under California law are breaches involving account, credit card, or debit card numbers in combination with any required security code, access code, or password that would permit access to an individual's financial account, medical information, health insurance information, and information or data collected through the use or operation of an automated license plate recognition system.⁵⁹

In 2015, Connecticut followed California and passed a law affirmatively requiring "appropriate identity theft prevention services and, if applicable, identity theft mitigation services" for at least one year. It is important to note that the Connecticut law, like the California law, does not require credit monitoring in all cases, but instead requires "appropriate identity theft prevention services." Connecticut Attorney General George Jepsen added the following in connection with the announcement of the new Connecticut law:

The bill also calls for companies who experience breaches to provide no less than one year of identity theft prevention services. This requirement sets a floor for the duration of the protection and does not state explicitly what features the free protection must include. I continue to have enforcement authority to seek more than one year's protection—and to seek broader kinds of protection—where circumstances warrant. Indeed, in matters involving breaches of highly sensitive information, like Social Security numbers, my practice has been to demand two years of protections. I intend to continue to that practice.⁶⁰

Effective October 1, 2018, Connecticut increased its credit monitoring requirement from 12 months to 24 months for residents who experience a security breach affecting Social Security numbers.⁶¹

Delaware's breach notification law is more limited than California's as it requires credit monitoring only in breaches involving Social Security numbers. Specifically, the Delaware law states the following:

If the breach of security includes a Social Security number, the person shall offer to each resident, whose personal information, including Social Security number, was breached or is reasonably believed to have been breached, credit monitoring services at no cost to such resident for a period of 1 year. Such person shall provide

⁵⁸ Cal Civ. Code § 1798.82(d)(2)(G).

⁵⁹ Cal. Civ. Code § 1798.90.5.

⁶⁰ Statement from AG Jepsen on Final Passage of Data Breach Notification and Consumer Protection Legislation, State of Connecticut, June 2, 2015, <https://portal.ct.gov/AG/Press-Releases-Archived/2015-Press-Releases/Statement-from-AG-Jepsen-on-Final-Passage-of-Data-Breach-Notification-and-Consumer-Protection-Legisl>.

⁶¹ Conn. Gen Stat. §36a-701b(b)(2).

all information necessary for such resident to enroll in such services and shall include information on how such resident can place a credit freeze on such resident's credit file.⁶²

On January 10, 2019, Governor of Massachusetts Charlie Baker signed legislation that became effective on April 11, 2019, that requires an offer of complimentary credit monitoring for “a period of not less than 18 months” when the data security incident involves a Massachusetts resident's Social Security number.⁶³

2. *Identity Theft Mitigation/Recovery Services*

In 2014, the Federal Trade Commission estimated that the average identity theft victim spent more than 200 hours across 18 months resolving their issues with credit-reporting agencies.⁶⁴ For this reason, identity theft recovery services provide a significant value to individuals who have been victimized by identity theft. Both California and Connecticut implicitly recognize this value by referring to identity theft mitigation services in connection with their respective laws.

Identity recovery services typically provide trained counselors to help individuals work through the fraud resolution process after receiving notice of a breach. The counselors can assist with writing letters to creditors and debt collectors to dispute unauthorized charges and close accounts, “plac[ing] a freeze on your credit report to prevent an identity thief from opening new accounts in your name, or guid[ing] you through documents you have to review.”⁶⁵ Some services will represent individuals in dealing with creditors or other institutions if formally granted authority to act on the individual's behalf.⁶⁶ Others may help individuals place fraud alerts with the consumer reporting agencies and government agencies. These kinds of services can be extremely valuable especially given the amount of time and effort individuals can spend in addressing issues associated with fraudulent use of name,⁶⁷ Social Security number and account information. For this reason, it is imperative that any state law requirement for credit monitoring include a requirement that the breached entity provide identity restoration services.

Individuals who have been the victim of a data breach may realize some benefits from credit monitoring, but will realize significantly enhanced benefits from having both monitoring and comprehensive identity theft mitigation resources available to them. It is for this reason that the proposed model language below combines credit monitoring with comprehensive identity theft prevention and mitigation/restoration services.

⁶² Del. Code. Ann. § 12B-102(e).

⁶³ Mass. Gen. Laws Ann. ch 93H § 3A(a).

⁶⁴ <https://www.businesswire.com/news/home/20151006006149/en/Latest-Data-Breach-Spotlights-Identity-Restoration>.

⁶⁵ *Id.*

⁶⁶ *See id.*

⁶⁷ “The average identity theft victim spends more than 30 hours dealing with the fallout [of a data breach].” *Worth It Or Not? Identity Theft Protection Reviewed*, (Sept. 24, 2015), (<http://www.magnifymoney.com/blog/identity-theft-protection/identity-theft-protection-worth-best-worst397370535>).

In certain incidents, Dark Web scans can be bundled with credit monitoring and identity restoration services to offer more comprehensive coverage to individuals. The scans can search known web pages on the Dark Web for Social Security numbers, email addresses, phone numbers, or medical information. Because Dark Web scans are only “a point in time,” regular, repeated scans are essential for this service to be effective.

Given the above considerations, the Drafting Team recommends that, if credit monitoring services are provided as a result of a security breach, breached entities should also consider services which include Dark Web monitoring and identity restoration to provide enhanced protections to individuals who were impacted by any security breach.

I. How Should PII Controllers Be Expected to Notify Law Enforcement and Regulatory Authorities?

The state statutes requiring affected entities to notify law enforcement or regulatory authorities vary widely and lack uniformity. Not only do they contain widely diverging timeframes for notice, but they also require notice to different governmental entities under different circumstances. Notably, state notification statutes generally do not require notification to criminal law enforcement authorities. The statutes are uniform, however, in one unfortunate respect: none requires notice to the FBI, the U.S. Secret Service, or the Department of Homeland Security—the three entities principally responsible for combatting cyber threats and other actors driving the number of data breaches across the nation.

1. Various Statutes Requiring Notification to a Law Enforcement Entity

The majority of states and Puerto Rico require notice to some governmental entity.⁶⁸ At least thirty of those states require notification to the Attorney General, three require notice to a consumer protection entity, one requires notice to the State Police, and two require notice to an insurance regulator in the event of a breach involving an insurance company. Notably, California requires notice to different state entities depending on the nature of the breach.

The circumstances giving rise to notification also differ among the states. For example, below is a list of various differences amongst state statutes.

- *No numerical threshold of individuals impacted*—Alaska, Connecticut, Idaho, Indiana, Louisiana, Maine, Maryland, Massachusetts, Montana, Nebraska, New Hampshire, New Jersey, New York, North Carolina, Puerto Rico, Texas, Vermont;
- *250 or more individuals affected*—North Dakota, Ohio, Oregon, Texas, South Dakota (Illinois, if a breach by a state agency occurs);
- *500 or more individuals affected*—California, Colorado, Delaware, Florida, Illinois, Iowa, Rhode Island, Washington;

⁶⁸ Data Breach Charts, Baker & Hostetler LLP, July 2018, available at www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than May 27, 2022.

- *1000 or more individuals affected*—Alabama, Arizona, Hawaii, Missouri, New Mexico, South Carolina, Virginia.

Notification time thresholds also vary:

- *24 hours*—Idaho (if a public agency experiences a data breach);
- *10 days*—Louisiana, Puerto Rico;
- *15 business days*—California (if medical information involved);
- *30 days*—Colorado;
- *45 days*—Alabama, New Mexico, Oregon.

Meanwhile, several states specify the information that affected entities must include in the notice: Alabama, California, Florida, Illinois, Maine (insurance entity), Montana, New Hampshire, New Mexico, North Carolina, Oregon, Rhode Island, Vermont, Virginia, and Washington.

2. *Criminal Law Enforcement Notification*

As a general matter, state data breach statutes appear to focus on the importance of notifying regulators or state attorneys general offices rather than criminal law enforcement authorities. Indeed, few state data breach notification statutes require notifying criminal law enforcement agencies. Although regulatory authorities and civil enforcement actions can play a role in encouraging private industries to adequately protect consumer data, criminal law enforcement authorities play a critical role in exposing, deterring, and incapacitating cyber-criminal threat actors that attack U.S. companies in the first instance.

While at least one state requires notification to the state police,⁶⁹ the lion's share of cybercriminal investigations and prosecutions is conducted by the U.S. Department of Justice, the Federal Bureau of Investigation, the U.S. Secret Service, and to some extent, the Department of Homeland Security. While state and local law enforcement agencies play an important role in combatting events that give rise to data breaches, the interstate and international character of cybercriminal conduct imposes limits on the ability of state and local law enforcement to adequately address the threat.

To that end, a proposed model data breach notification law should consider requiring notification to federal criminal law enforcement authorities. Any such notification requirements should also explicitly assure notifying companies that disclosure of the facts of a data breach to a criminal law enforcement authority shall not waive the attorney-client privilege or work product protections. Unfortunately, concerns about waiving the attorney-client privilege or the results of a privileged internal investigation, especially where companies face the possibility of significant civil liability, often stymie efforts to quickly transmit information to federal law enforcement authorities. The loss of that information can mean the difference between successfully apprehending a malicious actor and failing to do so.

⁶⁹ N.J. Stat. Ann. § 56:6-163.

This approach carries some risk of overwhelming criminal law enforcement authorities with information. But agencies such as the FBI have online portals designed to capture a high volume of complaints: <https://www.ic3.gov>. Moreover, the risks are not unique to notifying criminal law enforcement, as anecdotal data suggests that EU regulators have been overwhelmed by data breach notifications since the GDPR came into force.

3. *Regulatory Notification or Civil Enforcement Notification*

As noted above, a number of jurisdictions require notification, often in very short order, to a regulator or a state entity with the authority to initiate a civil enforcement proceeding, a regulatory action, or to impose fines. Indeed, the GDPR requires regulatory notification within 72 hours unless the breach is “unlikely to result in a risk to the rights and freedoms of natural persons.”

Consideration should be given to the purpose of requiring such notifications, especially on such a swift time horizon. There may be little benefit to requiring a PII Controller to notify a regulator or civil enforcement authority before an PII Controller has had time to sufficiently identify the salient facts of a data breach. Indeed, many forensic investigations into a data security incident can proceed for several weeks before an PII Controller has an appropriate handle on the scope of the problem. Given the limited ability of regulatory and civil enforcement authorities to affirmatively assist an PII Controller impacted by a data security incident, it may be more useful to provide a PII Controller with reasonable time for providing a detailed notice to a regulatory or civil enforcement authority, i.e., requiring at least 30-45 days. This approach would also have the benefit of avoiding multiple rounds of notice to regulators, and thereby avoiding inundating a governmental authority with new information every time a forensic investigator uncovered a previously unknown fact, especially where a risk averse PII Controller may be concerned about the appearance of “hiding” information.

Whatever the timetables requiring notification, care should be taken to create parity with the requirement for notifying impacted individuals.

4. *The Notification to Multiple Regulators*

The challenges of notifying multiple regulatory authorities are a pervasive problem for PII Controllers impacted by a data breach involving a wide swath of data belonging to individuals located in a wide swath of states. Overlapping notification requirements add to the costs of data breaches and impose additional burdens on entities in the midst of what is often a fast-moving crisis.

One solution may be to create a centralized notification system that gives an affected entity the ability to provide notice via an online portal; ideally, the system would be accessible by the different state regulators. One model may be the Federation of Tax Administrators (“FTA”), which acts as a central reporting point for W-2 breaches to state agencies. The FTA processes W-2 breach reporting and then contacts the 42 income tax states with a single process at no charge. (StateAlert@taxadmin.org).

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than May 27, 2022.

Given the above considerations, the Drafting Team recommends that, if an obligation exists pursuant to the Model Breach Notification Statute to provide notice of a Security Breach to a PII Subject, then such notice shall also be provided simultaneously to a state or federal regulatory authority, and that the state enacting language consistent with this model statute should establish a centralized reporting mechanism available via the Internet.

SECTION IV. PROPOSED MODEL DATA BREACH NOTIFICATION LAW

This section sets forth the Commentary's proposed Model Data Breach Notification Law in its entirety.

A. Definitions as used in this section, the term:

1. **“Access”** means the unauthorized viewing, disclosure, acquisition, or exfiltration of data however accomplished, whether by human interaction, automated process (*e.g.*, malware), or other, and whether occurring deliberately, through negligence, innocently, or otherwise.
2. **“Category I PII”** is PII where an (i) an individual's first name, or first initial, and last name in combination with and linked to any one or more of the following data elements:
 - a. Social Security number;
 - b. motor vehicle operator's license number or government identification card number;
 - c. financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords to access the financial account;
 - d. account passwords or personal identification numbers or other access codes for a financial account;
 - e. biometric information, including a fingerprint, retinal scan, and facial recognition data, and genetic information;
 - f. health information about sensitive diagnosis including HIV, STDs, substance abuse or mental health;
 - g. login credentials (including but not limited to email address or username, in combination with password or other access code such as a personal identification number (“pin” or “pin number”)).
3. **“Category II PII”** means PII where the PII controller must evaluate closely the possibility of the PII impacted by the Security Breach causing harm to the PII Subject(s), because the information breached may not be Category I PII but unauthorized access to the PII may still cause harm to the PII Subject. Examples of Category II PII include, but are not limited to:
 - a. date of birth;
 - b. maiden name of the individual's mother;
 - c. digitized or other electronic signature;
 - d. passport number;
 - e. insurance information (identification numbers, insurance policy numbers or any other unique identifying number);

- f. health information that is not sensitive diagnosis information (health history, information about illnesses, information or observations about a patient, etc.);
 - g. employee personnel files or similar evaluations or personal commentary (subjective or objective employee performance metrics, any kind of personal analysis, goals that might be about an identifiable individual, etc.);
 - h. physical asset information that consistently links an item to an individual (MAC address, IP address, car license plate number, home address);
 - i. geolocation data (data used on ride-sharing apps, augmented reality apps or games);
 - j. customer loyalty or affinity account numbers;
 - k. physical asset or software usage data (browser history, cookies, software tokens, usage metadata, etc.);
 - l. data concerning a person's sex life or sexual orientation;
 - m. political affiliations, donations, or beliefs held related to political or social topics;
 - n. information gathered for the specific purpose of allowing an individual to reset his or her password or account credentials;
 - o. any other unique number-based code or characteristic that is about an identifiable individual (phone number, an organizational anonymized code for an individual, etc.).
4. **“De-identified”** means there is no reasonable basis to believe the data is capable of identifying or being associated with a particular individual or a household.
5. **“Encryption”** means a technology for securing computerized data in such a manner that it is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key, which is not accessible by unauthorized persons, and in accordance with generally accepted industry standards.
6. **“Harm”** means loss or damage and includes financial injury (such as increased risk of identity theft or other fraud, or loss of financial or educational opportunity), serious and prolonged emotional injury, embarrassment, humiliation, or loss of reputation. The analysis of “Harm” pursuant to this statute shall have no bearing on a party's ability to bring suit against an entity related to a Security Breach, or a court's jurisdiction over such a suit.
7. **“Notice”** means communication to PII Subjects in the event of a Security Breach, where either Category I PII was involved, or a risk of Harm analysis was performed in connection with Category II PII. Such Notice shall be in the format of Appendix A hereto, or substantially similar.

8. **“Personally Identifiable Information”** (“PII”) means information, whether recorded in electronic or hard copy form or not, about, or pertaining to, or traceable to, either alone or in combination with other information, an identifiable individual.
9. **“PII Controller”** means any for-profit or non-profit entity, or government entity, that collects, receives, maintains, possesses, controls, or has custody of PII.
10. **“PII Subject”** means any individual to whom PII relates.
11. **“Security Breach”** means a circumstance that leads a PII Controller to believe or would lead a reasonable PII Controller to believe that Access to PII has occurred as to PII that it maintains, controls, or has custody, where the PII is neither Encrypted nor De-Identified.

B. Risk of Harm

Any PII Controller which has experienced a Security Breach shall determine (1) whether the PII that has been compromised falls within the list designated herein which automatically triggers reporting obligations on the basis of presumed harm; and if not, (2) whether the PII that has been compromised otherwise has likely caused or is likely to cause Harm.

In the event of a Security Breach involving Category I PII, the PII Controller shall notify the PII Subject and is not required to conduct a risk of Harm evaluation.

Any PII Controller that has experienced a Security Breach of Category II PII shall determine as to each PII Subject associated with the PII in question whether the Security Breach as to that associated PII has likely caused or is likely to cause Harm to that PII Subject.

In determining whether the Security Breach has likely caused or is likely to cause such Harm, the PII Controller shall consider:

- the nature, extent and sensitivity of the PII;
- the extent to which the data integrity or availability of the PII to the PII Subject may have been adversely impacted;
- the identity of the person who Accessed the PII without authorization;
- the likelihood that the PII has been or will be misused in a manner resulting in harm;
- whether the risk that the PII would be misused in such a manner has been mitigated following its unauthorized Access;
- the type of breach (e.g., whether a fraudulent third party is involved) and the likelihood of misuse;
- ease of identification of individuals (is full name present or are they well known);

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than May 27, 2022.

- severity of consequences for individuals arising from misuse of their information (e.g., financial fraud, identity fraud, physical harm or distress); and/or
- special characteristics of the individuals (e.g., elderly, children or vulnerable categories of individuals)

If a PII Controller that has experienced a Security Breach determines, after conducting the investigation required by this Section, that it has no obligation under Section D to provide notice of the Security Breach to one or more of the PII Subjects associated with the PII in question, the PII Controller shall make and preserve a record of its investigation and determination for production to any regulator when requested.

C. Effect of Encryption, De-identification, and Similar Technologies

Access to PII does not constitute a Security Breach if the PII has been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of an effective technology or methodology or has otherwise been made not reasonably capable of being associated with an individual or household. For example, a Security Breach has not occurred if (i) the PII is Encrypted, anonymized, pseudonymized, or De-identified; and (ii) the Encryption key and/or re-identification key likely has not been acquired by the unauthorized person; and (iii) the PII is not otherwise likely capable of de-anonymization, de-pseudonymization, or re-identification by an unauthorized person.

D. Notification Procedures

If a PII Controller that has experienced a Security Breach determines following an investigation conducted in accordance with Section B above that the Security Breach likely caused or is likely to cause Harm to one or more of the PII Subjects associated with the PII in question, then the PII Controller shall provide Notice of the Security Breach to each PII Subject as to which the PII Controller made such determination.

Where an obligation to provide Notice of a Security Breach to a PII Subject exists under this Paragraph D, such Notice shall be provided either by the PII Controller or by another party that has an agreement with the PII Controller that allows the PII Controller to require the other party to provide such Notice absent exigent circumstances. The PII Controller remains responsible for ensuring that Notice of the Security Breach is provided, either by itself or by its service provider or contract partner.

Where an obligation exists under this Paragraph D above to provide Notice of a Security Breach to a PII Subject, such Notice to such PII Subject should be provided either through traditional U.S. mail or, if the party providing the notice has previously communicated with the PII subject via email, through email with a subject line which will ensure that 1) the message will be delivered to the PII Subject and will not be captured by spam or junk filters; 2) will communicate the importance of the notice; and 3) will encourage the PII Subject to read the notice.

If the PII Controller does not have access to the U.S. mail or email of each PII Subject, the PII Controller shall make a post for at least 60 days on the PII Controller's website if the PII Controller maintains one. This post shall consist of a link to the Notice on the home page or first significant page after entering the website that is in larger type or contrasting type, font or color to surrounding text of the same size or set off from other text by symbols or marks that call attention to the link. If the PII Controller does not have a website, notice may be given through notification to major print or broadcast media where the affected individuals likely reside.

PII Controllers shall provide supplemental Notice to individuals as reasonably needed, as new information about a breach is uncovered through the course of investigation, including but not limited to new information about the nature of the breach or the individuals affected. Supplemental Notice should be made in the same manner as the original notices.

E. Form of Notice

Any notice required to be given to a PII Subject by Paragraph D shall be in the following form and shall include at least the following information:

- Title "NOTICE OF DATA BREACH" in all capital letters
- Salutation: "Dear [First and Last Name of Individual]:"
- Introductory Statement:
 - a. Brief statement of why the notice is being sent to the PII Subject.
 - b. For example: "We are writing to provide you with information about a data incident involving [Name of organization experiencing the breach]. You are receiving this letter because you [Describe relationship between the PII Subject in question and the PII Controller in question]."
- What Happened?
 - a. Brief description of the Security Breach that triggered the notification, including the number of individuals involved, if known.
 - b. Date of Security Breach discovery and, if known, date range during which the Security Breach occurred.
- What Information Was Involved?
 - a. Description of the PII in question specific to the PII Subject.
- What Are We Doing About It?
 - a. General description of any actions taken by the PII Controller to address the Security Breach.

- b. Who else has been notified? (Law enforcement, credit bureaus, state agencies)
 - c. Describe cooperation with law enforcement, as appropriate
- What Can You Do?
 - a. General description of/recommendations for what the PII Subject can do to further protect himself/herself from whatever harm the PII Controller has determined the Security Breach has likely caused or is likely to cause the PII Subject

Where appropriate the “What Can You Do” section may include any or all of the following:

- i. Provide contact information for three major credit bureaus, and statement of right to free credit report;
 - ii. Provide contact information for FTC; and
 - iii. Provide contact information for State Attorney General/Protection Agency
- Where required by Paragraph G, include offer of services called for by Paragraph G.
- For More Information: Provide contact information for point person at entity giving the notice to respond to questions and/or address concerns that the PII Subject can use to inquire about the Security Breach and the other matters set forth in the notice.

F. Notification Timeline

Where an obligation exists under Paragraph D to provide Notice of a Security Breach to a PII Subject, such Notice shall be provided without unreasonable delay and in an expedient manner but not later than 60 days after the PII Controller in question first came to believe, or reasonably should have come to believe, that a Security Breach had occurred as to the PII associated with such PII Subject, unless good cause exists to delay providing such Notice.

G. Identity Theft Prevention and Mitigation Services

Where an obligation exists under Paragraph D to provide Notice of a Security Breach, such Notice shall include an offer to provide credit monitoring in combination with identity theft prevention and mitigation/restoration services, all of which services shall be provided at no cost to the PII Subject in question, for not less than 24 months along with all information necessary to enable such PII Subject to take advantage of the offer, if the Security Breach in question involved unauthorized Access to the PII Subject’s Social Security number, driver’s license number, or state or federal identification number (*e.g.*, passport number). For purposes of the preceding sentence, “identity theft mitigation and restoration services” shall include, but are not necessarily limited to: (1) assistance with communicating with creditors and debt collectors; (2) notifying lenders and

credit card companies; (3) providing information and assistance with notifying state's Department of Motor Vehicles in connection with driver's license fraud, notifying the FTC and the Social Security Administration for Social Security number fraud, the U.S. State Department, Passport Services Department for passport fraud and the U.S. Postal Service for mail theft; or (4) assistance to the PII Subject in question in placing a freeze on his or her credit report to prevent an identity thief from opening new accounts in his or her name and in completing the necessary forms. The PII Subject shall not be charged for any of these services, nor shall the PII Subject be "upsold" any services in connection with these services. The PII Subject shall receive notification before any such services described in this section expire, and in no event shall the PII Subject be automatically charged for a continuation of such services after they expire unless the PII Subject explicitly elects to continue such services via separate communication and in writing.

H. Regulator Notification

Where an obligation exists under Paragraph D above to provide notice of a Security Breach to a PII Subject, notice of such Security Breach shall simultaneously be provided to [enacting authority to identify notice recipient], in the form and manner specified by such entity. Notwithstanding anything to the contrary in the preceding sentence, in the event notice of a particular Security Breach is required to be given to multiple governmental entities within a state or to multiple jurisdictions, the notice required by the preceding sentence may be provided via centralized reporting through [insert website], in the form and manner specified by such website, with such notice to be processed and forwarded to government entities as specified by such website.

APPENDIX A: MODEL DATA BREACH NOTICE

[to be inserted]

APPENDIX B: DECISION TREE FOR DATA BREACH NOTIFICATION STATUTE

[to be inserted]