

The Sedona Conference Draft Commentary on Proposed Model Data Breach Notification Law (September 2020) – Redline Version



Copyright 2020, The Sedona Conference.
All rights reserved.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission.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 November 1, 2020.

The Sedona Conference Draft Commentary on Proposed Model Data Breach Notification Law (September 2020 Redline* Draft)

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.)

Lawrence Wescott

Al Saikali (Steering Committee Liaison)

*This redline version highlights the changes made to the last draft circulated for member review and comment. A clean version is also available.

The Sedona Conference

WG11 Draft Commentary on Proposed Model Data Breach Notification Law

I. INTRODUCTION

This Commentary is intended to assist federal and state lawmakers update or enact ~~laws governing~~ data breach notification ~~laws~~ that: (i) ~~appropriately~~ protect individuals; and (ii) provide concise, clear and consistent direction to organizations ~~who are~~ responding to data security incidents. ~~Lawmakers in the United States would benefit from a model data breach notification law, informed by~~ This commentary was prepared by a cross-section of experienced privacy lawyers, technology experts, and regulatory authorities; ~~that would replace separate and often conflicting state~~ who seek to reduce conflict between the various state data breach notification laws.

~~In this commentary we have identified~~ The Commentary addresses eight areas ~~in typical states where~~ model data breach notification laws ~~that would benefit from the~~ can be improved by uniformity of ~~a model data breach notification law~~: (1) definition of security breach; (2) definition of personally identifiable information (“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. 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., right of private action, notification to consumer reporting agencies, definitions of records, covered entities, substitute notice, law enforcement delay, form of regulator notice, etc. We focused on these eight areas because, based upon our collective experience, these requirements would benefit the most from the uniformity of a Model Data Breach Notification Law.

II. PURPOSE

1. The current patchwork of timelines, definitions, requirements, and expectations creates confusion and is inefficient.
- ~~2. Many organizations that must comply with current breach notification requirements do not have specialized data breach counsel or do not have counsel at all — and must try to interpret these laws themselves. The more complicated and opaque a law is, the more difficult it is for smaller organizations to comply with their obligations. A model data breach notification law written in plain language that is generally understandable would make compliance less daunting.~~
2. To ensure that data subjects learn of data breaches impacting their personal information in an expedient, clear, and consistent way, so they can take steps, like enrolling in credit monitoring, to remediate any potential risks.

3. To make breach notification laws easier for organizations without privacy counsel (or any counsel) to understand.

~~4. To better protect themselves, individuals impacted by a data breach need to know, with sufficient detail, about breaches in the most expedient time possible and without unreasonable delay. One uniform law applying to all breached entities would ensure clear, concise and consistent notices to all affected individuals regardless of where they live or where the breach occurs. Armed with the knowledge that they may be exposed, individuals can take steps like signing up for credit monitoring, identity theft prevention, mitigation and restoration services.~~

4. A single standard method and single point of contact for reporting data breaches would ~~both simplify processes for all organizations in the decrease~~ regulatory community overlap and enhance the protection of PII ~~both before and after a breach. This would benefit individuals who are impacted by breaches.~~

5. Timely awareness by regulators and law enforcement will help them discern trends and the potential for more systemic outbreaks. A model law applying to all entities would ensure timely alerts to the applicable regulator regardless of where they transact business, where the breach occurs, or where the affected individuals reside.

5-6. Standardization of reporting would aid researchers, security officers, and consultants, and policy makers who track statistics and trends in data breaches.

III. BACKGROUND

Security breach notification ~~requirements are laws of general applicability—they can potentially~~ impose obligations on any organization, regardless of its size, sophistication, or industry. ~~All~~ Similarly, all organizations are vulnerable to security breaches, regardless of how mindful they are of data security. Organizations frequently experience security incidents that may give rise to breach notice obligations.¹

A Model Data Breach Notification Law should be tailored to require that only certain incidents be considered reportable security breaches. ~~It~~ Such would not be appropriate policy to require that *all* security incidents be reported. This would lead to notice fatigue in consumers, 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

¹ 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.

to be concerned about their data security, despite recent major data breaches.² 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.”³

Thus, not only would frequent notices lose their effectiveness, but they would also impose an unnecessary burden on the business community. As discussed in more detail in Section V, 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 qualifies as a breach can be time consuming and costly. If the media affected includes emails, file systems, backup tapes, or paper records, search algorithms might not suffice, and individuals might be required to pore over terabytes of data. Often forensic investigators must be retained by counsel to determine exactly what happened and, working with counsel to determine whether an incident qualifies as a breach. In addition to expense, these activities take time, during which consumers who may be vulnerable to fraud and identity theft are not being made aware of their exposure. These activities are also expensive for organizations and their insurers. Thus, a Model Data Breach Notification Law should be drafted to make it as clear as possible what constitutes a breach 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 organizations, it must remain broad enough to ensure that consumers are protected. Any consideration of what should or should not be included in such a law must be weighed against the fundamental need to protect consumers.

It is critical that a Model Data Breach Notification Law should be drafted with these principles in mind. It should first make clear what constitutes a data breach, as all other obligations flow from that initial analysis.

IV. PROPOSED MODEL DATA BREACH NOTIFICATION LAW

This section sets forth the proposed model data breach notification law in its entirety. Subsequent sections explain each section, and why the Commentary made certain choices in the language used.

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

“Security Breach” means a circumstance ~~which would lead~~that would leads a reasonable PII ~~Collector~~Controller to believe ~~that PII Controller that~~ unauthorized Access to PII ~~that is neither Encrypted nor De-identified has~~as to PII that it maintains, controls, or has custody of occurred and that such unauthorized Access compromises the security, confidentiality, or integrity of such PII.

² 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).

³ *Id.*

1. “Personally Identifiable Information” (“PII”) means factual or subjective 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 (any such individual being defined as the “PII Subject” with respect to information that is about or pertains to or is traceable to him or her).
- 1.2. “PII CollectorControllerController” means any for-profit or non-profit entity, or government entity, that collects, receives, maintains, possesses, controls, or is in the custody of PII.
3. “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.
- 2.4. “Encryption” means 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.
2. “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.
3. “Encryption” means 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.
- 3.5.4. “Access” to data means the 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).

Good faith unauthorized Access to PII by an employee or agent of a PII CollectorController is not a Security Breach to the extent that, such Access, while unauthorized, was engaged in for purposes within the scope of the PII Collector’sController’s legally authorized Access to or use of the PII in question.

In determining whether a Security Breach as defined above, has occurred, a PII Collector shall consider the following factors, among others:
PII Controller

The following non-exclusive list of examples provides guidance as to what constitutes Access:

Factors to consider in determining if there is a reasonable belief that there is access a Security breach has occurred include:

- a. indications that the PII ~~in question~~ is no longer in the ~~physical~~ possession and control of the PII ~~Collector~~Controller and as a consequence is at risk of unauthorized Access or use, such as a lost or stolen ~~computer or other~~mobile device containing ~~information, where the device~~PII (subject to the exclusions in Section C below) ~~that is not Encrypted, there is PII on the device, the PII is not or~~ De-identified, and the device was not remotely deactivated or wiped pursuant to the entity's data loss procedures;
- b. indications that the PII ~~in question~~ has been downloaded, copied ~~or~~, queried or searched without authorization;
- c. indications that the PII ~~in question~~ was used by an unauthorized person, ~~such as to open~~ fraudulent accounts ~~opened or instances of~~ for identity theft ~~reported~~;
- d. information that the PII has been made public (e.g., provided to media, available on the Dark Web) and indications that the source of the PII ~~in question~~ is the PII ~~Collector~~Controller;
- e. indications ~~of a of a~~ larger pattern of potentially unauthorized activity sufficient to warrant further internal investigation (e.g., spikes in account creation from certain locations, spikes in coupon code usage, prolonged anomalous internet traffic to specific pages, etc.); ~~or and~~
- f. ~~i~~ indications that any unauthorized Access ~~that may have occurred as to of~~ the PII ~~in question~~ could ~~not~~ have resulted in misuse of that PII (e.g., PII sent in the mail and returned by recipient or post office unopened could not have been misused even if it was thought to have thereby been accessed).

~~4. 5. "Personally Identifiable Information" ("PII") means factual or subjective 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 (any such individual being defined as a the "PII Subject" with respect to information that is about or pertains to or is traceable to him or her).~~

B. Risk of Harm

Any PII ~~Collector~~Controller that has experienced a Security Breach 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 ~~legally cognizable~~ harm to ~~one or more of the PII Subjects associated with the PII in question~~that PII Subject. In determining whether the Security Breach has caused or is likely to cause such ~~legally cognizable~~ harm, the PII ~~Collector~~Controller shall consider:

1. whether the PII ~~in question~~ was secured in such a way that rendered it unusable, based on generally accepted industry standards;
2. the nature and extent of the PII ~~in question~~;

3. the extent to which the data integrity or availability of the PII to the PII Subject may have been adversely impacted;
4. ~~3.~~ the identity of the person who Accessed the PII ~~in-question~~ without authorization; and
4. ~~the extent to which the risk that the PII in question would be misused has been mitigated following its unauthorized Access; and~~
5. the likelihood that the PII ~~in-question~~ has been or will be misused to perpetrate identity theft or attacks and/or crimes beyond identity theft resulting in ~~legally cognizable~~ injury; and
6. whether the risk that the PII would be misused has been mitigated following its unauthorized Access.

If a PII ~~Collector~~Controller that has experienced a Security Breach determines, after conducting the investigation required by this Section, that the Security Breach has not caused or is not likely to cause ~~legally cognizable~~ harm to one or more ~~of the~~ PII Subjects ~~associated with the PII in question~~, the PII ~~Collector~~Controller shall make and preserve a record of its investigation and findings for production to any regulator when requested.⁴

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 has not been acquired by ~~an~~ unauthorized person ~~that materially compromises the security, confidentiality, or integrity of the encrypted PII~~; and (iii) the PII is not otherwise ~~subject to~~ likely capable of de-anonymization, de-pseudonymization, or re-identification by an unauthorized person.

D. Notification Procedures

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

⁴ 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 situation described in this sentence; and, if such notification is required, (2) what the consequences should be in the event~~ the regulator ~~must~~does not agree with the PII ~~Controller~~Collector's determination. For this reason, the Drafting Team seeks input from WG 11 on the most effective approach.

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 ~~Collector that experienced the Security Breach~~Controller or by another party that has an agreement with the PII ~~Collector that obliges~~Controller that allows the PII Controller to require the party to provide such notice. The PII ~~Collector~~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.

If an Organization does not have access to the U.S. mail or email of each PII Subject, the Organization shall post for at least 60 days on the Organization's website if the Organization 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 an Organization does not have a website, notice may be given through notification to major print or broadcast media where the affected individuals likely reside.

Commented [U1]: Modeled this off of California's language. This makes things more complicated, but I was thinking notice should be through U.S. Mail or email, if not that, then the website, and if not a website, then through statewide media. Please see note below on whether we need to plan for situation for an org that has no email, U.S. mail, not a website.

Organizations may 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:

1. Title "NOTICE OF DATA BREACH" in all capital letters
2. Salutation: "Dear [First and Last Name of Individual]:"
3. Introductory Statement:
 - a. Brief statement of why the notice is being sent to the PII Subject ~~in question~~.
 - 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 ~~Collector~~Controller in question]."
4. What Happened?
 - a. Brief description of the Security Breach that triggered the notification
 - b. Date of Security Breach discovery and, if known, date range during which the Security Breach occurred

5. What Information Was Involved?
 - a. Description of the PII in question
6. What Are We Doing About It?
 - a. General description of any actions taken by the PII ~~Collector~~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
7. What Can You Do?
 - a. General description of/recommendations for what the PII Subject can do to further protect himself/herself from whatever ~~legally cognizable~~ harm the PII ~~Collector~~Controller has determined the Security Breach has 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
 - iii. Provide contact information for State Attorney General/Consumer Protection Agency
8. Where required by Paragraph G, include offer of services called for by Paragraph G.
9. 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 ~~Collector~~Controller in question first learned of the Security Breach, unless good cause exists to delay providing such notice.⁵

G. Identity Theft Prevention and Mitigation Services

Where an obligation exists under Paragraph D to provide notice of a Security Breach ~~to a~~ ~~PII Subject~~, 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

⁵ 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.

restoration services” shall include, but are not necessarily ~~be limited to, services that include the following:~~ (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; ~~and 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.

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.

V. ANALYSIS AND DISCUSSION OF DATA BREACH NOTIFICATION LAWS

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 proposed model language.

A. What Should ~~be~~Be the Definition of a Data Security Breach?

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

The first ~~test as to~~issue in deciding whether a security incident should trigger a notice obligation is whether be considered a breach is whether PII was affected.⁶ An organization that does not collect PII need not worry about having to provide notice to a consumer for a breach of PII, and organizations that must 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 breach.

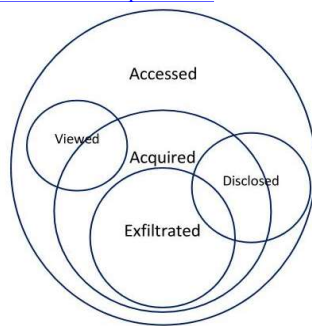
~~Currently, state data breach notice laws vary significantly in the definition of PII. Most states contain a laundry list of data elements that are amended from time to time in order to keep up with~~

⁶ See, e.g. *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.

~~advances in technology. These lists can vary widely from state to state. See discussion of what constitutes PHI in Section V.B *infra*.~~

Assuming that PII was affected, the next question is ~~how~~ whether the data involved in the incident was affected in a manner sufficient to make notice worthy of consideration. The terms most often used ~~in this analysis~~ 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*.

~~While these~~ These different terms are subject to interpretation, and debate – the Venn diagram below provides ~~some guidance~~ one such interpretation:



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 emails 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

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

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

Some states have recognized that it is difficult to determine absolutely that access took place due to inadequate logging, sophisticated attackers, or intervening circumstances. They have required that an organization report a breach if it has a *reasonable belief* of access without providing any examples of what constitutes a reasonable belief.¹⁰

~~A breach notice statute might be limited to certain types of organizations, to exclude public or non-profit entities, to include only electronic data or to limit breaches to a certain threshold number of consumers affected. We recommend against including such limiting factors and to adopt a broad definition of PH Collector/Controller that includes both public and private entities and both electronic and paper records.~~

Thus, a broad definition of breach would be:

⁸ See, e.g., Fla. Stat. Ann. §501.171(1)(a) (LexisNexis2019)(“ ‘Breach of security’ or ‘breach’ means unauthorized access of data in electronic form containing personal information.”); N.J. Stat. Ann. § 56:8-163(a) (LexisNexis 2019)(“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) (LexisNexis 2019)(“ ‘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)(LexisNexis 2019)(“ ‘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) (LexisNexis 2019)(“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) (LexisNexis 2019) (“ ‘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) (LexisNexis2019) (“ ‘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)(LexisNexis 2019)(“ ‘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 See, e.g., Alaska Stat. § 45.48.090(1) (LexisNexis 2019) (“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) (LexisNexis 2019) (“ ‘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.”).

“Security Breach” means unauthorized Access to data or a circumstance which would lead a reasonable PII ~~Collector~~Controller to believe that an unauthorized Access to Unencrypted data has occurred that compromises the security, confidentiality, or integrity of an individual’s PII maintained by that PII ~~Collector~~Controller.

However, ~~within~~ this definition of breach, includes certain incidents that have no, or a low, likelihood of causing harm to the ~~individual~~individual(s) whose PII was accessed without authorization during the incident, and such incidents therefore can safely be excluded. ~~In addition, exclusions might be considered if they have from the definition, particularly where the exclusion~~ has the benefit of encouraging organizations to adopt best practices. One such exclusion would be for unauthorized access to encrypted or sufficiently de-identified data.¹¹ Where the accessed data is encrypted or de-identified, it should be unusable by bad actors. For this reason, access to encrypted or de-identified data ~~is~~should not be considered a ~~data breach. Obviously, the exclusion is not applicable if~~security breach potentially worthy of requiring notice, unless the bad actor also possesses the encryption key or is otherwise likely able to re-identify the data ~~through reasonable means~~.¹² 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.” See the further discussion of encryption, de-identification and related technologies in Section V.D, *infra*.

Another situation in which there is a low likelihood of injury to the individual(s) in question is 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.¹³

2. Challenges Created by Current Laws

¹¹ 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 here. 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.

¹² See, e.g. Tex. Bus. & Com. Code § 521.053(a)(LexisNexis 2019)(“ 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.”)

¹³ See, e.g. Iowa Code § 715C.1(1) (LexisNexis 2019)(“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.”).

The use of the term “acquisition” as the means of data interaction for triggering the notice obligation not only is less consumer-friendly, but also may create difficulties in the cloud computing context. ~~Cloud computing arrangements create problems for establishing data misappropriation when applying the term “acquisition.”~~

To the extent that states fail to include risk of harm provisions in their notice statutes, or provide different language in their risk of loss provisions, organizations will be disadvantaged in being required to implement different notice thresholds in different states, or at least analyze the varying provisions in order to make notice determinations.

Finally, because security incidents are often very fact 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 beginning on page 5). 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 an organization to rationalize why any individual breach is unlikely to lead to harm.

Proposed Model Language

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

“**Security Breach**” means a circumstance ~~that would lead~~~~which would lead~~ a reasonable PII ~~Collector~~~~Controller~~ to believe that unauthorized Access to PII ~~that is neither Encrypted nor De-identified~~ has occurred as to PII that it maintains, controls, or has custody of and that such unauthorized Access compromises the security, confidentiality, or integrity of such PII.

“**Personally Identifiable Information**” (“**PII**”) means factual or subjective 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 (any such individual being defined as the “PII Subject” with respect to information that is about or pertains to or is traceable to him or her).

“**PII ~~Collector~~Controller**” means any for-profit or non-profit entity, or government entity, that collects, receives, maintains, possesses, controls or is in the custody of PII.

“**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.

“**Encryption**” means 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.

1. “**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.

2. ~~“Encryption” means 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.~~

“Access” ~~to data~~ means the 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).

Good faith unauthorized Access to PII by an employee or agent of a PII ~~Collector~~Controller is not a Security Breach to the extent that, such Access, while unauthorized, was engaged in for purposes within the scope of the PII ~~Collector’s~~Controller’s legally authorized Access to or use of the PII in question.

The following non-exclusive list of examples provides guidance as to what constitutes Access:

Factors to consider if there is a reasonable belief there is access include:

~~In determining whether a Security Breach as defined above, has occurred, a PII CollectorController shall consider the following factors, among others:~~

- a. indications that the PII ~~in question~~ is no longer in the physical possession and control of the PII ~~Collector~~Controller and as a consequence is at risk of unauthorized Access or use, such as a lost or stolen ~~mobile computer or other device containing information, where the device is not Encrypted, there is PII on the device, (subject to the exclusions in Section C below) the PII is not De-identified,~~ and the device was not remotely deactivated or wiped pursuant to the entity’s data loss procedures;
- b. indications that the PII ~~in question~~ has been downloaded, copied or queried or searched without authorization;
- c. indications that the PII ~~in question~~ was used by an unauthorized person ~~to open, such as fraudulent accounts foreopened or instances of identity theft reported;~~
- d. information that the PII has been made public (e.g., provided to media, available on the Dark Web) and indications that the source of the PII in question is the PII ~~Collector~~Controller;
- e. indications of a larger pattern of potentially unauthorized activity sufficient to warrant further internal investigation (e.g., spikes in account creation from certain locations, spikes in coupon code usage, prolonged anomalous internet traffic to specific pages, etc.); ~~or and~~
- f. indications that any unauthorized Access ~~of that may have occurred as to the PII in question could not~~ have resulted in misuse of that PII (e.g., PII sent in the mail and returned by recipient or post office

unopened could not have been misused even if it was thought to have thereby been accessed).

B. What Should be the Meaning of PII for the Purpose of Data Breach Notification?

The second issue in deciding whether a security incident should trigger a notice obligation is whether the data involved in the incident was personally identifiable information (PII).¹⁴ An organization that does not collect, maintain, control, or have custody of PII thus normally need not worry about having to provide notice of a security incident. Other organizations, however, do.

Currently, state data breach notice laws vary significantly in the definition of what sort 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 vary widely from state to state.

A broad definition of PII is proposed [here](#). This [definition](#) will capture new types of “personal” information as our online habits change and the landscape of cyber threats evolves. Further, this [flexiblebroad](#) approach to defining PII is necessary to support the [the proposed definition of harm](#)~~proposed definition of harm which includes~~[paper’s proposal that the risk of harm analysis focus on “legally cognizable harm,” which \(depending on the jurisdiction\) could include](#) (among other things) bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities. Given the regular emergence of new technologies it is unduly limiting to create a finite list of PII. Such a list necessarily would not anticipate what specific forms of information could ~~conceivably~~[likely](#) give rise to harm of this nature [when subjected to unauthorized access](#), because this [risk-of-harm](#) analysis is context-sensitive.

1. Current State Data Breach Notification Laws

In the United States there are varying definitions of PII among the states. The state data breach notification laws each specify the particular information that is defined to be “personal,” such that a compromise of that kind of information may amount to a reportable breach. ~~Providing specific types of data that trigger a breach informs businesses when making data protection and tracking decisions. However, there are new types~~[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 ~~can be~~[is not already expressly identified](#).

[This static approach to defining PII does not account for the evolving cyber threat landscape where new types of PII are](#) compromised and [can](#) cause the same or greater level of harm as the compromise of traditionally accepted categories of PII~~such as credit card numbers. This static approach to defining PII ignores the evolving cyber threat landscape and could become outdated quickly.~~[For example, categories of PII that are increasingly compromised include a data subject’s](#)

¹⁴ See, e.g. *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.

[contact list, geolocation data, and employment information. The ability of threat actors to monetize increasing categories of PII continues to expand. A static definition of PII does not account for this evolving threat.](#)

[This threat to an expanding number of categories of PII 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 PII that is subject to compromise through a security breach.](#)

~~The static approach to defining PII requires legislative reform each time a breach highlights an additional example of personal information that might cause harm when accessed without authorization. Consider how the State of California modified its definition of PII in the wake of the Marriott breach so that passport numbers were included in the definition of PII. Rather than being forced to enact legislative reform upon a breach involving a form of PII that has not previously been defined as notice triggering PII, the proposed flexible approach allows the custodians of the information and the regulators to assess whether the information in question should properly be defined as PII in the circumstances of the particular breach.~~

[Additionally, the static definition of PII does not account for new categories of PII 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 further example of the benefit of the flexible approach is highlighted from the Uber breach. Consider how the emergence of Uber may have created a new category of PII. With the use of Uber, the routes we take, the frequency and the times of day that we take Uber may be considered to be PII \(“geolocation data”\). A similar example involves the geolocation data collected by augmented-reality applications such as Pokémon Go, which are typically used by children. It is conceivable that disclosure of this information could cause harm, as discussed in Part V.C *infra*.](#)

[The static approach to defining PII requires legislative reform as new categories of PII are revealed to be at risk and which may give rise to cognizable harm.](#)

2. Current Compliance Challenges

The practical problem that an organization faces in the event of an incident is the conflicting state regimes with which it must comply. What may constitute a reportable breach in one state is not in another. ~~This also creates difficulty for organizations in developing their data protection strategy. When identifying the types of information that they must protect, an organization will need to comply with the varied definitions of PII.~~

[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 cognizable 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 cognizable harm in that jurisdiction and for that reason, notice to impacted individuals involving that category of information is not required. Based on those categories of information identified in the definition of PII, an organization may develop a data protection strategy that focuses on protecting listed categories of information. In this way, the state breach notification laws identify](#)

[obligations on custodians 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 difficulty for organizations in developing their data protection strategy](#)

The following types of PII have been included in various states' definitions:

1. Social Security number;
2. motor vehicle operator's license number or non-driver identification card number;
3. 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;
4. account passwords or personal identification numbers or other access codes for a financial account;
5. biometric information, including a fingerprint, retinal scan, and facial recognition data;
6. genetic information;
7. health information;
8. health insurance policy number or health insurance identification number and any unique identifier used by a health insurer to identify an individual;
9. login credentials, including a username or password; and
10. 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,¹⁴¹⁵ but not in others such as Alabama, Arkansas, ~~California~~, Florida, Indiana, Kansas, Massachusetts, and Nevada.¹⁵¹⁶

¹⁴¹⁵ [Cal. Civ. Code Ann. § 1798.29\(g\)\(LexisNexis 2020\)](#); Colo. Rev. Stat. Ann. § 6-1-716(g)(LexisNexis 2019); Del. Code. Ann. tit 6 § 12B-101(7)(LexisNexis 2019); La. Rev. Stat. § 51:3073(4)(a)(LexisNexis 2019); Md. Com. Law. Code Ann. § 14-3501(e)(LexisNexis 2019); Neb. Rev. Stat. § 87-802(5)(LexisNexis 2019); N.M. Stat. Ann. § 57-12C-2(C)(LexisNexis 2019); N.M. Stat. Ann. § 57-12C-2(C)(LexisNexis 2019); [Vt. Stat. Ann. tit. 9 § 2430 \(10\)\(LexisNexis 2020\)](#).

¹⁵ Code of Ala. § 8-38-2(6) (LexisNexis 2019); Ark. Code. Ann. § 4-110-103(7)(LexisNexis 2019); Cal. Civ. Code Ann. § 1798.29(g)(LexisNexis 2019); Fla. Stat. Ann. § 501.171(1)(g)(LexisNexis 2019); Ind. Code. Ann. § 24-4.9-2-10 (LexisNexis 2019); Kan. Stat. Ann. § 50-7a01(g)(LexisNexis 2019); Mass. Gen. Laws Ann. ch. 93H, § 1(a)(LexisNexis 2019); Nev. Rev. Stat. Ann. § 603A.040(1)(LexisNexis 2019).

¹⁶ Code of Ala. § 8-38-2(6) (LexisNexis 2019); Ark. Code. Ann. § 4-110-103(7)(LexisNexis 2019); Fla. Stat. Ann. § 501.171(1)(g)(LexisNexis 2019); Ind. Code. Ann. § 24-4.9-2-10 (LexisNexis 2019); Kan. Stat. Ann. § 50-7a01(g)(LexisNexis 2019); Mass. Gen. Laws Ann. ch. 93H, § 1(a)(LexisNexis 2019); Nev. Rev. Stat. Ann. § 603A.040(1)(LexisNexis 2019).

Passport number is included in the definition of PII in states such as Alabama, Colorado, Delaware, Florida, Louisiana, ~~and Maryland~~ and Vermont,¹⁶¹⁷ but not in others such as Arkansas, California, Indiana, Massachusetts, Minnesota, Nebraska, New Mexico, Nevada, and Rhode Island.¹⁷¹⁸

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

3. Guidance Regarding the Scope of PII

A potential criticism of the ~~flexible~~ broad PII definition is that organizations will not have advance notice of the specific types of PII ~~they are obligated to safeguard that that~~ could trigger a notice obligation if accessed without authorization and that organizations may be penalized for failing to ~~protect PH~~ provide notice based on unauthorized access to data that they did not consider to be ~~so defined~~ PII. However, the proposed definition is simple: ~~any information that could be used to identify an individual through the use of that information, alone or in combination with other information is PII, with the following exceptions: factual or subjective information, pertaining to, or traceable to, an identifiable individual.~~]

- ~~1. Business contact information such as an employee's name, title, business address, telephone number, or email addresses that is collected, used or disclosed solely for the purpose of communicating with that person in relation to their employment, business or profession.~~
- ~~2. An organization's collection, use, or disclosure of personal information solely for journalistic, artistic or literary purposes.~~
- ~~3. Personal information handled by government organizations when collected, used or disclosed solely for governmental purposes. [NTD: this exclusion presumes there is parallel legislation that governs government institutions.]~~

~~As such, PH is factual or subjective information, 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.~~ Guidance is provided on the scope of PII as follows:

- Information will ~~be about~~ pertain to, be traceable to, an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.
- PII covers all means of information that meets the definition of PII regardless of how or from whom its acquisition occurred: whether consciously provided, observed, derived, or inferred.

The following is an illustrative, but non-exhaustive, list of classes of PII to aide in current understanding and future analysis:

¹⁶ See *supra* notes 14 & 15¹⁷ Code of Ala. §8-38-2(6) (LexisNexis 2020); Colo. Rev. Stat. Ann. § 6-1-716(1)(g) (LexisNexis 2020); Del. Code. Ann. tit 6 §12B-101(7) (LexisNexis 2020); Fla. Stat. Ann. §501.171(1)(g) (LexisNexis 2020); La. Rev. Stat. §1:3073(4)(a) (LexisNexis 2020); Md. Com. Law. Code Ann. §14-3501(e) (LexisNexis 2020); Vt. Stat. Ann. tit. 9 § 2430 (10) (LexisNexis 2020).

¹⁷¹⁸ See *id*; Minn. Stat. Ann. §325E.61(1)(e) (LexisNexis 2019); R.I. Gen. Laws §11-49.3-3(a)(8) (LexisNexis 2019).

1. Name (including full name)
2. Government issued numbers or other unique identifiers (social security numbers, passport numbers, motor vehicle operator's license numbers, state identification card numbers, etc.)
3. Dates pertaining to an individual (birth date, death date, military enlistment or discharge date, etc.)
4. Financial account numbers – real or virtual (any bank account numbers, credit card numbers, investment or retirement account numbers, virtual currency account numbers, etc.)
5. Any login credentials (email address, username, password or other access code such as a personal identification number (“pin” or “pin number”))
6. Biometric data (~~“hard biometrics”: DNA, vasculature scans, fingerprints, retinal scans, facial recognition data; or “soft biometrics”: 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).~~)
7. Insurance information (identification numbers, insurance policy numbers or any other unique identifying number)
8. Health information (health history, information about illnesses, information or observations about a patient, etc.)
9. 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.)
10. Physical asset information ~~of or about~~ [that consistently links an item to an individual \(MAC address, IP address, car license plate number, home address\)](#)
11. Geolocation data (data used on ride-sharing apps, augmented reality apps or games)
12. Customer loyalty or affinity account numbers
13. Physical asset or software usage data (browser history, cookies, software tokens, usage metadata, etc.)
14. 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. Advantages of the Flexible PHI Approach~~

~~The flexible approach to defining PHI encourages organizations to address the risk of breach in a proactive way. They can consider what forms of PHI 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 levels of safeguards that are appropriate to protect that PHI.~~

~~Some PHI is so sensitive in nature (such as health data) that [unauthorized access to it will usually give rise to a risk of harm sufficient to warrant notification](#). However, other PHI (such as subscription to a magazine or membership to an organization) will be sufficiently sensitive depending on the context such as the nature of the magazine or the organization [and the nature of](#)~~

~~the PII. For example, a membership list for Alcoholics Anonymous is may be sufficiently sensitive whereas, a membership list for a “dog-lovers” organization would may not be. The potential risk of harm with a breach of from unauthorized access to information relating to membership to showing the names of members of Alcoholics Anonymous is evident.~~

~~This context-specific analysis incentives organizations 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 organization’s assessment of the required safeguards.~~

45. International Trends Regarding PII

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

The GDPR 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.”¹⁸²⁰¹⁹

Likewise, the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA) uses a broad definition of PII. Under PIPEDA, personal information is defined as follows: “means information about an identifiable individual.”¹⁹²¹²⁰ 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 provided²⁰²². ~~The OPC has further stated that information will be about an “identifiable individual” where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.~~²¹

Proposed Model Language

“Personally Identifiable Information” (“PII”) means factual or subjective information, whether recorded in electronic or hard copy form or not, about, or pertaining to, or traceable to,

¹⁸²⁰¹⁹ General Data Protection Regulation, art. 4 (1), located at <https://gdpr-info.eu/art-4-gdpr/> (last visited May 24, 2019).

¹⁹²¹²⁰ S.C. 2000, c.5, §2(1).

²⁰²² 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).

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).

either alone or in combination with other information, an identifiable individual (any such individual being defined as the “PII Subject” with respect to information that is about or pertains to or is traceable to him or her).

~~“Personally Identifiable Information” (“PII”) means information about, or pertaining to, or traceable to, either alone or in combination with other information, an identifiable individual (any such individual being defined as a “PII Subject” with respect to information that is about or pertains to or is traceable to him or her).~~

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

Of all the U.S. state breach notification laws, the vast majority require some analysis by the impacted organization of the risk of harm to the individual by ~~the impacted organization~~reason of the event in question before a notification requirement is triggered.²⁴²² The ~~standards~~standard for the determination of whether there is a risk of harm ~~that requires~~sufficient to require notification varies across ~~the~~those states.

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

For most states, the statutory formulation looks to whether it is reasonable to assume that actual, tangible harm to the individual from the breach could occur. 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.²⁴²³ 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.²⁴²⁴

Other states look not at what is reasonable to assume, but at whether the breach creates a substantial or significant risk to the individual. For example, in Massachusetts, the breach must create 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.²⁴²⁵ 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.”²⁴²⁶

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 organizations may underestimate or misunderstand the potential risk of harm and inadvertently

²⁴²² 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 standing. Accordingly, this commentary refers only to “risk of harm” in the notification context.

²⁴²³ N.J. Stat. Ann. § 56:8-163(a)(LexisNexis 2019).

²⁴²⁴ N.C. Gen. Stat. § 75-61(14)(LexisNexis 2019).

²⁴²⁵ See *supra* note 15.

²⁴²⁶ Ind. Code Ann. § 24-4-9-3.1(a)(LexisNexis 2019).

default to finding that the likelihood of injury is low and therefore not be incentivized to provide notice to individuals. Under other frameworks, there is a presumption of harm (and thus a requirement to give notice) unless reasonable to conclude otherwise. Vermont, for example, has a “negative option” harm trigger which states that if a data ~~collector~~ [PII Controller](#) believes misuse of personal information is not reasonably possible, and they inform the Attorney General, they need not notify potentially affected persons.²⁶²⁷ Florida requires that the risk of harm analysis be conducted in consultation with relevant federal, state, or local law enforcement agencies.²⁷²⁸ Alaska similarly requires the giving of notice to the state Attorney General as a condition of determining that no reasonable likelihood of harm exists.²⁸²⁹

In the context of defining a breach, HIPAA covered entities assume there is a breach unless they can apply a four-factor test to determine a low probability of compromise.²⁹³⁰ If the HIPAA covered entity determines there is a low probability of compromise, there is no obligation to report to any regulator.³⁰³¹

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.³¹³²

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

The breach notification standard and the test for evaluating whether there is a low probability of compromise under HIPAA is particularly helpful in devising a framework to address some of the confusion associated with evaluating risk of harm.

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 unavailability, modification or absence of the PII materially prejudice the data subject? See discussion of what constitutes PII in Section V.B, *supra*.

ii. The Recipient of the PII

Consider the unauthorized person who accessed or acquired the PII. Certain notification statutes provide for a safe harbor for breaches that result in the unauthorized disclosure of PII to persons that may be ascertainable as not likely to be a threat to any individuals. For example, the recipient may be a current or former employee of the entity that experienced the breach who is not authorized to view the PII but remains under the direct or indirect control of the entity. Consider whether this person has legal obligations to protect the information – for example, is the person or

²⁶²⁷ Vt. Stat. Ann. tit. 9 § 2435(d)(LexisNexis 2019).

²⁷²⁸ Fla. Stat. Ann. § 501.171(4)(c)(LexisNexis 2019).

²⁸²⁹ Alaska Stat. Ann. § 45.48.101(c)(LexisNexis 2019).

²⁹³⁰ 45 CFR § 164.402(2)(LexisNexis 2019).

³⁰³¹ *Id.*

³¹³² See generally GDPR, article 35.

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

Some breaches 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. This is an important consideration because data sources can be said to have been accessed by an unauthorized person even if it is indeterminable what data within the source was actually used or viewed.

In other instances, it may be possible to determine that the PII acquired as a result of the breach has not, in fact, been viewed or used in a manner that could cause a ~~legally cognizable~~ harm. For example, 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 to be provided.

iv. Mitigation of the Risk Following Unauthorized Disclosure

Consider the extent to which the risk of harm from unauthorized disclosure of the PII has been mitigated by the entity that suffered the breach (as compared to mitigation efforts the affected individuals might employ). For example, by obtaining 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 destroyed. This factor, when applied in combination with the factor regarding the nature of the unauthorized recipient, may lead to different results in terms of the risk of harm. For example, an entity may be able to obtain and rely on the assurances of an employee, affiliated entity, or vendor that the person destroyed the information. However, such assurances from other third parties may not be sufficient.)

34. Advantages of the Flexible PII Approach Discussed in Section

The flexible approach to defining PII encourages organizations to address the risk of harm breach 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 levels of safeguards that are appropriate to protect that PII.

Some PII is so sensitive in nature (such as health data) that unauthorized access to it will usually give rise to a risk of harm sufficient to warrant notification. However, other PII (such as subscription to a magazine or membership to an organization) will be sufficiently sensitive depending on the context such as the nature of the magazine or the organization and the nature of the PII. For example, a membership list for Alcoholics Anonymous is may be sufficiently sensitive whereas, a membership list for a "dog lovers" organization would may not be. The potential risk of harm with a breach of from unauthorized access to information relating to membership to showing the names of members of Alcoholics Anonymous is evident.

This context-specific analysis incentivizes organizations 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 organization's assessment of the required safeguards.

Proposed Model Language

Any PII ~~Collector~~Controller that has experienced a Security Breach 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 legally cognizable harm to one or more of the that PII Subjects associated with the PII in question. In determining whether the Security Breach has caused or is likely to cause such ~~legally cognizable~~ harm, the PII ~~Collector~~Controller shall consider:

1. whether the PII ~~in question~~ was secured in such a way that rendered it unusable, based on generally accepted industry standards;
2. the nature and extent of the PII ~~in question~~;
3. the extent to which the integrity and availability of the PII to the PII Subject PII have been adversely affected;
- ~~4. 3-~~the identity of the person who Accessed the PII ~~in question~~ without authorization;
- ~~4. the extent to which the risk that the PII in question would be misused has been mitigated following its unauthorized Access; and~~
5. the likelihood that the PII ~~in question~~ has been or will be misused to perpetrate identity theft or attacks and/or crimes beyond identity theft resulting in ~~legally cognizable injury~~; and
6. whether the extent to which the risk that the PII in question would be misused has been mitigated following its unauthorized Access;

If a PII ~~Collector~~Controller that has experienced a Security Breach determines, after conducting the investigation required by this Section, that the Security Breach has not caused or is not likely to cause ~~legally cognizable~~ harm to one or more ~~of the~~ PII Subjects ~~associated with the PII in question~~, the PII ~~Collector~~Controller shall make and preserve a record of its investigation and findings for production to any regulator when requested.³²³³

D. 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 exfiltrated data is either not accessible to or usable by anyone

³²³³ 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.

other than its owner, or it is not reasonably 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 tangible 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

As discussed above, encryption for purposes of this commentary broadly means: “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.” 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. For purposes of this Commentary, “encrypted” means computerized data that is rendered unusable, unreadable, or indecipherable in its original format without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2.

Most state’s 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 defining that notification is required 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.³³³⁴

The data breach notification statutes of other states, like Illinois, simply remove encrypted data from the definition of “Personal Information” 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

³³³⁴ Cal. Civ. Code § 1798.29(a) (LexisNexis 2019).

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 otherwise read the data elements have been obtained through the breach of security.”)³⁴³⁵

~~However, some states have viewed this issue differently. For a period of time in 2016 Tennessee changed its data breach notification to remove the word “unencrypted” from describing the type of compromised information that would necessitate notification. This effectively required notification of unauthorized access regardless of whether the data was encrypted. In 2017, Tennessee further amended its data breach notification statute to clarify that any person or business that conducts business in Tennessee is only required to give data breach notification if the information acquired was unencrypted.³⁵~~

2. Many Existing Data Breach Laws do not Account for De-identification

Data anonymization and pseudonymization are types of information sanitization whose intent is privacy protection by de-identification. It is the process of either encrypting or removing personally identifiable information 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. 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 personally identifiable information 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~~[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 ~~that~~ the data could be compromised.

~~E. What Methods of Notification should be Permissible?~~

Proposed Model Language

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

³⁴³⁵ 105 ILCS §530/5 (LexisNexis 2019).

³⁵ See Tenn. Code Ann. §47-18-2107(a)(1)(LexisNexis 2019)(defining a “breach of system security” to include either unencrypted computerized data, or encrypted computerized data along with the encryption key).

individual or household. For example, a Security Breach has not occurred if (i) the PII is Encrypted or De-identified; and (ii) the Encryption key and/or re-identification key has not been acquired by the unauthorized; and (iii) the PII is not otherwise likely capable of de-anonymization, de-pseudonymization, or re-identification by an unauthorized person.

E. 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) if the company does not have 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, generally requiring, 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;³⁶ 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;³⁷ or
- Email notice, if a prior business relationship exists and the person or entity has a valid email address for the individual.³⁸

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. ~~In addition~~ Most state laws have substitute notice provisions, which should provide a cheaper alternative to written U.S. mail notice. However, the substitute notice provisions in most state law statutes, though they vary, are available are often triggered by consumer numbers or cost ~~number~~ levels so high that they are not accessible for to most

³⁶ See, e.g. Conn. Gen. Stat. § 35a-701b(e)(LexisNexis 2019); Miss. Code Ann. § 75-25-29(6)(LexisNexis 2019); Mo. Rev. Stat. § 407.1500(2)(6)(b)(LexisNexis 2019).

³⁷ Vt. Code. Ann. tit 9 § 2435(b)(6)(A)(ii)(II)(LexisNexis 2019).

³⁸ Ala. Code Ann. § 8-38-5(d)(LexisNexis 2019).

~~organizations that might need them. Each state having their own triggers also may be problematic for companies operating in one more than one state. In addition, though the substitute notice provisions may, in some cases, be more streamlined and less costly, the added requirement in many state statutes for~~ 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 ~~can also be a costly factor for small and mid-size organizations.~~ Since data breach will likely affect most organizations 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 broader goal of data breach notification, which is to alert consumers 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 so that they can act to protect ~~secure, and monitor their own PII themselves against whatever harm they are at risk of suffering by reason of the event in question.~~ As such, a model method of notification should be simple and low-cost, which will allow organizations to accomplish this task quickly.

To that end, organizations should be able to provide notice through traditional U.S. mail or email, if the organization already communicates with the consumer 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. Virtually all organizations will have current email addresses of their customers. If organizations already communicate with their consumers 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.

If an Organization does not have access to the U.S. mail or email of each PII Subject, the Organization shall post for at least 60 days on the Organization's website if the Organization 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.

4. Who Should Send Notice?

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 caused or is likely to cause legally cognizable 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

Commented [U2]: In drafting this, I'm assuming PII Collector means whoever is collecting the information, and PII Collector, per our definition, could include Service Provider.

party to provide such notice. It is common for organizations to share information related to PII Subjects with service providers and other 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”³⁹ 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) functions the service provider or contract partner performs on behalf of the entity; and (2) which entity has the relationship with the individual.⁴⁰ Parties should take steps to ensure that the individual does not receive notifications from both the organization and the service provider about the same breach, which may create confusion.⁴¹ 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.

Proposed Model Language

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

Commented [U3]: In drafting this, I’m assuming PII Collector means whoever is collecting the information, and PII Collector, per our definition, could include Service Provider.

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 ~~Collector~~Controller that experienced the Security Breach or by another party that has an agreement with the PII ~~Collector~~Controller that obliges the party to provide such notice. The PII ~~Collector~~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. Organizations may 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.

Proposed Model Notice

³⁹ <https://www.federalregister.gov/documents/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the>.

⁴⁰ *Id.*

⁴¹ *Id.*

The notices, whether provided on paper or electronically should contain the following information (modeled off the California sample notice available on the California Attorney General website):⁴²

1. Title “NOTICE OF DATA BREACH” in all capital letters
2. Salutation: “Dear [First and Last Name of Individual]:”
3. Introductory Statement:
 - a. Brief statement of why the notice is being sent to the PII Subject in question.
 - 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 ~~Collector~~Controller in question].”
4. What Happened?
 - a. Brief description of the Security Breach that triggered the notification
 - b. Date of Security Breach discovery and, if known, date range during which the Security Breach occurred
5. What Information Was Involved?
 - a. Description of the PII in question
6. What Are We Doing About It?
 - a. General description of any actions taken by the PII ~~Collector~~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
7. What Can You Do?
 - a. General description of/recommendations for what the PII Subject can do to further protect himself/herself from whatever ~~legally cognizable~~ harm the PII ~~Collector~~Controller has determined the Security Breach has 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
 - iii. Provide contact information for State Attorney General/Consumer Protection Agency
8. Where required by Paragraph G, include offer of services called for by Paragraph G.
9. 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.

⁴² <https://oag.ca.gov/privacy/databreach/list> (last visited May 28, 2019).

EF. ~~What should be the timeline for notification~~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 organization, 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.

Several factors⁴³ contribute to the amount of harm affected individuals ~~suffer~~ may suffer from a security breach, including, (a) whether the underlying security breach is ongoing, (b) what steps the organization 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. Reducing harm through each of these factors reveals a tension between the time since the breach and information about the security breach. On the one hand, with the right information about the security breach, the organization and affected individuals can respond precisely and thoroughly to the specific threat. On the other hand, gathering all the relevant information about the security breach takes time, and during that time, affected individuals could suffer increasing harm. The more harm individuals suffer the more likely an organization could be liable 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 organization may not have had time to determine whether the security breach is still ongoing. On the other end of the time spectrum, 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 organization) may be provide to notifications as soon as the breach is discovered. For example, if a rogue employee gained

⁴³ 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.

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,⁴⁴ the individual's and organization'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 organization 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 organization to incur liability. This timing of notification standard generally leaves the courts in the best position to quantify harms and apportion liability. Some states with this timing standard include California,⁴⁵ New York,⁴⁶ Texas,⁴⁷ and Illinois.⁴⁸

It appears that without a set deadline, many organizations argue that as long as a good faith investigation into the breach is ongoing such organizations do not need to provide notice to affected individuals. ~~It is important to note that organization in states with this notification standard often wait several months to provide notifications affected individuals.~~ Though this approach might match the letter of the law, it defeats the spirit of the law that aims to help consumers 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 set 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 any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system."⁴⁹

Like approach (i), the specific facts of a security breach can generally dictate whether speed or information about the breach should be prioritized in the notification to affected individuals. Assuming the organization 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

⁴⁴ <http://heartbleed.com/>

⁴⁵ Cal. Civ. Code § 1798.29(a)(LexisNexis 2019).

⁴⁶ N.Y. Gen. Bus. Law § 899-aa(2)(LexisNexis 2019).

⁴⁷ Tex. Bus. Com. Code § 521.053(b)(LexisNexis 2019).

⁴⁸ Ill. Comp. Stat. Ann. ch. 815 §530/10(a)(LexisNexis 2019).

⁴⁹ Colo. Rev. Stat. Ann. § 6-1-716(2)(LexisNexis 2019).

individuals would be diminished. The deadline for notice under such circumstances could appear arbitrary.

If an organization does not work diligently in response to a security breach, the deadline could act as a “safe harbor.” Organizations 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 organization might not be held liable because it met the statutory deadline.

~~Nonetheless, the greater harm is likely suffered when individuals do not receive timely notice of the breach. Providing some notice appears to be better than providing delayed notice.~~ This approach sets a standard for what constitutes timely notice. Therefore, it takes an important step in protecting affected individuals, even if organizations suffering a breach have to operate with incomplete information at the time of the notification.

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 organizations 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. Organizations working diligently in response to a breach will work provide the right information to affected individuals as quickly as possible. However, like approach (ii), when organizations 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 deadline⁵⁰.

Unlike approach (ii), this timing of notification standard does not require organizations to provide notifications without unreasonable delay (or as quickly as possible). By setting a hard deadline, though, organizations 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, organizations have no disincentive to provide notifications anytime sooner than the deadline.

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

⁵⁰ S.D. Stat. Ann § 22-40-20 (LexisNexis 2019).

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 organizations.

Proposed Model Language

~~With these considerations in mind, these guidelines recommend timing of security breach notifications that reads as follows:~~

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 ~~Collector~~ Controller in question first learned of the Security Breach, unless good cause exists to delay providing such notice.⁵¹

F. 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.”⁵² 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.”⁵³ The timing of the alerts received in connection with credit monitoring is problematic as well. A consumer 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.”⁵⁴

1. Credit Monitoring and State Breach Notification Laws

Despite some of the inherent weaknesses with credit monitoring four states [\(see discussion on page 33\)](#) 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

⁵¹ 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.

⁵² *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).

⁵³ *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>.

⁵⁴ *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.).

exposed PII defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).⁵⁵

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, as defined in Section 1798.90.5.

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.⁵⁶

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.⁵⁷

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

⁵⁵ Cal Civ. Code § 1798.82(d)(2)(G)(LexisNexis 2019).

⁵⁶ 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>.

⁵⁷ Conn. Gen Stat. §36a-701b(b)(2)(LexisNexis 2019).

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.⁵⁸

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.⁵⁹

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.⁶⁰ 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 letters to creditors and debt collectors to dispute unauthorized charges and close accounts, “place a freeze on your credit report to prevent an identity thief from opening new accounts in your name, or guide you through documents you have to review.”⁶¹ Some services will represent you in dealing with creditors or other institutions if you formally grant them authority to act on your behalf.⁶² Others may help you place fraud alerts with the consumer reporting agencies and government agencies. Given the amount of time and effort individuals can spend in addressing issues associated with fraudulent use of name,⁶³ Social Security number and account information on their own this type of service can be extremely valuable to an individual impacted by a breach. 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.

Consumers who have been the victim of a data breach may realize some small benefit from credit monitoring in certain limited circumstances will realize significantly enhanced benefits from having 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.

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

⁵⁸ Del. Code. Ann. § 12B-102(e)(LexisNexis 2019).

⁵⁹ Mass. Gen. Laws Ann. ch 93H § 3A(a)(LexisNexis 2019).

⁶⁰ <https://www.businesswire.com/news/home/20151006006149/en/Latest-Data-Breach-Spotlights-Identity-Restoration>.

⁶¹ *Id.*

⁶² *See id.*

⁶³ “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>).

pages on the Dark Web for Social Security number, email, phone number or medical information. Because Dark Web scans are only “a point in time” regular scans are essential for this service to be effective.

Proposed Model Language

Where an obligation exists under Paragraph D to provide notice of a Security Breach ~~to a PII Subject~~, 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 or use of 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 ~~be limited to, services that include the following~~: (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; and (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.

G. How Should Organizations 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, they require notice to different governmental entities, and 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 Thirty-five~~ states and Puerto Rico require notice to some governmental entity.⁶⁴ ~~At least thirty~~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.

⁶⁴ Data Breach Charts, Baker & Hostetler LLP, July 2018, available at www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf.

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

1. *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;
2. *250 or more individuals affected* – North Dakota, Ohio, Oregon, Texas, South Dakota (Illinois, if a breach by a state agency occurs)
3. *500 or more individuals affected* – California, Colorado, Delaware, Florida, Illinois, Iowa, Rhode Island, Washington;
4. *1000 or more individuals affected* – Alabama, Arizona, Hawaii, Missouri, New Mexico, South Carolina, Virginia.

Notification time thresholds also vary:

1. *24 hours* – Idaho (if a public agency experiences a data breach);
2. *10 days* – Louisiana, Puerto Rico;
3. *15 business days* – California (if medical information involved);
4. *30 days* – Colorado;
5. *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 that any criminal law enforcement agencies be notified at all. 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, ~~New Jersey~~, requires notification to the state police⁶⁵, the lion's share of cybercriminal investigations and prosecutions are 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.

⁶⁵ N.J. Stat. Ann. § 56:6-163(LexisNexis 2019).

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.

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 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 the purpose of requiring such notifications, especially on such a swift time horizon. There may be little benefit to requiring an organization to notify a regulator or civil enforcement authority before an organization 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 organization has an appropriate handle on the scope of the problem. Given the limited ability of regulatory and civil enforcement authorities to affirmatively assist an organization impacted by a data security incident, it may be more useful to provide an organization 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 inundating a governmental authority with new information every time a forensic investigator uncovered a previously unknown fact, especially where a risk-averse organization 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 is a pervasive problem for organizations 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).

Proposed Model Language

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.⁶⁶

⁶⁶ These governmental entities should include criminal law enforcement agencies including the Federal Bureau of Investigation. To ensure that concerns about waiving any attorney-client privilege or work product protections associated with a victim company’s forensic investigation do not chill the sharing of information with law enforcement agencies, policymakers should also refer to the proposals identified in “The Sedona Conference Working Group Series: Commentary on Application of Attorney-Client Privilege and Work Protection to Documents and Communications Generated in the Cybersecurity Context,”. Nov. 2019, at https://thesedonaconference.org/publication/Commentary_on_Application_of_Attorney-Client_Privilege_and_Work-Product_Protection_to_Documents_and_Communications_Generated_in_the_Cybersecurity_Context