

# The Sedona Conference Draft Commentary on Proposed Model Data Breach Notification Law (Proposed Model Language Excerpted) (June 2019)



Copyright 2019, The Sedona Conference.  
All rights reserved.

# **The Sedona Conference**

## **WG11 Draft Commentary on Proposed Model Data Breach Notification Law**

### **Proposed Model Language**

#### **A. Definition of a Data Security Breach?**

“Security Breach” means unauthorized access to data or a reasonable belief of an unauthorized access to unencrypted data that compromises the security, confidentiality, or integrity of an individual’s PII maintained by the PII Collector.

1. “PII Collector” means any for-profit or non-profit entity, or government entity, that collects data about or related to an identifiable natural person.
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.
3. Good faith access of PII by an employee or agent of the person or business or organization for the purposes of the person or business or organization is not a security breach, provided that the PII is not used or subject to further unauthorized disclosure.

In determining whether PII has been accessed or misused or is reasonably believed to have been accessed or misused by a person without valid authorization, a PII Collector may consider the following factors, among others:

1. indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information provided the device is not encrypted, there is PII on the device, and the device was not remotely deactivated or wiped pursuant to the entity’s data loss procedures;
2. indications that the information has been downloaded, copied or queried or searched without authorization;
3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported;
4. that the information has been made public (e.g., provided to media, available on the Dark Web) and it is reasonable to conclude that the source of the data is the breached organization;
5. 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
6. when the entity has a good faith belief that the unauthorized person who received the PII would not have been able to retain it (e.g., PII sent in the mail and returned by recipient or post office unopened could not have been accessed).

Security Breach does not include an acquisition of PII where PII Collector determines that misuse of the PII is not reasonably possible, the PII Collector provides notice of this determination in the most expedient manner possible to the appropriate regulator, and the regulator agrees with the determination.<sup>1</sup>

## **B. Meaning of PII**

Personally Identifiable Information (“PII”) is information about an identifiable individual.

## **C. Risk of Harm Analysis**

In determining, after a prompt and good faith investigation, whether a data breach presents a substantial likelihood of material harm to data or individuals, an entity should consider: (i) the nature and extent of the PII involved; (ii) the recipient of the PII; (iii) whether the PII was actually acquired, used or viewed; (iv) the extent to which the risk that the PII was compromised has been mitigated following its unauthorized disclosure; (v) whether the PII is likely to or could be used to perpetuate further attacks and or crimes beyond identity theft; (vi) whether the PII was secured in such a way that it is rendered unusable, based on generally accepted industry standards; and (vii) whether the data breach causes or is likely to cause bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, investigative effects on credit, and damage to or loss of property.

## **D. Safe Harbors from Notification**

Access to or the acquisition of PII ordinarily does not constitute a data breach or give rise to a substantial likelihood of tangible harm to individuals if the PII has been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of an effective technology or methodology. For example, if (i) the PII is encrypted, anonymized or pseudonymized; and (ii) the encryption key and/or pseudonymization 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 de-anonymization or de-pseudonymization by an unauthorized person.

---

<sup>1</sup> The Drafting Team notes that there is disagreement regarding the need to consult with regulators in this situation and seeks input from WG 11 on the most effective approach.

## **E. Methods of Notification**

Notices to affected individuals should be provided primarily using e-mail. Virtually all organizations will have current e-mail addresses of the individuals whose PII may have been breached. E-mail is the primary mode of communication for most individuals today, and one that most individuals can be relied upon to check regularly. In cases where an organization does not have an e-mail address but a U.S. mailing address, written notice through U.S. Mail should be the substitute form of notification. Organizations should also be given the opportunity to 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.

## **F. Timeline for notification**

Reporting to government and notification to impacted individuals must be made without unreasonable delay and in the most expedient time possible but not later than 60 days after becoming aware of the breach.<sup>2</sup>

## **G. Credit Monitoring**

If the person or organization providing the notification was the source of the breach, an offer to provide credit monitoring in combination with appropriate identity theft prevention and mitigation/restoration services, shall be provided at no cost to the affected person for not less than 24 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 exposed the individual's Social Security number, driver's license number, or state or federal identification (e.g., passport, etc.). Identity theft mitigation and restoration services include, but are not limited to, 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 with placing a freeze on your credit report to prevent an identity thief from opening new accounts in your name and guiding through necessary forms.

---

<sup>2</sup> 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.

## **H. Notification to Law Enforcement and Regulatory Authorities**

In breaches where notice is provided to residents of more than one state, breaches shall be reported via centralized reporting through [insert website]. Notifications will be processed and forwarded to the appropriate law enforcement agency in each impacted state as well as the FBI and Secret Service. Any disclosures to law enforcement agencies, through the the website or otherwise, shall not constitute a breach of the attorney-client privilege or attorney work-product protection.

## APPENDIX

### **Proposed Model Notice**

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):<sup>3</sup>

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 letter is being sent to the individual
  - b. “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 data subject and organization that experienced the breach]”
4. What Happened?
  - a. Brief description of the data security incident that triggered the giving of notification
  - b. Date of breach discovery and date range of breach
5. What Information Was Involved?
  - a. Description of the PII or other protected information that was compromised
6. What Are We Doing About It?
  - a. General description of actions taken to restore security and confidentiality of covered information
  - 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 individual can do to further protect themselves from identity theft (monitor accounts, contact credit bureaus, place fraud alert on accounts)
  - b. Provide contact information for three major credit bureaus, and statement of right to free credit report
  - c. Provide contact information for FTC
  - d. Provide contact information for State Attorney General/Consumer Protection Agency
8. Next Step of Identity Protection: Availability of Free Credit Monitoring/Identity Restoration service (2 year standard)
9. For More Information: Provide contact information for point person at organization giving notice to respond to and questions or concerns that affected individuals can use to inquire about breach

---

<sup>3</sup> <https://oag.ca.gov/privacy/databreach/list> (last visited May 28, 2019).