State of California

Department of Technology

Requirements to Respond to Incidents Involving a Breach of Personal Information

Statewide Information Management Manual – 5340-C

August 2025

Table of Contents

Document History 3

I. Executive Summary 5

II. Introduction 6

III. Information Practices Act Requirements 6

A. Background 6

B. Breach Notification Requirement 7

IV. State Policy Requirements 10

A. Information Processing Standards 10

B. Incident Management 11

V. Essential Elements to Consider 15

A. Whether Breach Notification Is Required by Law 15

B. Whether Breach Notification Is Required by State Policy 19

C. Timeliness of the Notification 21

D. Source of the Notification 22

E. Format of the Notification 22

F. Content of the Notification 23

G. Approval of the Notification 25

H. Method(s) of Notification 26

I. Preparation for Follow-on Inquiries from Noticed Individuals 28

J. Other Situations When Breach Notification Should Be considered 29

K. Other Actions Agencies Can Take to Mitigate Harm to Individuals 34

L. Other Considerations When State Employee Data Is Involved 34

I. Other Considerations 34

A. Advance Notification to the Media 34

B. Credit Monitoring Services 35

II. Notifying Others When Required 36
A. Notifying the Attorney General 36
B. Notifying Credit Reporting Agencies 36
III. Questions 37
IV. Appendices 37
Appendix A: Breach Response and Notification Assessment Checklist 39
Appendix B: Sample Breach Notice: Social Security Number 52
Appendix C: Sample Breach Notice – Unique Identification Number* 53
Appendix D: Sample Breach Notice - Credit Card or Financial Account Number 54
Appendix E: Sample Breach Notice - Medical Information Only 55
Appendix F: Sample Breach Notice - Health Insurance Information Only 56
Appendix G: Sample Breach Notice – Unique Biometric Data 57
Appendix H: Sample Breach Notice – Hybrid (SSN and Health Information) 58
Appendix I: Sample Breach Notice – Automated License Plate Recognition System 59
Appendix J: Sample Breach Notice – Genetic Data 60
Appendix K: Sample Breach Notice – Username or E-Mail Address 61
Appendix L: Office of the Attorney General Data Breach Help 62

Document History

Revision	Date of Release	Owner	Summary of Changes
Initial Release		California Office of Information Security (CISO)	
Minor Update	May 2012	CISO	Added Attorney General requirements pursuant to Civil Code Section 1798.29€ effective 1/2012.
Minor Update	December 2012	CISO	Name change to shortened document title, added additional examples under section *A. Whether Breach Notification Is Required by Law,* and replaced reference to contacting California Office of Privacy Protection for assistance with use of Credit Monitoring Services with reference to published guidance.
Minor Update	September 2013	CISO	SIMM number change, replaced reference to California Office of Privacy Protection in the Sample Breach Notices.
Minor Update	January 2014	CISO	Added new notice triggering data elements and notification requirements to coincide with enacted Legislation.
Update	January 2016	CISO	Added new notice triggering data elements and notification requirements to coincide with enacted Legislation (Civil Code Sections 1798.29, 1798.82).
Minor Update	April 2016	CISO	Non-substantial change to breach notification templates clarifying signature requirements per SAM 5300.3 and adding hyperlink to Breach Help pages.
Minor Update	June 2016	CISO	Update incident reporting instructions for the SIMM 5340-B: eliminating incident reporting through ENTAC; directing all incident reports to be made through the Cal-CSIRS system.

Revision	Date of Release	Owner	Summary of Changes
Update	March 2017	CISO	Added reporting/notification requirements to include breach of encrypted personal information to coincide with enacted Legislation (Civil Code Section 1798.29).
Minor Update	January 2018	Office of Information Security (OIS)	Office name change
Update	February 2020	Office of Information Security (OIS)	Added new notice triggering data elements and notification requirements to coincide with enacted Legislation (Civil Code Sections 1798.29 and 1798.82).
Update	June 2022	Office of Information Security (OIS)	Add new notice triggering data elements and notification requirements to coincide with enacted Legislation (Civil Code Sections 1798.29, 1798.81.5 and 1798.82).
Minor Update	March 2025	Office of Information Security (OIS)	Updated to new template and updated references from FIPS 140-2 to FIPS 140-3. Minor formatting and grammar revisions.
Minor Update	August 2025	Office of Information Security (OIS)	Minor changes to align templates and requirements.

I. Executive Summary

Agencies/state entities are required to operate in accordance with a myriad of laws and state policies related to the protection of information assets, and the timely and efficient management of security incidents. California's breach notification law (Civil Code Section 1798.29), enacted in 2002, is one such law, intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so they could take steps to protect themselves against identity theft or to otherwise mitigate the crime's impact and other possible harms associated with a breach of personal information.

While the law originally focused on breaches involving the kind of information used in financial identity theft, growing concern about medical identity theft led to the addition of medical and health insurance information as "notice-triggering" in 2008. In 2015 the addition of a username or e-mail address, in combination with a password or security question that would permit access to an online account, was added to the list. In 2016, encrypted personal information acquired by an unauthorized person with access to the encryption key or security credential and the Automated License Plate Recognition System were added as "notice- triggering" elements. In 2020, unique biometric data and tax identification numbers, passport numbers, military identification numbers, and any other unique identification numbers issued on a government document were added as "notice- triggering" elements, and in 2021 legislation added genetic data.

Safeguarding against and preventing security breaches involving personal information entrusted to government is essential to establishing and maintaining public trust. Equally important is the ability to provide accurate and timely information about a breach to affected individuals when a breach occurs because failure to do so can exacerbate the problem and increase the risk of harm to individuals.

To ensure that agencies/state entities understand the responsibilities for making timely and accurate notification to individuals affected by a breach, this SIMM 5340-C document identifies the existing personal information breach notification requirements and sets out specific instructions and guidance for agencies/state entities to follow when responding to a security incident that involves a breach of personal information. This document also

provides a checklist and a set of breach notification templates as tools to assist agencies/state entities with fulfilling the notification requirements.

II. Introduction

To ensure compliance and consistency across state government, this document identifies the current breach notification requirements for breaches involving personal information, accompanied by questions and factors agencies/state entities should consider in determining whether and when a breach notification should be made, and a specification of the means for fulfilling notification requirements. This document does not attempt to establish an absolute standard for breach notification, since decisions are dependent upon the specific facts surrounding the breach and the applicable law. In some cases, notification is clearly required by law, and in others it may be unclear whether notification is required. In some instances, where notification is, by law, clearly not required, notification may nonetheless, serve the best interests of those affected.

The procedures discussed in this document will assist agencies/state entities in confronting the problems associated with a breach involving personal information, by providing instruction and guidance regarding developing an appropriate response, understanding notification requirements, and making decisions in cases where the obligation to notify may be uncertain.

The term “agency” refers to any office, department, board, bureau, commission or other organizational entity within state government. Within this document, “agency” and “department” are used interchangeably.

III. Information Practices Act Requirements

A. Background

The California Information Practices Act (IPA) of 1977 (Civil Code Sections 1798 et seq.) is the primary authority that governs state agencies’ collection, use, maintenance, and dissemination of individuals’ personal information. The IPA also specifies the circumstances that compel breach notification.

For the general purposes of the IPA, Civil Code Section 1798.3 defines personal information very broadly as "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, Social Security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual."

B. Breach Notification Requirement

Subdivision (a) of Civil Code Section 1798.29, requires "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 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 usable". For purposes of this section, encrypted has been defined as "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security". For purposes of this section, "encryption key" and "security credential" mean the confidential key or process designed to render the data usable, readable, and decipherable.

The breach notification section of the IPA, subdivision (g) of Civil Code Section 1798.29, more narrowly defines, "personal information" as the following:

1. An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
    a. Social Security number.

b. Driver's License number, California Identification Card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

c. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

d. Medical information (as defined in Civil Code Section 1798.29).

e. Health insurance information (as defined in Civil Code Section 1798.29).

f. Unique biometric data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

g. Automated License Plate Recognition (ALPR) System Information (as defined in Civil Code Section 1798.90.5).

h. Genetic data

2. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Subdivisions (h) (1) through (3) of Civil Code Section 1798.29 specifically define personal information, medical information, and health information for purposes of this section as follows:

1. For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Note; however, personal information held in public records, or portions thereof, may need to be redacted prior to disclosure to comply with Civil Code Section 1798.24).

2. For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

3. For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

4. For purposes of this section, “encrypted” means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

5. For purposes of this section, “genetic data” means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

Subdivisions (b) and (d) of Civil Code Section 1798.90.5 specifically defines the ALPR System and the information received through the use of the ALPR Systems as follows:

1. ALPR system means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.

2. ALPR information means information or data collected using an ALPR system.

For purposes of this document the elements of personal information described in subdivisions (e) and (f) of Civil Code Section 1798.29 are hereinafter referred to as "notice-triggering" data elements.

Effective January 1, 2016, Civil Code Section 1798.29 subsections (1) (A through E), specified formatting requirements for the breach notification letters and subsections (2) (A through F) specified content requirements.

Further, effective January 1, 2012, Civil Code Section 1798.29 (e), requires any agency that is required to issue a security breach notification to more than 500 California residents as a result of a single breach to electronically submit a sample copy of the breach notification, excluding any personally identifiable information, to the Attorney General. The Attorney General's procedures for sample submission are available on its website at: http://oag.ca.gov/ecrime/databreach/reporting

IV. State Policy Requirements

A. Information Processing Standards

State policy, in accordance with State Administrative Manual (SAM) Section 5100, requires agencies/state entities to use the American National Standards Institute (ANSI) management information standards and the Federal Information Processing Standards (FIPS) in their information management planning and operations. The ANSI standards are national consensus standards that provide guidance on a variety of issues central to the public and industrial sectors. Under the Information Technology Management Reform

Act (Public Law 104-106). The Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) as FIPS for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

In relation to Civil Code Section 1798.29's exemption from the breach notification requirement for a breaches involving encrypted notice-triggering information, this requirement, includes without limitation, those NIST standards related to the validation of

cryptographic modules found in **encryption products used in the protection of confidential, personal, or sensitive information.** The exemption is only applicable to those incidents involving data encrypted with products validated by NIST as FIPS 140-3 compliant.

B. Incident Management

State policy (SAM Section 5340) requires agency management to promptly investigate incidents involving loss, damage, misuse of information assets, unauthorized access, or improper dissemination of information, and immediately report the occurrence of such incidents to the Office of Information Security (OIS) and the California Highway Patrol (CHP), through the California Compliance and Security Incidents Reporting System (Cal-CSIRS). Incident reporting instructions can be found in the Incident Reporting and Response Instructions (SIMM 5340-A).

Proper incident management includes the formulation and adoption of an incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents. In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences.

In conjunction with the aforementioned requirements, SIMM 5340-A requires every state agency that collects, uses, or maintains personal information to include in their incident management plan, procedures for responding to a security breach involving personal information **regardless of the medium in which the breached information is held** (e.g., paper, electronic, oral, or the combination of data elements involved including non-notice-triggering personal information). These procedures must be documented and must address, at a minimum, the following:

1. Agency Incident Response Team: An agency's procedures shall identify the positions responsible for responding to a security breach involving personal information. An agency's response team must include, at a minimum, the following:

- An escalation manager
- The Program Manager of the program or office experiencing the breach
- The Information Security Officer (ISO)
- The Chief Privacy Officer/Coordinator (CPO) or Senior Official for Privacy
- The Public Information or Communications Officer
- Legal Counsel
- Others as directed by OIS

The escalation manager, often the ISO or CPO, is responsible for ensuring appropriate representatives from across the organization are involved and are driving the process to completion. Some incidents will require the involvement of other persons not mentioned above. For example, if the source of the compromised information was a computer system or database, the Chief Information Officer should also be involved in the response activity. As another example, if the incident involves unauthorized access, misuse, or other inappropriate behavior by a state employee, or the security breach involves a compromise of state employee's personal information, the Personnel Officer or Human Resources Manager should also be involved in the response activity.

Further, if the incident involves multiple agencies/state entities, the response team from each agency/state entity may be involved.

2. Protocol for Escalation, Internal Reporting, and Response: An agency's procedures shall outline the method, manner, and progression of internal reporting, so as to ensure that the agency's executive management is informed about the breach of personal information, the Agency Incident Response Team is assembled, and the incident is addressed in the most expeditious and efficient manner.

An initial impact assessment and response coordination meeting, attended by all response team personnel, is highly recommended when a security incident involves notifying a large number of individuals, involves multiple agencies/state agencies, or is likely to garner media attention. This meeting clarifies roles, responsibilities, and timelines for incident reporting and response activities.

When multiple agency personnel are involved; attendee and sign-in rosters are used to track participant involvement. Non-disclosure agreements may also be used to ensure confidential information remains confidential and communications do not compromise or complicate an active investigation.

3. Protocol for Security Incident Reporting: Any actual or suspected incident meeting the criteria described earlier or breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is to be reported immediately to OIS and CHP through Cal-CSIRS. Representatives from the OIS and/or CHP's Computer Crime Investigation Unit (CCIU) will contact the state entity as soon as possible following their receipt of the Cal-CSIRS notification.
   IMPORTANT: A report made to CHP, other law enforcement agencies, or the OIS outside of the Cal-CSIRS notification process by email or other means is NOT an acceptable substitute for the required report through Cal- CSIRS.

   In the case that the Cal-CSIRS system is offline during normal business hours, contact OIS directly by phone at (916)-245-2583or by e-mail at security@state.ca.gov for assistance. If the Cal-CSIRS system is offline outside of normal business hours and you require immediate law enforcement assistance, contact CHP's Emergency Notification and Tactical Alert Center (ENTAC) at (916) 843-4199. This telephone number is staffed 24-hours a day, seven days a week. The officers at ENTAC will forward that information to CCIU for immediate assistance. In the situation that notification is made outside of normal business hours through CHP, it is the state entity's responsibility to notify OIS of incident the next business day.

A state entity report must outline the details of the incident and corrective actions taken, or to be taken, to address the root cause of the incident. The report must be completed through Cal-CSIRS within 10 business days following creation of the incident. If corrective actions cannot be completed immediately, follow the instructions outlined in Risk Register and Plan of Action and Milestones Instructions (SIMM 5305-B) to submit a Risk Register and Plan of Actions and Milestones (SIMM 5305-C) that identifies all corrective actions along with timelines indicating when these corrective actions will be completed. If the agency/state entity currently has a RRPOAM on file, they will need to update the existing RRPOAM and resubmit.

4. Decision-Making Criteria and Protocol for Notifying Individuals.

   Both the decision to provide external notification on the occasion of a breach and the nature of the notification will require agencies/state entities to resolve a number of questions. An agency's/state entity's procedures shall include documentation of the methods and manner for determining when and how notification is to be made.

   To assist agencies with navigating the decision-making process, a checklist is provided as Appendix A, Breach Response and Notification Assessment Checklist. The procedures shall, at a minimum, address the following elements:

   a. Whether the notification is required by law.
   b. Whether the notification is required by state policy.
   c. Timeliness of notification.
   d. Source of notice.
   e. Content of notice.
   f. Approval of notice prior to release.
   g. Method(s) of notification.
   h. Preparation for follow-on inquiries.

i. Other actions that agencies/state entities can take to mitigate harm to individuals.

j. Other situations when notification should be considered.

A more detailed description of these elements is set forth in the following section.

V. Essential Elements to Consider

A. Whether Breach Notification Is Required by Law

California's Breach Notification Law (Civil Code Section 1798.29) requires "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 usable".

The law is intended to give individuals early warning when their personal information is reasonably believed to have been acquired by an unauthorized person, so that those individuals can take steps to protect themselves against identity theft or to otherwise mitigate the crime's impact. While the law originally focused on breaches involving the kind of information used in financial identity theft, growing concern about medical identity theft led, in 2008, to the addition of medical and health insurance information as notice- triggering information. In 2015 the addition of a username or e-mail address, in combination with a password or security question that would permit access to an online account, was also added to the list. In 2016, the Automated License Plate Recognition (ALPR) System was determined to have the ability to store personal identifiable

information and was added as a “notice-triggering” element. Most recently, unique biometric data and tax identification numbers, passport numbers, military identification numbers, and any other unique identification numbers issued on a government document were added as “notice-triggering” elements.

To determine whether notification of a breach is required by law, the agency should consult with their legal counsel. Note, other sector specific laws and regulations may also require notification, such as laws governing Federal Tax Information (FTI), and the Health Information Portability and Accountability Act (HIPAA). Answering the following questions should assist the agency and its legal counsel in making the determination as it relates to Civil Code Section 1798.29:

1. Was computerized data owned or licensed by the state agency involved?

   When determining whether or not the incident involved computerized data, the agency is to consider, at a minimum, whether the data involved was processed or stored with or in a computer or computer system. This includes, but is not limited to, copier, facsimile and business hub machines, mobile telephone and Portable Digital Assistant (PDA) devices, data processed or stored with or in electronic mail systems, online accounts, and data collected through an ALPR system.

2. Was a computer system, or computer peripheral, or storage device with the capability of storing computerized data owned or licensed by the state agency involved?

   When determining whether or not the incident involved a computer system, or computer peripheral, or storage device with capability of storing computerized data the agency is to consider the wide array of data storage devices available today.

   This includes, but is not limited to, those mentioned above, as well as USB flash, jump or pen drives, CDs and DVDs, external and removable hard drives, and magnetic and optical backup tapes/disks.

3. Were notice-triggering data elements involved?
    a. In accordance with Civil Code Section 1798.29, notice triggering data elements include an individual's first name or first initial and the individual's last name in combination with any one or more of the following:
        i. Social Security number.
        ii. Driver's License number, California Identification Card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
        iii. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
        iv. Medical information (as defined in Civil Code Section 1798.29).
        v. Health insurance information (as defined in Civil Code Section 1798.29).
        vi. Unique biometric data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
        vii. ALPR System information (as defined in Civil Code Section 1798.90.5).
        viii. Genetic data.
    b. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

4. Were the notice-triggering data elements encrypted using FIPS 140-3 validated or NIST certified cryptographic modules?

3. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standards (FIPS 140-3 and others). An alphabetical list of vendors who have implemented NIST validated cryptographic modules list is available on NIST's CMVP website at http://csrc.nist.gov/groups/STM/cmvp/validation.html

   FIPS 140-3 precludes the use of invalidated cryptography **for the cryptographic protection** of sensitive or valuable data. Invalidated cryptography is viewed by NIST as providing **no protection** to the information or data - in effect the data would be considered unprotected plaintext.

5. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person?

   When determining whether or not acquisition has actually or is reasonably believed to have occurred, an agency is to consider, at a minimum, the following indicators:

   a. The information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other devices that have the capability of containing information, or such as a misdirected electronic mail transmission received and opened by an unauthorized person containing notice-triggering information.

   b. The information has been downloaded or copied (e.g., any evidence that download or copy activity has occurred which may require forensic analysis).

   c. The attacker deleted security logs or otherwise "covered their tracks."

   d. The duration of exposure in relation to maintenance of system logs or in cases of an inadvertent or unauthorized Web site posting.

e. The attack vector is known for seeking and collecting personal information.

f. The information was used by an unauthorized person, such as instances of identity theft reported or fraudulent accounts opened.

B. Whether Breach Notification Is Required by State Policy

The compromise of notice-triggering data elements found in physical information systems poses the same level of risk to individuals as a compromise of notice-triggering data elements found in computerized systems; thus, state policy requires notification be made to individuals in these cases, as well. To determine whether notification is required by state policy, the agency should still consult with its legal counsel. However, answering the following questions, which are a slight variation to those above, should assist the agency and its legal counsel in making this determination:

1. Was data, on **any other media type or format** (e.g., paper, cassette tape), owned or licensed by the state agency involved?
2. Were notice-triggering data elements involved?
    a. In accordance with Civil Code Section 1798.29, notice triggering data elements include an individual's first name or first initial and the individual's last name in combination with any one or more of the following:
        i. Social Security number.
        ii. Driver's License number, California Identification Card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
        iii. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

iv. Medical information (as defined in Civil Code Section 1798.29).

v. Health insurance information (as defined in Civil Code Section 1798.29).

vi. Unique biometric data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

vii. ALPR System information (as defined in Civil Code Section 1798.90.5).

viii. Genetic data.

b. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

3. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person?

   When determining whether or not acquisition has actually or is reasonably believed to have occurred, an agency is to consider the following indicators:

   a. The information is in the physical possession and control of an unauthorized person, such as a misdirected, lost, or stolen hardcopy document, or file containing notice-triggering information. This includes, but is not limited to, documents containing notice-triggering data elements which have been

   b. addressed and mailed to an unauthorized person, transmitted by facsimile to an unauthorized person, or information containing notice-triggering data elements which is otherwise conveyed, such as by word-of-mouth, to unauthorized persons.

c. The information has been viewed, acquired, or copied by an unauthorized person, or a person exceeding the limits of their authorized access.

d. The information has been shared by an unauthorized person or was used by an unauthorized person, such as instances of sharing the personal information with the media or tabloids, or identity theft reported, or fraudulent accounts opened.

C. Timeliness of the Notification

Following the discovery of a breach that involves personal information which meets the statutory or policy criteria for notification, agencies/state entities should provide notification to affected individuals in a timely manner and without unreasonable delay.

To the extent possible, notification should be made within ten (10) business days from the date the agency has determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person. The following are examples of circumstances which may warrant the delay of notification beyond the 10 days following discovery:

- Legitimate needs of law enforcement, when notification would impede or compromise a criminal investigation, or pose other security concerns [Civil Code Section 1798.29 (c)].
- Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system, so that the harm of the initial incident is not compounded by premature announcement. For example, if a data breach resulted from a failure in a security or information system, that system should be repaired and tested before disclosing details related to the incident. [Civil Code Section 1798.29 (a)].

Any decision to delay notification should be made by the agency head, or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf, and any delay should not exacerbate the risk of harm to any affected individual(s).

D. Source of the Notification

Given the serious security and privacy concerns raised by breaches involving personal information, the notice to individuals affected by the loss should be issued and signed by a responsible official of the agency. In those instances in which the breach involves a widely known component of an agency, notification should be given by a responsible official of the component. In general, notification to individuals affected by the breach should be issued by the agency head, or by the senior-level individual designated in writing by the agency head as having authority to act on his/her

behalf. Such action, demonstrates that the incident has the attention of the chief executive of the organization.

There may be some instances in which notice of a breach may appropriately come from an entity other than the actual agency that suffered the loss. For example, when the breach involves a contractor operating a system of records on behalf of the agency or a public- private partnership. The roles, responsibilities, and relationships with contractors or partners for complying with notification procedures should be established in writing with the contractor or partner prior to entering the business relationship, and must be reflected in the agency's breach response plan and in the contractual agreements with those entities.

Whenever practical, to avoid creating confusion and anxiety for recipients of the notice, the notice should come from the entity that the affected individuals are more likely to perceive as the entity with which they have a relationship. In all instances, when the breach involves a contractor or a public-private partnership operating a system on behalf of the agency, the agency is responsible for providing any required or necessary notification, and for taking appropriate corrective actions.

E. Format of the Notification

The breach notification shall be designed to call attention to the nature and significance of the information it contains, and shall be formatted on official letterhead to include:

1. No smaller than 10-point Ariel font type.

2. A title “Notice of Data Breach.”
3. Contain at a minimum the following headings:
    a. “What Happened”
    b. “What Information Was Involved”
    c. “What We Are Doing”
    d. “What You Can Do”
    e. “Other Important Information”
    f. “For More Information”
    g. “Agency Contact”

F. Content of the Notification

The substance of the notice should be written in clear, concise, and easy-to-understand language. The notice should avoid the use of technical jargon and shall include, at a minimum, the following elements:

1. A general description of what happened; including the date of breach if known; if not known, the estimated date or date range within which the breach occurred. Agencies/state entities should be mindful of the impact of disclosing either an insufficient amount of detail or too much detail in the general description of what happened. For example, in cases where an investigation is ongoing, disclosing certain details may impede or compromise the investigation, or cause other security concerns. On the other hand, failure to disclose a sufficient amount of detail may not provide the recipient with enough information to fully understand and mitigate their own risk. An agency must work with law enforcement authorities to ensure the content strikes the necessary balance.
2. A description of the type of personal information involved in the breach (e.g., full name, Social Security number, Driver’s License number or California Identification Card number, date of birth, home address, account number, disability code, medical or health information (as defined), etc.). The specific type

or types of notice-triggering data elements are to be provided in the notice. This is extremely important to help the recipient of the notice to fully understand how to mitigate their risk.

3. All of the steps that the individual could take to protect themselves from potential harm, if any.
4. An apology and a description of the steps the agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches.
5. The name and contact information of the individual contact(s) at the agency with the ability to provide more information about the breach to the affected individuals.
6. A toll-free telephone number for the agency contact, physical address, e-mail address, and if available, postal address. If the agency does not have a toll-free telephone number a local telephone number may be provided.

When the agency has knowledge that the affected individuals are not English speaking, to the extent practical, the notice should also be provided in the appropriate language(s).

Given the amount of information required above, in cases where it is only the name and Social Security number that has been breached, agencies/state entities may want to consider using the one-page Breach Help –Consumer Tips from the California Attorney General document as an enclosure with the notice letter. It is available in English and in Spanish and can be downloaded at: https://www.oag.ca.gov/privacy/business-privacy

The Breach Help –Consumer Tips from the California Attorney General document, as well as standardized breach notification templates for breaches involving other notice-triggering information, is provided as appendices (B through K) in this document. Using the standardized breach notifications templates provided in the appendices is required. In some cases it may be necessary to combine the language from multiple templates, such as in the hybrid template provided.

Consistent with Section 504 of the Rehabilitation Act of 1973, the agency should also give special consideration in providing notice to individuals who are visually or hearing impaired. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the agency's Web site.

G. Approval of the Notification

SIMM 5340-A requires agencies/state entities to submit draft breach notices to OIS for review and approval **prior to their release**. The intent is to ensure the consistency and clarity of notices, as well as the accuracy of privacy protection steps and instructions provided in notices. The procedures for submitting a request for review and approval of a draft breach notice to the OIS are as follows:

1. **Communicate with OIS security representative by telephone at (916) 245-2583 immediately prior to submission of any document, in order to alert the Office that a document requiring review will soon arrive.**
2. Upload breach notification into Cal-CSIRS.
3. Indicate the target date of release. Allow at least one full business day for OIS's review and approval of the initial and any subsequent submittals that are necessary due to changes not previously reviewed and approved by OIS.

Depending on the circumstances, the agency may also need to contact other public and private sector agencies, particularly those that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach. For example, an agency may need to seek confirmation from law enforcement that notification will not compromise the investigation. Or, when as a result of a large breach in individual names and Driver’s License numbers, the agency intends to reference the Department of Motor Vehicle (DMV) Fraud Hotline in the notice; the agency should seek DMV’s approval and provide DMV with advanced warning that DMV may experience a surge of inquiries.

Note: This Fraud Hotline is only used when an individual has evidence to suggest their Driver’s License number has been misused.

H. Method(s) of Notification

The best means for providing notification will depend on the nature and availability of contact information of the affected individuals, as well as the number of individuals affected. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following are examples of the types of notification which may be considered.

1. First-Class Mail: Written notice to the named individual, whenever possible by first- class mail to the last known address in the agency's records, should be the primary means of notification. For example, the notice should be addressed to "Jane Doe", and in cases of minor children the notice should be addressed "To the Parent of: Jane Doe". Where there is reason to believe the address is no longer current, an agency should take reasonable steps to update the address by consulting with other agencies, such as the U.S. Postal Service (USPS). The USPS will forward mail to a new address or will provide an updated address via established processes. The notice should also be sent separately from any other mailing so that it stands out to the recipient, and it should be labeled to alert the recipient to the importance of its contents, (e.g., "Important Information Enclosed"), and as to reduce the possibility that it may be mistaken as advertising mail.

   Notification should include sender or return address information unless there are special circumstances which necessitate not doing so. For example, the inclusion of the healthcare office or clinic name or return address may be more harmful than helpful and further reveal personal information.

2. Telephone: Notification by telephone may be appropriate as a supplement to written notice in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Persons making the notification by telephone should only do so by personal contact with the affected individual, never through a message on answering machine or other parties. In all cases, written notice by first-class mail must be made concurrently.

3. E-Mail: E-mail may only be used to make notification if the notice triggering data elements involved are limited to an individual's username or e-mail address in combination with a password or security question and answer that would permit access to the online account and as consistent with the Federal Electronic Signatures Act (15 U.S. Code 7001). The Federal Electronic Signatures Act requires, among other things, that an agency must have received express consent from the individual to use e-mail as the primary means of communication before making the breach notification. In such cases the agency may provide the security breach notification by e-mail or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account and all other online accounts for which the person uses the same user name or e-mail address and password or security question or answer.

   Agencies/state entities must keep in mind that notification by e-mail may be problematic because individuals change their e-mail address and often do not notify all parties of the change, and it may be difficult for individuals to distinguish the agency's e-mail notice from a "phishing" e-mail.

4. Substitute Notification. Subdivision (j), (3) of Civil Code Section 1798.29, provides for substitute notification when an agency can demonstrate that more than 500,000 individuals were affected, or the cost of providing notification would exceed $250,000, or the agency does not have adequate contact information on those affected. In accordance with that provision of law, substitute notification consists of all of the following methods:

   a. Conspicuous posting, for a minimum of 30 days of the notice on the agency's internet website, if the agency maintains one. This includes providing a link to the notice on the home page, or first significant page after entering the internet website. This link shall be displayed in a larger or contrasting text than the surrounding text in order to call attention to the link.

b. Notification to major statewide media and to the California Office of Information Security within the Department of Technology; and

c. E-mail notification when the agency has an e-mail address for the individuals. Here, because an agency is also doing a. and b., the e-mail notice does not need to meet the requirements of the Federal Electronic Signature Act.

The posting should also include a link to Frequently Asked Questions (FAQs) and other talking points to assist the public's understanding of the breach and notification process. See the Security Breach FAQ's provided on the Office of the Attorney General's website.

Further, when making a substitute notification, the public media should be notified as soon as possible after the discovery of the breach because delayed notification may erode public trust. However, an agency's decision to notify the public media in conjunction with substitute notification, or in other situations, will require careful planning and execution so that the agency is adequately prepared to handle follow- on inquiries.

I. Preparation for Follow-on Inquiries from Noticed Individuals

Those affected by the breach can experience considerable frustration if, in the wake of the individual notification or the initial public announcement, they are unable to find sources of additional accurate information. This applies to both follow-on inquiries made to the agency that experienced the breach, as well as to counterpart entities that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach. For example, depending upon the nature of the incident and the information involved, certain entities, such as the credit-reporting agencies, may also need to prepare for a surge in inquiries that might far exceed normal workloads (e.g., requests for copies of credit reports and posting of fraud alerts).

Consequently, and as appropriate, agencies/state entities must adequately prepare for follow-on inquiries and must address inquiries in the most efficient and accurate manner possible. In doing so, an agency should consider provisioning for the following:

1. Instructions to each of its public inquiry intake units about where they should direct both telephone and in-person inquiries about the breach from affected individuals, the media, and the public.
2. A toll-free phone line, answered by personnel specifically trained to handle inquiries from affected individuals and the public, especially when the breach has affected a large number of individuals.
3. A complaint resolution and/or escalation process. For example, individuals may be directed to the agency's Office of Civil Rights, if one is available.
4. Early warning and information about the timing of notification to all counterpart entities, so that they may adequately prepare for any potential surge in inquiries.
5. The timing for delivery of the notice to noticed individuals in conjunction with the availability of staff to respond to follow-on inquiries must also be considered. For example, an agency should not release a notification so that it is likely to be received on the last work day before major holiday weekend or the day of an observed holiday.

The OIS can assist agencies/state entities with the development of scripts, FAQs, staff training and other related notification activities.

J. Other Situations When Breach Notification Should Be considered

Neither state law nor state policy requires notification in the case of breaches involving non- notice-triggering personal information. Nevertheless, breaches involving certain types of non- notice triggering personal information can also implicate a broad range of harms to individuals. The other types of harm that an agency should consider, depending upon the nature of the personal information involved, and the circumstances of the loss or theft, include but are not limited to, the following:

- Harm to reputation.
- Potential for harassment.

- Potential for prejudice, particularly when health or financial benefits information is involved.
- Other types of financial loss, such as an increase or denial of insurance premiums which may be associated with the latter.
- Embarrassment.
- Legal problems.

In situations where other (non-notice-triggering) personal information is involved, an agency should, in consultation with its legal counsel and the OIS, consider the following factors when making an assessment of the likely risks of harm and the decision to notify:

1. Nature of the Data Elements Breached: The nature of the compromised data elements is a key factor to consider in determining if notification should be provided to affected individuals. It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive in another context. For example, the breach of a list containing the names and home addresses of undercover peace officers or domestic violence victims, poses a higher risk of harm than a list containing the names of individuals that subscribe to an agency's monthly newsletter on general family issues. Yet in the context of this subscriber list, if the newsletter were specific to a certain profession or clientele it could pose a higher level of risk, such as a newsletter that is specific to a support group for battered persons. It is also important to note that a Social Security number alone is useful in committing identity theft. In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of possible harms that could result from their acquisition by or disclosure to unauthorized individuals.

2. Likelihood the Information Is Accessible and Usable: Upon learning of a breach, agencies/state entities should assess the likelihood that personal information will be or has been acquired and misused by unauthorized individuals. An increased

risk that the information will be misused by unauthorized individuals should influence the agency's decision to provide notification.

The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals; however, depending upon any number of physical, technological, and procedural safeguards employed by the agency, the risk of compromise may be low to non-existent. For example, exposure on a public website for many weeks or months would increase the likelihood that it was acquired by an unauthorized individual. Also, if the information was properly protected by encryption, then the likelihood the information is accessible and usable is non-existent; whereas "paper copies" of printed personal information are essentially unprotected and would be considered a much higher risk of compromise depending upon the type of information involved.

In this context, the encryption product and algorithm used has been validated by the National Institute of Standards and Technology (NIST) to the American National Standards Institute (ANSI) management information standards and the Federal Information Processing Standards (FIPS), as state agencies are required to use the ANSI and FIPS standards in their information management planning and operations (SAM section 5100).

3. Likelihood the Breach May Lead to Harm: The IPA (Civil Code Section 1798.21) requires agencies to protect against anticipated threats or hazards to the security or integrity of records containing personal information which could result in any injury to individuals. When considering injury to individuals, agencies should consider the broad reach of potential harm and the likelihood harm will occur.
    a. *Broad Reach of Potential Harm*: The number of possible harms associated with the loss or compromise of information may include, but are not necessarily limited to, the following:
        i. the effect of a breach of confidentiality or fiduciary responsibility.

ii. The disclosure of address information for victims of stalking or abuse, or persons in certain high-risk professions (e.g., law enforcement officers, reproductive health care clinic workers, etc.).

iii. legal problems (e.g., an individual uses another individual's name and Driver's License number when arrested, or a pregnant woman uses the medical identity of a mother and delivers a baby who tested positive for illegal drugs. Consequently, Social Services takes her children from her and she must hire an attorney to prove that she is the victim of medical identity theft).

iv. harm to reputation.

v. financial loss.

vi. the disclosure of private facts and unwarranted exposure leading to embarrassment, humiliation, mental pain, emotional distress, or loss of self- esteem; the potential for secondary uses of the information which could result in fear or uncertainty.

vii. the potential for harassment, blackmail, or prejudice, particularly when health or financial benefits information is involved.

b. *Likelihood Harm Will Occur*: The likelihood that a breach of non-notice triggering personal information may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. While not considered notice-triggering under the law, a Social Security number alone is useful in committing identity theft, and if there is evidence that this information was the specific target of attack by a known identity theft fraud ring, the likelihood of harm would be considered greater than if this same information had been inadvertently exposed or acquired.

4. Ability of the Agency to Mitigate the Risk of Harm to Individuals. Within an information system, the risk of harm will depend on how the agency is able to

mitigate further compromise of the system(s) and/or information affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken. For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.

The ability of an agency or other affected entities to monitor for and prevent attempts to misuse the compromised information is a factor in determining the risk of harm, particularly the harms associated with identity theft. Such mitigation may not prevent the use of personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

Where practical, the agency should exhaust its ability to mitigate any risk of harm and provide timely instruction and guidance in the notice to affected individuals about steps they can take to protect themselves.

5. Ability of the Notified Individuals to Mitigate the Risk of Harm to Themselves: Notification should be designed to afford affected individuals an opportunity to mitigate their risk. For example, in the case where the name and home address of a victim of abuse has been compromised, the individual may, in order to mitigate their risk, choose to move or to affect a greater situational awareness.

   In some cases, the apology and assurance of corrective action, addressed through notification, may serve as a satisfactory remedy for those individuals who have been impacted, or potentially impacted, by the breach.

   On the other hand, agencies/state entities should bear in mind that notification, when there is little or no risk of harm might create unnecessary concern and confusion.

   Additionally, under circumstances where notification could increase the risk of harm, the prudent course of action is not to notify.

K. Other Actions Agencies Can Take to Mitigate Harm to Individuals

In addition to notifying affected individuals, it may be necessary for an agency to take other actions to mitigate the risk of harm. For example, if the breach involves government credit cards, the agency should notify the issuing bank promptly; or, if the breach is likely to lead to benefit fraud (e.g., Medi-Cal, Unemployment Insurance, etc.), the agency should notify the benefit agency, so that they can take appropriate actions, such as flagging accounts associated with the affected individuals.

L. Other Considerations When State Employee Data Is Involved

- Agency has treated affected employees with the same care and concern as any other individual affected by breach.
- Agency has considered other early warning and notification methods to augment the first-class mail notification (e.g., such as e-mail, Intranet posting, town hall meetings).
- Agency has notified managers and supervisors of the affected employees and adequately prepared them to answer questions from employees.
- Agency has considered notifying represented employee organizations as may be appropriate.
- Agency has considered the use of town hall meetings to respond to employee questions and concerns following notification.

I. Other Considerations

Outside of the legal and policy requirements discussed earlier there are two other steps an agency may consider to mitigate the effects of a breach on the agency and the individuals. The first is advanced notification to the media and the second is credit monitoring services. These are discussed in more detail below.

A. Advance Notification to the Media

Though not required, in breaches likely to receive greater attention, an agency may consider providing advance notification to the media as notifications are mailed to individuals. This allows the agency to present the facts of the story first, rather than

trying to correct inaccurate or incomplete news stories after they are published. Advance notification to the media also demonstrates openness and can promote good ongoing communications with reporters. In addition, providing accurate information through the news media is another way to reach those affected and to explain what steps they can take to protect themselves.

As mentioned above, the timing of any notification to media or individuals is critical. The agency must ensure it is prepared to handle follow-on inquiries and is appropriate given the circumstances. In some cases, it may be more prudent not to notify news media at the same time notification is made to affected individuals. For example, an individual who has stolen a password-protected laptop in order to resell it may be completely unaware of the nature and value of the information the laptop contains, and may wipe the laptop clean before selling it. In such a case, public announcement may actually alert a thief to what he possesses, increasing the risk that the information will be misused, and it would be wise to delay media notification at least until affected individuals have received notice and had time to take defensive action.

B. Credit Monitoring Services

The offer of credit monitoring services can provide an additional measure of protection for individuals affected by a breach - especially where the compromised information presents a risk of new accounts being opened. However, this involves agency expense and the services are only useful in cases where there has been a breach of Social Security number, California Driver’s License, or California Identification Card number.

Credit monitoring is not helpful for breaches of account numbers only. When a “free” mitigation product is offered, be sure that the individuals are not automatically enrolled for a renewal at their own cost.

Credit monitoring is a commercial service that cannot prevent or guarantee that identity theft will not occur; however, it can assist individuals in early detection of instances of new-account identity theft, thereby allowing them to take steps to minimize the harm. Typically, the service notifies individuals of activities on their credit files, such as creation of a new account or inquiries to the file. Consult the

Consumer Federation of America consumer resource publications "Best Practices for Identity Theft Services" and "Best Practices for Identity Theft Services: How Are Services Measuring Up?".

II. Notifying Others When Required

A. Notifying the Attorney General

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. [Civil Code section 1798.29 (a) and Civil Code Section 1798.82 (a)].

Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. [Civil Code Section 1798.29(e) and Civil Code section 1798.82(f)]

Use the Attorney General's online form to submit a sample of the security breach notification at: http://oag.ca.gov/ecrime/databreach/reporting.

B. Notifying Credit Reporting Agencies

Sending breach notification letters involving a breach of Social Security numbers or Driver's License/California ID numbers can result in a large volume of calls to consumer credit reporting agencies, affecting their ability to respond efficiently. Be sure to contact these agencies before you send out notices in cases involving a large number of individuals - 10,000 or more. Note that this step is not relevant for breaches of a single account number or of medical or health insurance information alone. Make arrangements with the credit reporting agencies during your preparations for giving notice, without delaying the notice for this reason. You may contact the credit reporting agencies as follows:

- Experian: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.
- Equifax: Send an e-mail to businessrecordsecurity@equifax.com.

- TransUnion: Send an e-mail to fvad@transunion.com, with “Database Compromise” as the subject.

III. Questions

Questions regarding this requirement may be sent to:
California Department of Technology
Office of Information Security
security@state.ca.gov

IV. Appendices

To assist the agency with responding to a breach and drafting a breach notice, the following breach response checklist, sample breach notices, and the corresponding document enclosure has been provided as appendices herein.

Note: If a breach involves more than one type of notice-triggering information, the notice should use language from all the relevant sample notices. Further, when deceased person’s or minor children’s personal information is involved, special content and recommended actions are necessary for inclusion in the notification. Consult OIS in these cases.

Appendix A: Breach Response and Notification Assessment Checklist

Appendix B: Sample Breach Notice - Social Security Number

Appendix C: Sample Breach Notice – Unique Identification Number:

> A unique identification number can be a Driver's License Number, California Identification Card Number, Tax Identification Number, Passport Number, Military Identification Number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

Appendix D: Sample Breach Notice – Debit or Credit Card or Financial Account Number

Appendix E: Sample Breach Notice - Medical Information

Appendix F: Sample Breach Notice - Health Insurance Information

Appendix G: Sample Breach Notice – Unique Biometric Data

Appendix H: Sample Breach Notice – Hybrid (SSN and Health Information)

Appendix I: Sample Breach Notice – Automated License Plate Recognition System

Appendix J: Sample Breach Notice – Genetic Data

Appendix K: Sample Breach Notice – Username or E-mail Address

Appendix L: Breach Help – Consumer Tips Enclosure (English)

Appendix M: Breach Help – Consumer Tips Enclosure (Spanish)

Appendix A: Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
1. Assemble State Entity Response Team	p. 12			
1.1. Escalation Manager/Team Lead	p. 12			
1.2. Program Manager (office experiencing the breach)	p. 12			
1.3. Information Security Officer	p. 12			
1.4. Chief Privacy Officer or Coordinator	p. 12			
1.5. Public Information Officer or Communications Officer	p. 12			
1.6. Legal Counsel	p. 12			
1.7. Other	p. 12			
1.8. Chief Information Officer or Technology Specialist	p. 12			
1.9. Personnel Office or Human Resources Manager	p. 12			
2. Escalation/Internal Reporting	p. 12			
2.1. Deputy Director	p. 12			
2.2. Director	p. 12			
2.3. Agency Secretary	p. 12			
2.4. Governor's Office	p. 12			
3. Is an impact assessment/coordination meeting necessary?	p. 13			
3.1. Agency Response Team Members to Attend	p. 13			
3.2. OIS Response Team Member to Attend	p. 13			
3.3. CCIU Response Team Members to Attend	p. 13			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
3.4. Sign in Sheet / Attendee roster needed	p. 13			
3.5. Non-disclosure agreement forms needed	p. 13			
4. Security Incident Reporting	p. 13			
4.1. Reported through Cal-CSIRS	p. 13			
4.2. Respond to CHP CCIU response inquiry	p. 13			
4.3. Respond to OIS response inquiry	p. 13			
4.4. Update the work notes in Cal-CSIRS	p. 13			
5. Is breach notification required by law (Civil Code Section 1798.29)?	p. 15			
5.1. Was computerized data owned or licensed by the agency involved?	p. 16			
5.2. Was a computer system, equipment, or peripheral storage device (capable of containing computer data) involved?	p. 16			
5.3. Were notice-triggering data elements involved?	p. 17			
5.3.1. First name or first initial and the individual's last name, and one or more of the following:	p. 17			
5.3.2. Social Security number.	p. 17			
5.3.3. Driver's License number or California Identification Card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.	p. 17			
5.3.4. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.	p. 17			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
5.3.5. Medical information (as defined in Civil Code Section 1798.29).	p. 17			
5.3.6. Health insurance information (as defined in Civil Code Section 1798.29).	p. 17			
5.3.7 Unique biometric data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes(as defined in Civil Code Section 1798.29).	p. 17			
5.3.8 Automated License Plate Recognition (ALPR) System information (as defined in Civil Code Section 1798.90.5).	p. 17			
5.3.9 Genetic data (as defined in Civil Code Section 1798.29)	p. 18			
5.3.10 A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.	p. 18			
5.4. Were the notice-triggering data elements encrypted?	p. 18			
5.4.1. Was the encryption product used, a FIPS 140-3 validated or NIST certified cryptographic module?	p. 18			
5.5. Were notice triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person? (Examples only- list is not limited to these):	p. 18			
5.5.1. The system, equipment, or information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other devices that have the capability of containing information.	p. 18			
5.5.2. The information has been downloaded or copied (e.g., any evidence that download or copy activity has occurred).	p. 18			
5.5.3. The attacker deleted security logs or otherwise "covered their tracks".	p. 19			
5.5.4. The duration of exposure in relation to maintenance of system logs or in cases of an inadvertent or unauthorized Web site posting.	p. 19			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
5.5.5. The attack vector used is known to seek and collect personal information.	p. 19			
5.5.6. The information was used by an unauthorized person, such as instances of identity theft reported or fraudulent accounts opened.	p. 19			
6. Is breach notification required by Information Technology policy?	p. 19			
6.1. Was data, of any media type or format (e.g., paper, cassette tape), owned or licensed by the agency involved?	p. 19			
6.2. Were notice-triggering data elements involved?	p. 19			
6.2.1. First name or first initial and the individual's last name, and one or more of the following:	p. 19			
6.2.2. Social Security number.	p. 19			
6.2.3. Driver's License number or California Identification Card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.	p. 19			
6.2.4. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.	p. 20			
6.2.5. Medical information (as defined in Civil Code Section 1798.29)	p. 20			
6.2.6. Health insurance information (as defined in Civil Code Section 1798.29)	p. 20			
6.2.7 Unique biometric data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.	p. 20			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
6.2.8 Automated License Plate Recognition (ALPR) System information (as defined in Civil Code Section 1798.90.5).	p. 20			
6.2.9 Genetic Data (as defined in Civil Code Section 1798.29)	p. 20			
6.2.10 A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.	p. 20			
6.3. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired? (Examples only-list is not limited to these):	p. 20			
6.3.1. The information is in the physical possession and control of an unauthorized person, such as a misdirected, lost, or stolen hardcopy document, or file containing notice-triggering information.	p. 20			
6.3.2. The information has been viewed, acquired, or copied by an unauthorized person, or a person exceeding the limits of their authorized access.	p. 21			
6.3.3. The information has been shared by an unauthorized person or was used by an unauthorized person, such as instances of sharing the personal information with the media or tabloids, or identity theft reported, or fraudulent accounts opened.	p. 21			
7. Timeliness of Notification	p.21			
7.1. Notification can be sent within ten (10) days from the date data acquisition has been determined.	p. 21			
7.2. Notification may be delayed due to legitimate needs of law enforcement.	p. 21			
7.3. Notification may be delayed to determine scope of breach.	p. 21			
7.4. Notification may be delayed to restore system to reasonable integrity.	p. 21			
7.5. Delay will or may exacerbate the risk of harm to individuals.	p. 22			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
7.6. Agency head (or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf) has authorized the delay of notification.	p. 22			
8. Source of Notification	p. 22			
8.1. Agency head (or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf) will sign the notice.	p. 22			
8.2. The notice is addressed by the entity in which the recipient has a relationship.	p. 22			
8.3. The notice is addressed by an entity in which the recipient has no direct relationship, but the relationship is explained sufficiently in the notice.	p. 22			
9. Format of Notice	p. 23			
9.1. The notice shall be designed to call attention to the nature and significance of the information it contains, and shall be formatted on official letterhead to include:	p. 23			
9.1.1. No smaller than 10-point Ariel font type;	p. 23			
9.1.2. A title “Notice of Data Breach”; and	p. 23			
9.1.3. Contain at a minimum the following headings: • “What Happened” • What Information Was Involved” • “What We Are Doing” • “What You Can Do” • “Other Important Information” • “For More Information” • “Agency Contact”	p. 23			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
10. Content of Notice	p. 23			
10.1. The notice leverages the sample notifications provided by OIS.	Appendices B-I			
10.2. The notice is clear and concise.	p. 23			
10.3. The notice uses easy-to-understand language and does not include technical jargon.	p. 23			
10.4. The notice includes a general description of what happened; including the date of breach if known, or estimated date or date range within which the breach occurred.	p. 23			
10.5. The notice specifically identifies the data elements involved.	p. 24			
10.6. The notice includes the steps the individual can/should take to protect themselves from harm (if any).	p. 24			
10.7. The notice includes an apology.	p. 24			
10.8. The notice includes information about what the agency has done or is doing to investigate the breach, mitigate the losses, and protect against any further breaches.	p. 24			
10.9. The notice includes the name and contact information of an individual contact(s) at the agency with the ability to provide more information about the breach to the affected individuals.	p. 24			
10.10. The notice provides a toll-free number for the agency contact, physical address, e-mail address, and postal address if available. If the agency does not have a toll-free number a local number for the contact is provided.	p. 24			
10.11. The agency has knowledge that affected individuals are not English speaking and has prepared notices in the appropriate languages.	p. 24			
10.12. The agency has given consideration in providing the notification to individuals who are visually or hearing impaired (e.g., establishing a TDD or posting a large-type notice).	p. 25			
11. Approval of the Notification	p. 25			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
11.1. Draft notice submitted to OIS for review and approval prior to their release:	p. 25			
11.1.1. Communicated with an OIS security representative by telephone contact, prior to submission.	p. 25			
11.1.2. Submitted breach notification into Cal-CSIRS, selecting “Breach Notification for Review” as the type.	p. 25			
11.1.3. Have allowed at least one full business day for OIS review.	p. 25			
11.2. Final notice submitted to OIS and includes required information.	p. 25			
11.3. The agency has notified and/or sought prior approval for release of notice or the use of reference from other public and private sector agencies that may be impacted by the breach or play a role in mitigating the potential harms (e.g., credit reporting agencies, etc.).	p. 25			
12. Method(s) of Notification	p. 26			
12.1. First-class mail notification will be made.	p. 26			
12.1.1. Addressed to the named individual.	p. 26			
12.1.2. Mailed to the last known address.	p. 26			
12.1.3. Mailed separately from other letters and notices.	p. 26			
12.1.4. Labeled on the outside of the envelope to alert recipient to the importance of its contents (e.g., "Important Information Enclosed"), and as to reduce the possibility that it may be mistaken for advertising mail.	p. 26			
12.1.5. Includes sender or return address information. Special caveats noted here.	p. 26			
12.2. Telephone notification will be made with a concurrent follow-up written by first-class mail.	p. 27			
12.3. E-mail notification will be made as the following criteria are met:	p. 27			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
12.3.1. Individual has provided agency with an e-mail address.	p. 27			
12.3.2. Individual has provided written consent to use e-mail as the primary means of communication.	p. 27			
12.3.4. E-mail notification is consistent with the provisions regarding electronic records and signatures set forth in the Federal Electronics Signatures Act (15 U.S. Code 7001).	p. 27			
12.4. Substitute notification will be made as the following criteria are met:	p. 27			
12.4.1. Agency has demonstrated that more than 500,000 individuals were affected; or the cost of providing notification would exceed $250,000; or the agency does not have adequate contact information on those affected (no known mailing address is available).	p. 27			
12.4.2. Substitute notification, as required, will include the following collectively: 1) Conspicuous posting on the agency website. 2) Notifications to statewide media. 3) E-mail notification when the agency has an e-mail address to individuals. Here, the requirements of the Federal Electronics Signatures Act do not need to be met.	p. 28			
12.4.3. Web posting will be made on homepage or a conspicuous link from the homepage.	p.28			
12.4.4. Web posting will also include a link to FAQs.	p.28			
12.4.5. Information in press release will not impede or compromise the investigation or pose other security risks.	p.28			
12.5. Agency has elected to issue press release, as well as first-class notification due to the number of individuals affected.	p.28			
12.5.1. Information in press release will not impede or compromise the investigation or pose other security risks.	p.28			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
13. Preparation for Follow-on Inquiries from Noticed Individuals	p.28			
13.1. The agency's public intake areas have been alerted and trained as appropriate to properly direct telephone and in-person inquiries about the breach.	p. 29			
13.1.1. Inquiries from the press are to be directed to:	p. 29			
13.1.2. Inquiries from individuals receiving the notice and needing more information are directed to:	p. 29			
13.2. The agency has provisioned for a toll-free call center, staffed with trained personnel.	p. 29			
13.3. The agency has provisioned for documented scripts, and answers to anticipated and frequently asked questions.	p. 29			
13.4. The agency has provisioned for a complaint resolution and/or escalation process.	p. 29			
13.5. The agency has provided early warning and information about the timing of notification to all counterparts, so that they are prepared for the potential surge in inquiries (e.g., credit reporting agencies, etc.).	p. 29			
14. Other Situations When Breach Notification Should be Considered	p. 30			
14.1. The agency has considered the nature of any non-notice triggering personal information involved in this breach and the potential harms it poses or may pose to affected individuals.	p. 30			
14.1.1 The agency has determined the nature of the information does potentially pose one or more of the following potential harms (Examples only-list is not limited to these):	p. 30			
14.1.1.1. Harm to reputation.	p. 30			
14.1.1.2. Potential for harassment.	p. 30			
14.1.1.3. Potential for prejudice, particularly when health or financial benefits information is involved.	p. 30			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
14.1.1.4. Financial loss.	p. 30			
14.1.1.5. Embarrassment.	p. 30			
14.1.1.6 Legal problems.	p. 30			
14.2. The agency has considered the likelihood that the information has been acquired or is accessible and usable.	p. 31			
14.2.1. The agency has determined whether it is known or highly likely the information has been acquired and has the potential for misuse by unauthorized persons due to the following (examples only- list is not limited to these):	p. 31			
14.2.1.1. The information was not encrypted.	p. 31			
14.2.1.2. The list was posted on the Internet for an extended period.	p. 31			
14.2.1.3. The encryption product used was not a NIST certified cryptographic module or FIPS 140-3 validated product.	p. 31			
14.3. The agency determined there is a likelihood that the breach may lead to harm due to the following (examples only-list is not limited to these):	p. 32			
14.3.1. breach of confidentiality or fiduciary responsibility.	p. 32			
14.3.2. disclosure of address for victims of stalking or abuse; or persons in high-risk professions.	p. 32			
14.3.3. legal problems.	p. 32			
14.3.4. harm to reputation.	p. 32			
14.3.5. financial loss.	p. 32			
14.3.6. disclosure of private facts and unwanted exposure; potential for secondary uses of the information which could result in fear or uncertainty.	p. 32			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
14.3.7. potential for harassment, blackmail, or prejudice.	p. 32			
14.3.8. the social security number alone can lead to identity theft.	p. 32			
14.4. The ability of the agency to mitigate the risk of harm to individuals.	p. 33			
14.4.1. The agency can mitigate further compromise of the system.	p. 33			
14.4.2. The agency can monitor systems for misuse of the personal information and patterns of suspicious behavior.	p. 33			
14.4.3. The agency has exhausted its ability to mitigate any further risk of harm.	p. 33			
14.4.4. The apology and assurance of corrective action may serve as a satisfactory remedy those impacted.	p. 33			
14.5. The ability of the noticed individual to mitigate the risk to themselves following notification.	p. 33			
15. Other Actions Agencies Can Take to Mitigate Harm	p. 34			
15.1. The agency has notified financial institutions if state payroll or bank account information was involved.	p. 34			
15.2. The agency has notified other agencies about the potential for benefit fraud as applicable (e.g., disability, unemployment, Medi-Cal)	p. 34			
16. Other Considerations When State Employee Data Is Involved	p. 34			
16.1. Agency has treated affected employees with the same care and concern as any other individual affected by breach.	p. 34			
16.2. Agency has considered other early warning and notification methods to augment the first-class mail notification (e.g., such as e-mail, Intranet posting, town hall meetings).	p. 34			
16.3. Agency has notified managers and supervisors of the affected employees and adequately prepared them to answer questions from employees.	p. 34			

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
16.4. Agency has considered notifying represented employee organizations as may be appropriate.	p. 34			
16.5. Agency has considered the use of town hall meetings to respond to employee questions and concerns following notification.	p. 35			
17. Other Considerations from a Public Relations Perspective	p. 35			
17.1. The agency has considered advanced notification to the media.	p. 35			
17.2. The agency has considered acquiring credit monitoring services for the affected individuals. Note: This should only be considered when the incident involves Social Security number.	p. 36			
18. Notifying Others When Required	p. 36			
18.1. Notifying the California Attorney General and uploading a redacted copy of the notification to their website when the incident requires notification to 500 or more individuals.	p. 36			
18.2. Notifying the Credit Reporting Agencies when notification is made to 10,000 or more individuals.	p. 37			

Appendix B: Sample Breach Notice: Social Security Number

[Agency Letterhead]

[Date]

[Addressee]

[Mailing Address]

[City] [State] [Zip Code]

[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*] The document contained your first and last name, along with your social security number.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files by following the recommended privacy protection steps outlined in the enclosure “Breach Help –Consumer Tips from the California Attorney General”.
Other Important Information:	Enclosure “Breach Help –Consumer Tips from the California Attorney General”
For More Information:	For more information on identity theft, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

_____ _____

[*Signature of State Entity Head or Delegate*] [*Title*]

Appendix C: Sample Breach Notice – Unique Identification Number*

As defined under IV Appendices topic.

[Agency Letterhead]

[Date]

[Addressee]

[Mailing Address]

[City] [State] [Zip Code]

[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*] The document contained your first and last name, along with your driver's license number.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files by following the recommended privacy protection steps outlined in the enclosure “Breach Help –Consumer Tips from the California Attorney General”.
Other Important Information:	Enclosure “Breach Help –Consumer Tips from the California Attorney General”
For More Information:	For more information on identity theft, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

[*Signature of State Entity Head or Delegate*] [*Title*]

* A unique identification number can be a Driver's License Number, California Identification Card Number, Tax Identification Number, Passport Number, Military Identification Number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

Appendix D: Sample Breach Notice - Credit Card or Financial Account Number

[Agency Letterhead]

[Date]

[Addressee]

[Mailing Address]

[City] [State] [Zip Code]

[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*] The document contained your first and last name, along with your bank account number.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	To help prevent unauthorized access and fraudulent activity on this account, we recommend that you immediately contact [the credit card or financial account issuer] and close your account. Tell them that your account may have been compromised and ask that they report it as "closed at customer request." If you want to open a new account, ask your account issuer to give you a PIN or password associated with the new account. This will help control access to the account.
Other Important Information:	Enclosure "Breach Help –Consumer Tips from the California Attorney General"
For More Information:	For more information on identity theft, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

_____ _____

[*Signature of State Entity Head or Delegate*] [*Title*]

Appendix E: Sample Breach Notice - Medical Information Only

[Agency Letterhead]

[Date]

[Addressee]

[Mailing Address]

[City] [State] [Zip Code]

[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*][1] Please note, the information was limited to [specify, (e.g., your name and medical treatment)] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your medical information [or medical history, medical condition, or medical treatment or diagnosis] was involved.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your <insert provider or plan name>, to serve as a baseline.
Other Important Information:	Enclosure “Breach Help –Consumer Tips from the California Attorney General”
For More Information:	For more information about your medical privacy rights, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

_____ _____

[*Signature of State Entity Head or Delegate*] [*Title*]

[1] Additional language will be necessary if other notice triggering information was involved. If the breach does not involve Social Security number, driver’s license/California Identification Card, or financial account numbers, say so and refer to the following language.

Appendix F: Sample Breach Notice - Health Insurance Information Only

[Agency Letterhead]
[Date]
[Addressee]
[Mailing Address]
[City] [State] [Zip Code]
[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*][1] Please note, the information was limited to [specify, (e.g., your name and health plan number] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your health insurance information [or policy, plan number, or subscriber identification number] was involved.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	Keep a copy of this notice for your records in case of future problems with your medical records. We also recommend that you regularly review the explanation of benefits statement that you receive from <Select ether, us, your health insurance plan, or your health insurer>. If you see any service that you believe you did not receive, please contact <Select ether, us, your health insurance plan, or your health insurer > at the number on the statement <or provide a number here>. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.
Other Important Information:	Enclosure “Breach Help –Consumer Tips from the California Attorney General”
For More Information:	For more information about your medical privacy rights, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

_____ _____
[*Signature of State Entity Head or Delegate*] [*Title*]

[1] Additional language will be necessary if other notice triggering information was involved. If the breach does not involve Social Security number, driver’s license/California Identification Card, or financial account numbers, say so and refer to the following language.

Appendix G: Sample Breach Notice – Unique Biometric Data

[Agency Letterhead]

[Date]

[Addressee]

[Mailing Address]

[City] [State] [Zip Code]

[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [date of incident] at [name of organization]. ABC Solutions, Inc. is contracted with the Department of Emergency Management to support use of biometric data for customer access to its online Emergency Management systems. Unique biometric data is defined as generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes On October 12, 2019 an inadvertent system configuration error lead to a five-hour exposure of the biometric data maintained by ABC Solutions. The error was immediately corrected upon discovery.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*][1] Please note, the information was limited to *your account name and fingerprints* and did not contain any other information, such as Social Security number, Driver's License number, California Identification Card Number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your personal biometric data was involved.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	If you use biometric data to access any accounts, we recommend you choose another form of authentication to protect against unauthorized access
Other Important Information:	Enclosure “Breach Help –Consumer Tips from the California Attorney General”
For More Information:	For more information about your privacy rights, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

_____ _____

[*Signature of State Entity Head or Delegate*] [*Title*]

Appendix H: Sample Breach Notice – Hybrid (SSN and Health Information)

[Agency Letterhead]

[Date]

[Addressee]

[Mailing Address]

[City] [State] [Zip Code]

[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	[[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*] The document contained your [*specify, (e.g., your name and health plan number)*] along with your social security number.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*]. We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [*provider or plan*], to serve as a baseline. Because your Social Security number was involved, in order to protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosure. Check your credit reports for any accounts or medical bills that you do not recognize. If you find anything suspicious, follow the instructions found in step four of the enclosure. Since your health insurance information was also involved, we recommend that you regularly review the explanation of benefits statement that you receive from [*name of health insurance provider*]. If you see any service that you believe you did not receive, please contact us at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.
Other Important Information:	Enclosure “Breach Help –Consumer Tips from the California Attorney General”
For More Information:	For more information about privacy protection steps and your medical privacy rights, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

_____ _____

[*Signature of State Entity Head or Delegate*] [*Title*]

Appendix I: Sample Breach Notice – Automated License Plate Recognition System

[Agency Letterhead]

[Date]

[Addressee]

[Mailing Address]

[City] [State] [Zip Code]

[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at [*XYZ Solutions, Inc.*]. XYZ Solutions, Inc. is an Automated License Plate Recognition (ALPR) system operator and maintains an ALPR system database used by many state and local law enforcement entities, including ours, to administer public safety and crime protection programs. We received notification on [*date notification received*] that an XYZ Solutions ALPR system database has been compromised.
What Information Was Involved?	*Describe what specific notice-triggering data element(s) were involved, see example below*] Please note, the information involved was limited to your name, address, vehicle license plate number, and the vehicle's location and patterns of movement, if any, between [*month day, year and month day, year*]. This incident did not involve any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	Your privacy is of utmost concern to us. For more information about your privacy rights, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Other Important Information:	Enclosure "Breach Help –Consumer Tips from the California Attorney General"
For More Information:	For more information on identity theft, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

_____ _____

[*Signature of State Entity Head or Delegate*] [*Title*]

Appendix J: Sample Breach Notice – Genetic Data

[Agency Letterhead]

[Date]

[Addressee]

[Mailing Address]

[City] [State] [Zip Code]

[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your genetic data information to the wrong person. “Genetic data” means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.
What Information Was Involved?	*Describe what specific notice-triggering data element(s) were involved, see example below*] Please note, the information was limited to genetic data only. This incident did not involve the compromise or access to any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	Your privacy is of utmost concern to us. For more information about your privacy rights, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Other Important Information:	Enclosure “Breach Help –Consumer Tips from the California Attorney General”
For More Information:	For more information on identity theft, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

_____ _____

[*Signature of State Entity Head or Delegate*] [*Title*]

Appendix K: Sample Breach Notice – Username or E-Mail Address

[Agency Letterhead]

[Date]

[Addressee]

[Mailing Address]

[City] [State] [Zip Code]

[Salutation]

Subject: **NOTICE OF DATA BREACH**

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*] involving the Online Information Sharing Portal (OISP). Our security systems detected an abnormally large number of attempts to access OISP user accounts. The computer-generated password guessing activity was designed to randomly guess user password combinations until account access is ultimately achieved. Further investigation revealed that some user account passwords were successfully guessed before the activity was detected and blocked.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*]. Please note, the information was limited to your user identification (email address), password and security questions for your OISP online account. This incident did not involve the compromise or access to any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. However, if you use the same user identification, password and or security question for any other online accounts those may be at risk.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we have implemented additional security controls to minimize the risk associated with this occurrence and the risk of recurrence. These include prompting all system users to update their profile and reset their passwords and security questions, and implementing automated validation at password creation to ensure the use of unique, hard-to-guess passwords, and established limits on the number of failed attempts to access your account.
What You Can Do:	To protect against unauthorized access and use of your online account(s), we recommend, if you haven't already done so, that you immediately change your password and security questions. Choose a unique, hard-to-guess password for each of your online accounts and always look for and report unusual activity in your accounts. A hard-to-guess password contains at least eight characters and is a combination of upper- and lower-case letters, numbers and special characters.
Other Important Information:	Enclosure "Breach Help –Consumer Tips from the California Attorney General"
For More Information:	For more information about online protections, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.oag.ca.gov/privacy
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*], at< physical address/postal address> or at <e-mail address>.

[*Signature of State Entity Head or Delegate*] [*Title*]

Appendix L: Office of the Attorney General Data Breach Help

The California Office of the Attorney General (OAG) offers an official guide designed to help consumers respond to data breaches. It outlines specific steps to take depending on what type of personal information was exposed, like Social Security numbers, bank accounts, medical information, or passwords. The tips aim to help protect people from identity theft or fraud after a data breach.

This resource can be found on the OAG website under the privacy section at: https://oag.ca.gov/privacy/other-privacy/breach-help-tips-for-consumers.

This resource is also available in PDF format in English at:

https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf

and in Spanish at:

https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/sp-cis-17-breach-help.pdf