

Determining Notification in the Event of a Security Breach

February 6, 2008

Background

California law¹ requires notification to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a security breach. Personal information is defined as an individual's **first name or first initial, and last name, in combination with any one or more of the following:**

- social security number
- driver's license number or California identification card number
- account number,² 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
- medical information
- health insurance information

Medical information is defined to mean any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; and health insurance information to mean 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.

General health information that is not a specific mental or physical condition or diagnosis by a health care professional does not meet this definition of medical information. Note that any unauthorized acquisition of medical information related to Worker's Compensation injuries or requests for accommodation, viz. American with Disabilities Act, would constitute a security breach as defined in this section.

If it is possible that the security breach involves medical or health insurance information as defined above, consult the Executive Director – Medical Services at the Office of the President.

University Policy

The University of California Business and Finance Bulletin IS-3 Electronic Information Resources establishes University policy for information security. Section III.D identifies requirements for University of California compliance with this statute.

¹ California Civil Code 1798.29

² The "account number" corresponds to an individual's *financial* account.

Deciding whether or not to notify

No criteria for reasonable belief are provided in the statute. Campuses should consider the factors listed below in making a determination to notify for any security incidents subject to this regulation.

The [California Office of Privacy Protection](#) in the California Department of Consumer Affairs recommends that the following factors be considered when making a determination to notify:

Acquisition

In determining whether unencrypted notice-triggering information has been *acquired*, or is reasonably believed to have been acquired, by an unauthorized person, consider the following factors, among others:

1. Indications that the information may be *in the physical possession and control* of an unauthorized person, such as when a computer or other device containing unencrypted notice-triggering information is lost, improperly disposed of, or stolen.
2. Indications that the information has been *downloaded* or copied, for example: an ftp log that contains the name of a file containing notice triggering information.
3. Indications that the information was *used* by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

The University of California recommends consideration of these additional factors:

- Duration of exposure since a very extended period of exposure increases the risk of unauthorized access.
- Indications that access logs may have been altered to disguise access.
- Indications that *any* download or copy activity has occurred, even if there is no specific evidence that there was a download or copy of data subject to the law.
- The extent to which the compromise indicates a directed attack, such as a pattern showing the machine itself was specifically targeted.
- Indication that the attack intended to seek and collect personal information.

Campuses may use additional criteria to determine whether to notify.

Other considerations

In addition to the factors listed above, there may be other circumstances to be considered when deciding whether or not to abide strictly by the requirements imposed by the law. As an example, although the law doesn't apply to data that is encrypted, if encrypted information is reasonably believed to have been acquired as a result of a security breach, the extent to which the encryption method would prevent the information from being used should be considered when deciding whether or not to notify.

The law states that a "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the

agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.” However, notification would be required if an employee misuses authorized access to disclose personal information. Note as well that an employee disclosing previously encrypted personal information on an unauthorized basis would trigger notification.

Decision to not notify

If there is difficulty reaching a decision whether or not there is a *reasonable belief* that data may have been acquired as defined by this law, campuses may also consider the potential of damage to individuals if the wrong decision is made.

- What harm might the individual experience if not notified; would it do more harm or good if individuals are or are not notified?
- One should weigh the potential for identity theft or financial abuse if it turns out that the data had been acquired and no notice was sent.
- The more ambiguous the situation, the greater the need to notify.

Decisions to notify or not notify should be well documented.

Forensics

A well managed log management infrastructure is an important tool to conduct analysis of security incidents and forensics examination of unauthorized access or use. A picture of relevant logs should be obtained without altering the history of events. When it is difficult to trace access and the magnitude of risk is high, outside forensic analysis services may be warranted. For more information, see [Log Management for the University of California: Issues and Recommendations](#).

University Collaboration

University of California Security Incident Response Coordination (UCSIRC) fosters the immediate and secure sharing of sensitive protection, incident, and response information through a trusted collaborative environment. UCSIRC also fosters the sharing of technical security observations that may reflect precursory incident information among University of California staff with computing/network security responsibilities. UCSIRC membership is listed at <http://www.ucop.edu/irc/itlc/ucsirc/membership.html>.