CALIFORNIA
OFFICE OF
PRIVACY
PROTECTION

Recommended Practices on Notice of Security Breach Involving Personal Information

January 2012

October 2003
Rev. April 2006
Rev. February 2007
Rev. May 2008
Rev. June 2009
Rev. January 2012

California Office of Privacy Protection
www.privacy.ca.gov
866-785-9663

Contents

Introduction

Origins of Data Breach Notification

Since 2002, when California passed its landmark data breach notification law, 46 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted similar legislation.[1] In 2009, the U. S. Department of Health and Human Services began requiring health care organizations subject to HIPAA and their business associates to notify of breaches of unsecured protected health information, and similar breach notification provisions were implemented by the Federal Trade Commission for vendors of personal health records and their third-party service providers.[2] At the same time, data protection authorities around the world have adopted or are moving to adopt similar notification requirements.

The original California law was modeled on right-to-know legislation from the environmental justice movement, which required public disclosure of uses and releases of hazardous substances to enable workers and communities to protect themselves.[3] Similarly data breach notification is intended to give individuals early warning that their personal information has gone astray to enable them to take protective actions. In addition to providing an alert, this transparency strategy has raised the issue of information security to public attention and has resulted in many organizations improving their practices for managing personal information. In fact, it can be argued that the data breach notification law, which does not impose any requirements regarding protection of personal information, has been the most effective information privacy statute in the past nine years.

Lessons Learned from Breaches

While perfect security and flawless execution of procedures will never be achieved, the lessons learned from publicly reported data breaches have helped organization improve their policies, practices, and technology. One lesson we have learned is that sensitive personal information is routinely stored outside the network, on a variety of portable devices and media. Many organizations now routinely protect information with encryption on laptops and other portable devices. Some have adopted procedures to safeguard the information on devices not intended to be portable, such as cabling PCs and laptops to desks. Some have tightly restricted the number of people who are permitted to carry sensitive personal information outside the office.

Some organizations have seen the wisdom of revising their data retention policies. After a breach that exposed 15-year-old data, a university decided not to retain certain information, including Social Security numbers, on applicants who were not admitted. Others have reconsidered their collection of the sensitive personal information in the first place. One blood bank which, like several others with mobile operations, had a laptop stolen, changed its policy of collecting Social Security numbers and decided to rely instead on the donor numbers that they were already using.

Cost of a Data Breach

A benchmark study of breaches at 51 organizations found that the average cost of a data breach in 2010 was $214 per record, making it the fifth year in a row that such costs have risen.[4] The study found that direct costs, such as printing, postage and legal fees, accounted for 34 percent of the total cost. Indirect costs, primarily lost customers, represented 66 percent.

The study also found that for the first time, malicious or criminal attacks, which accounted

for nearly a third of the incidents, were the most costly. Such breaches cost an average of $318. The impact of a data breach on reputation can also be significant. In a 2011 study, senior-level managers estimated that the loss or theft of confidential customer information diminshed the value of their brand by an average of 21 percent and restoring the damaged reputation took an average of a year.

Data Breaches and Identity Theft

The stated purpose of the California breach notice law was to enable individuals to protect themselves from identity theft.[5] This "crime of the 21st century" can have serious consequences for victims, requiring them to spend time and money to clear up their records. In the meantime, victims may be unjustly harassed by debt collectors, denied credit or employment opportunities; they may lose their cars or their homes, or be repeatedly arrested for crimes they did not commit.

According to the most recent nationwide survey, 8.1 million Americans were victims of identity theft in 2010. The same survey estimated the total cost of identity theft in the U.S. at $37 billion. The average victim spent $631 and 33 hours to resolve the problem and clear up records.[6]

The survey also asked respondents whether they had received a data breach notice in the past year. The results indicated a strong correlation between breach and identity theft. Those who reported receiving a breach notice were five times more likely to be victims of identity theft than those who had not received a notice. Furthermore identity theft victims who had received a breach notice had higher costs in time and money for recovering from identity theft: breach notice recipients' out-of-pocket costs averaged $1,108 and they spent 41 hours on resolution, compared to $510 and 30 hours for victims who had not received a breach notice.[7]

In recent years, a particularly pernicious type of identity theft has been noticed. Medical identity theft occurs when someone uses an individual's name and sometimes other identifying information without the individual's knowledge to obtain medical services or products. Medical identity theft has been called the information crime that can kill you, because in addition to a financial dimension it can also result in putting dangerously inaccurate information in the victim's medical records. This form of identity theft can be very difficult to discover and to correct, and the procedures for responding to the more common forms of financial identity theft are not available in the medical arena.[8]

Keeping Breach Notice Law Current

Growing awareness of medical identity theft led to new breach notice provisions. In 2008 the California breach notice law was amended to add medical and health insurance information to the original financial information (account numbers, Social Security number, and driver's license number) that could trigger the notice requirement. In 2009, a separate California law took effect for state-licensed health facilities. Inspired by reports of hospital employees browsing the medical records of celebrities, this law establishes fines and notification requirements for health facilities that fail to prevent unauthorized access to patients' medical records.[9]

The latest amendment to the breach notice law took effect in 2012.[10] The amendments require specific contents in breach notices, such as the type of personal information compromised and what individuals can do to protect themselves. In addition, organizations are required to send sample notices to the Attorney General and to notify other specified state agencies in certain situations. This requirement enables the creation of a repository of notices, which will help researchers and organizations to get a full picture of the nature of the incidents and therefore be able to make needed improvements in privacy and security practices.

The California Office of Privacy Protection's Recommended Practices

California law obligates the Office of Privacy Protection to protect the privacy of indi-

viduals' personal information by "identifying consumer problems in the privacy area and facilitating [the] development of fair information practices."[11] One of the ways that the Office is directed to do this is by making "recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers."[12]

The recommendations offered here are neither regulations, nor mandates, nor legal opinions. Rather, they are a contribution to the development of "best practices" for businesses and other organizations to follow in managing personal information in ways that promote and protect individual privacy interests.

In developing the original version of the recommendations, the Office received consultation and advice from an advisory group made up of representatives of the financial, health care, retail, technology and information industries, state government agencies, law enforcement, and consumer privacy advocates. When updating the recommendations to address medical information, additional advisors were consulted. A list of advisory group members can be found in Appendix 1. The group members' contributions were very helpful and are greatly appreciated.

Recommended Practices

The California Office of Privacy Protection's recommended practices are intended to assist organizations in supplementing their information privacy and security programs. The recommendations are not regulations and are not binding. Nor are they limited to the scope of the California law on notice of security breach, but rather they represent a broader approach and a higher standard.

These "best practices" recommendations can serve as guidelines for organizations, to assist them in providing timely and helpful information to individuals whose personal information has been compromised while in the organization's care. Unlike many best practices sets, however, these recommendations do not contain all the practices that should be observed. Information-handling practices and technology are changing rapidly, and organizations should continuously review and update their own situation to ensure compliance with the laws and principles of privacy protection. It is recognized that specific or unique considerations, including compliance with other laws, may make some of these practices inappropriate for some organizations.

Our practice recommendations are presented in three parts: Part 1 - Protection and Prevention, Part II - Preparation for Notification, and Part III - Notification. While the California law on notice of security breach applies to unencrypted "computerized data," we recommend applying these practices to records in any media, including paper records.

Definitions

The following are definitions of key terms used in these recommended practices. (Note that the bold terms are not used in the statute.)

Notice-triggering information: As provided in California law, this is unencrypted, computerized information, specifically first name or initial and last name plus any of the following:

- Social Security number,
- driver's license number or California Identification Card number,
- financial account number, in combination with any required code or password permitting access to an individual's financial account,
- medical information, as defined on pages 22-23 OR
- health insurance information, as defined on pages 22-23.

Data owner: The individual or organization with primary responsibility for determining the purpose and function of a record system.

Data custodian: The individual or organization that has responsibility delegated by the data owner for maintenance and technological management of the record system.

Data subject: An individual whose notice-triggering information is involved in a security breach.

Part I: Protection and Prevention

While an organization's information security program may be unique to its situation, there are recognized basic components of a comprehensive, multi-layered program to protect personal information from unauthorized access.[13] An organization should protect the confidentiality of personal information whether it pertains to customers, employees or others. For both paper and electronic records, these components include physical, technical and administrative safeguards. Among such safeguards are the following recommended practices.

1. Collect the minimum amount of personal information necessary to accomplish your business purposes, and retain it for the minimum time necessary.

- Identify your business reasons for collecting and retaining personal information, particularly notice-triggering information (Social Security numbers, driver's license or State ID numbers, financial account numbers, medical information, health insurance information).

2. Inventory records systems, critical computing systems, and storage media to identify those containing personal information.

- Include laptops and portable devices used to store personal information.

3. Classify personal information in records systems according to senstivity.

- Identify notice-triggering personal information.

4. Use appropriate physical and technological security safeguards to protect personal information, particularly notice-triggering information, in paper as well as electronic records.

- Authorize employees to have access to only the specific categories of personal information their job responsibilities require.
- Where possible, use technological means to restrict internal access to specific categories of personal information.
- Monitor employee access to personal information.
- Remove access privileges of former employees and contractors immediately.

5. Pay particular attention to protecting notice-triggering personal information on laptops and other portable computers and storage devices.

- Restrict the number of people who are permitted to carry such information on portable devices.
- Consider procedures such as cabling PCs to desks or prohibiting the downloading of higher-risk personal information from servers onto PCs or laptops.
- Use encryption to protect personal information on portable computers and devices.[14]

6. Do not use data containing personal information in testing software or systems.

7. Promote awareness of security and privacy policies and procedures through ongoing employee training and communications.

- Monitor employee compliance with policies and procedures.
- Include all new, temporary, and contract employees in security and privacy training and monitoring.
- Impose penalties for violation of security and privacy policies and procedures.

8. Require service providers and business partners who handle personal information on behalf of your organization to follow your security policies and procedures.

- Make privacy and security obligations of third parties enforceable by contract.[15]
- Monitor and enforce third-party compliance with your privacy and security policies and procedures.

9. Use intrusion detection technology and procedures to ensure rapid detection of unauthorized access to higher-risk personal information.

- Conduct periodic penetration tests to determine effectiveness of systems and staff procedures in detecting and responding to security breaches.

10. Wherever feasible, use data encryption, in combination with host protection and access control, to protect higher-risk personal information.

- Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard.[16]

11. Dispose of records and equipment containing personal information in a secure manner.

- Shred paper records with a cross-cut shredder and use a program to "wipe" and overwrite the data on hard drives.[17]

12. Review your security plan at least annually or whenever there is a material change in business practices that may reasonably implicate the security of personal information.

- For example, if an organization decides to outsource functions that use personal information, such as using a call center, the plans should be revisited to take the new third parties into account.

13. If you are a health plan or health insurer, provide patients with regular explanation of benefits statements.

- Explanation of benefits statements should be sent promptly following every service or in response to patient request.
- Statements should be in plain, consumer-friendly language and should contain a contact number for patients to ask questions about the statements.

Part II: Preparation for Notification

An information security program should contain an incident response plan, which addresses security incidents including unauthorized access to or acquisition of higher-risk personal information.[18] To ensure timely notice to affected individuals, the following practices are among those that should be included in an incident response plan.

1. Adopt written procedures for internal notification of security incidents that may involve unauthorized access to higher-risk personal information.

2. Designate one individual as responsible for coordinating your internal notification procedures.

3. Regularly train employees, including all new, temporary and contract employees, in their roles and responsibilities in your incident response plan.

- Collect 24/7 contact numbers for incident response team and provide to team members.
- Make sure that all employees and contractors can recognize a potential breach and know where to report it.

4. Define key terms in your incident response plan and identify responsible individuals.

5. Plan for and use measures to contain, control and correct any security incident that may involve personal information.

6. Require the data custodian or others who detect an information security incident to immediately notify the data owner upon detection.

7. Identify appropriate law enforcement contacts to notify on security incidents that may involve illegal activities.

- Appropriate law enforcement agencies may include California's regional high-tech crimes task forces, the Federal Bureau of Investigation, the U.S. Secret Service, and the local police or sheriff's department. See Appendix 5 for contact information.

8. Consider suggestions from law enforcement with expertise in investigating high-technology crimes for inclusion in your incident response plan.[19]

9. Identify any government agencies that you are required to notify of a breach.

- Collect appropriate contact information for making such notifications.

10. If you plan to notify affected individuals by e-mail, get the individuals' prior consent to the use of e-mail for that purpose.

- See the consent procedures in the federal Electronic Signature Act.[20]

11. Adopt written procedures for notification of individuals whose unencrypted notice-triggering personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.

- Include unauthorized acquisition of computer printouts and other paper records containing notice-triggering personal information in your notification procedures.

12. Document response actions taken on an incident. This will be useful to your organization and to law enforcement, if involved.

- At the conclusion of an incident, review events and actions and make any indicated changes in your technology and response plan.

13. Review your incident response plan at least annually or whenever there is a material change in your business practices.

- Update your breach response plan to address breaches of medical and health insurance information.

14. If you are a health plan or health insurer, be prepared to implement additional safeguards when member or subscriber information is compromised in a breach.

- If an individual reports that his or her health insurance policy number or subscriber identification number was used by someone else or was compromised in a breach, give the individual a new number, if feasible.
- Consider "flagging" compromised policy or subscriber numbers, if feasible, and using special procedures to verify identity of anyone requesting services under flagged numbers.

Part III: Notification

Openness or transparency is another basic privacy principle. An organization that collects or manages personal information should be open

about its information policies and practices. This responsibility includes informing individuals about incidents such as security breaches that have caused their unencrypted personal information to be acquired by unauthorized persons. The purpose of notifying individuals of such incidents is to enable them to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm.

To ensure giving timely and helpful notice to affected individuals, the following practices are recommended.

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 is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information.
2. Indications that the information has been downloaded or copied.
3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Timing of Notification

Notify affected individuals in the most expedient time possible after the discovery of an incident involving unauthorized access to notice-triggering information.

NOTE: Certain health facilities licensed in California are required to notify the California Department of Public Health and affected individuals within five days of detection. See Appendix 4 for more information of these requirements.

1. Take necessary steps to contain and control the systems affected by the breach and conduct a preliminary internal assessment of the scope of the breach.
2. Once you have determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person, notify affected individuals within 10 business days.
   - Do this unless law enforcement authorities tell you that providing notice at that time would impede their investigation.

Contacting Law Enforcement

If you believe that the incident may involve illegal activities, report it to appropriate law enforcement agencies.

1. In contacting law enforcement, inform the law enforcement official in charge of the investigation that you intend to notify affected individuals within 10 business days.
2. If the law enforcement official in charge tells you that giving notice within that time period would impede the criminal investigation:
   - Ask the official to inform you as soon as you can notify the affected individuals without impeding the criminal investigation.
   - Be prepared to send the notices immediately upon being so informed.
   - It should not be necessary for a law enforcement agency to complete an investigation before notification can be given.

Notify Individuals

If your assessment leads you to reasonably believe that notice-triggering information was acquired by an unauthorized person, implement your notification plan.

1. Notify California residents whose notice-triggering information was acquired by an unauthorized person.

2. Notify affected individuals in situations involving unauthorized acquisition of notice-triggering information in any format, including computer printouts and other paper records.
3. If you cannot identify the specific individuals whose notice-triggering information was acquired, notify all those in the groups likely to have been affected, such as all whose information is stored in the files involved.
    - Implement procedures for determining who gets included in the notice and who does not. Make reasonable efforts to obtain current mailing addresses.
    - Document your process for determining inclusion in the group to be notified.

Send Notice to the California Attorney General

Send a sample copy of notices of breaches affecting more than 500 California residents to the California Attorney General at https://oag.ca.gov/ecrime/databreach/report-a-breach.

- Be sure the notice submitted does not include name, address or any personal information of recipients.

Contacting Credit Reporting Agencies

Sending notice letters of 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 the 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.

1. Make arrangements with the credit reporting agencies during your preparations for giving notice, without delaying the notice for this reason.
2. 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.

Credit Monitoring and Related Products

If you are considering offering notice recipients credit monitoring or another identity theft assistance service as a mitigation, make sure it is relevant to the situation.

- Credit monitoring provides early notice when new accounts are opened or applied for. It is helpful for breaches of Social Security numbers or driver's license/California ID numbers.
- Credit monitoring is not helpful for breaches of account numbers only.
- When you offer a "free" mitigation product, be sure that the individuals are not automatically enrolled for a renewal at their own cost.
- Consult the advice on selecting such a product in "Best Practices for Identity Theft Services," at www.idtheftinfo.org.

Contents of Notice

A sample notice letter is attached as Appendix 2. Include the following information in your notice to affected individuals:

1. The date of the notice. If the notice was delayed as the result of a law enforcement investigation, say so.
2. A general description of the breach incident.
3. The specific types of personal information that were involved.
4. The name and contact information of the

organization sending the notice (usually the data owner).

5. The date or estimated date when the breach occurred.

6. The toll-free telephone numbers and addresses of the major credit reporting agencies, but only in a breach involving Social Security numbers or driver's license or California ID numbers.

7. What you have done to protect the individual's personal information from further unauthorized acquisition.

8. What your organization will do to assist individuals, including providing your toll-free contact telephone number for more information and assistance.

9. Information on what individuals can do to protect themselves from identity theft, as appropriate for the specific type of personal information involved.

   - See the sample notice letter in Appendix 2. Note that this sample letter is intended for California residents. The information on contacting DMV, for example, does not apply to other states.

10. Contact information for the Web site of the California Office of Privacy Protection (www.privacy.ca.gov) for additional information for California residents on protection against identity theft.

Form and Style of Notice

Make the notice clear, conspicuous and helpful.

1. Use plain, simple language, guiding subheads, and plenty of white space in the layout.

2. Avoid jargon or technical language.

Means of Notification

Individual Notice: Individually notify those affected whenever possible.

1. Send the notice by first-class mail.

2. As an alternative, notify by e-mail, if you normally communicate with the affected individuals by e-mail and you have received their prior consent to that form of notification, as required by the Electronic Signature Act.

Substitute Notice: If more than 500,000 individuals were affected, the cost of individual notification is more than $250,000, or you do not have adequate contact information on those affected, provide notice using public communication channels.

1. Post the notice conspicuously on your web site, AND

2.. Notify through major statewide media (television, radio, print), AND

3. Send the notice by e-mail to any affected party whose e-mail address you have, AND

4. E-mail a link to your web site notice to the California Office of Privacy Protection at privacy@scsa.ca.gov. California state agencies should contact the Office of Information Security at OIS.Security@state.ca.gov.

Notes

[1] The states without breach notice laws, as of July 2011, are AL, KY, NM and SD (National Conference of State Legislatures, "Security Breach Legislation 2011," www.ncsl.org/default.aspx?tabid=22295).

[2] The Health Information Technology for Economic and Clinical Health (HITECH) Act, for the HHS rule under section 13402, see www..hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html. For the FTC's rule under section 13407, see www2.ftc.gov/opa/2009/08/hbn.shtm.

[3] See the Environmental Protection Agency's Toxics Release Inventory at www..epa.gov/tri/.

[4] Ponemon Institute, *2010 Annual Study: U.S. Cost of a Data Breach*. Also see the Ponemon Institute's *Reputation Impact of a Data Breach (November 2011)*.

[5] California State Assembly Judiciary Committee Analysis of SB 1386 (June 18, 2002), at www.leginfo.ca.gov.

[6] Javelin Strategy & Research, 2011 Identity Fraud Survey Report (February 2011), at page 6.

[7] The 2011 Javelin Report found that 16.9% of respondents who had received a data breach notice in the past year were also victims of identity theft, while only 2.5% of non-recipients of notices, at page 47.

[8] See the research on medical identity theft by the World Privacy Forum, at www.worldprivacyforum.org.

[9] SB 541 of 2008 enacted Health and Safety Code §§ 1280.1, 1280.3 and 1280.15, which, among other things, sets fines and notification requirements for breaches of patient medical information and requires facilities to report such breaches to the California Department of Public Health. It authorizes the Department of Public Health to assess administrative penalties of $100 per day for failure to report a breach, to a maximum of $250,000.

[10] SB 24 of 2011.

[11] California Government Code § 11549.5(a).

[12] California Government Code § 11549.5(c).

[13] ISO/IEC 27001 is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is ISO/IEC 27001:2005-Information technology-Security techniques-Information security management systems-Requirements, but it is commonly known as "ISO 27001." It is intended to be used in conjunction with ISO/IEC 27002, the Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls.

[14] The State of California has adopted a policy requiring State agencies to encrypt confidential, senstivie and personal information on portable computing devices and portable storage media. See State Administratie Manual § 5345.2, available on the Government/Policy page at www.infosecurity.ca.gov.

[15] See California Civil Code § 1798.81.5.

[16] The encryption standard approved for U.S. Government organizations and others to protect higher-risk information is FIPS 197. For more information, see http://csrc.nist.gov/publications/PubsFIPS.html.

[17] See Special Publication 800-88, *Guidelines for Media Sanitization*, revised in September 2006

by the Computer Security Division of the National Institute of Standards and Technology, available at http://csrc.nist.gov/publications/PubsSPs.html.

[18] ISO/IEC 27001, cited in note 13 above, includes practices related to responding to and reporting security incidents and malfunctions "as quickly as possible."

[19] See suggestions on computer security incident response from the California Highway Patrol's Computer Crimes Investigations Unit at www.chp.ca.gov/programs/ccrime-incident.html.

[20] 15 U.S. Code § 7001 contains the requirements for consumer disclosure and consent to electronic notification, as required by California Civil Code §§ 1798.29(g)(2) and 1798.82(g)(2).

Appendix 1: Advisory Group

2003 Original Version

The following people provided consultation and advice to the California Office of Privacy Protection in the development of the original version of these Recommended Practices, issued in Ocotber 2003.

Brent Barnhart
Senior Counsel
Kaiser Foundation Health Plan, Inc.

Camille Busette
Senior Policy Manager
Intuit

Dianne Carpenter
Senior Attorney
J.C. Penney Corporation
California Retailers Association

James Clark
Senior Vice President
Government Relations
California Bankers Association

Mari Frank
Attorney, Privacy Consultant, and Author

Beth Givens
Director
Privacy Rights Clearinghouse

Roxanne Gould
Vice President,
CA Public and Legislative Affairs
American Electronics Association

Chief Kevin Green
California Highway Patrol

Craig Grivette
Deputy Secretary
California Business,
Transportation and Housing Agency

Tony Hadley
Vice President
Government Affairs
Experian

Gail Hillebrand
Senior Attorney
Consumers Union

Clark Kelso
Chief Information Officer
State of California

Barbara Lawler
Chief Privacy Officer
Hewlett-Packard

Fran Maier
Executive Director
TRUSTe

Dana Mitchell
Counsel to Rules Committee
California State Senate

Peter Neumann
Principal Scientist
Computer Science Lab
SRI International

Dr. Larry Ponemon
Chairman
Ponemon Institute

Debra Reiger
Chief Information Security Officer
State of California

Tim Shea
Legal Counsel
California Franchise Tax Board

Scott Shipman
Privacy Counsel
eBay

Preston Taylor
Consultant to
Assemblyman Joseph Simitian
California State Assembly

Tracey Thomas
Identity Theft Resource Center

Tom Timmons
President & CEO, Spectrum Bank
California Independent Bankers

2008 Revision

The Office of Privacy Protection was assisted in the May 2008 revision by advice from the following people.

Linda Ackerman
Staff Counsel
Privacy Activisim

Sharon Anolik
Director, Corporate Compliance and Ethics
Chief Privacy Officer
Blue Shield of California

Pam Dixon
Executive Director
World Privacy Forum

Mari Frank
Attorney, Privacy Consultant and Author

Beth Givens
Director
Privacy Rights Clearinghouse

Robert Herrell
Legislative Director
Assembly Member Dave Jones

Reece Hirsch
Sonnenschein, Nath & Rosenthal

Bobbie Holm
Chief, Policy Branch
California Office of HIPAA Implementation

Chris Hoofnagle
Senior Staff Attorney
Samuelson Law, Technology & Public Policy Clinic

Edward Howard
Howard Advocacy Inc.
for American Electronics Association

Dr. Rory Jaffe
Executive Director, Medical Services
University of California Office of the President

Saskia Kim
Principal Consultant
Senate Office of Research

Valerie Nera
Policy Advocate
California Chamber of Commerce

Lori Potter
Counsel, Legal and Government Relations
Kaiser Foundation Health Plan, Inc.

Appendix 2: Sample Notice Letter

Date:

Dear :

We are writing to you because of an incident at [*name of organization*]. *Describe what happened in general terms and give the date or approximate date of the incident. If the notice was delayed because of a law enforcement investigation, say so. State specifically what types of personal information were involved. Describe what you are doing in response.*

Tell people what they can do to protect themselves. What actions to recommend will depend on the type of information involved, in addition to name. Use the information from one or more on the following sections.

Social Security Number

Because your Social Security number was involved, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. Just call one of the three credit reporting agencies at a number below. This will let you automatically place an alert with all of the agencies. You will receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report from each.

Experian 1-888-397-3742 Equifax 1-800-525-6285 TransUnion 1-800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*If appropriate, also give the contact number for the law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically. You can keep the fraud alert in place by calling again after 90 days. For more information on identity theft, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov.

If there is anything that [*name of organization*] can do to assist you, please call us at [*toll-free phone number*].

California Driver's License or Identification Card Number

Since your California driver's license [or California Identification Card] number was involved, we recommend that you call the DMV Fraud Hotline at 1-866-658-5758 to report it.

Continue with above advice on placing a fraud alert on credit files.

Financial Account Number

To protect yourself from the possibility of identity theft., we recommend that you immediately contact [*credit card or financial account issuer*] at [*phone number*] 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 [*name of account issuer*] to give you a PIN or password. This will help control access to the account.

For more information on identity theft, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov.

If there is anything that [*name of organization*] can do to assist you, please call us at [*toll-free phone number*].

Medical Information or Health insurance Information (as defined)

If the breach does not include Social Security, driver's license/California Identification Card, or financial account numbers, say so. If it does include any of those numbers in addition to medical or health insurance information, then also include the information on what to do from the appropriate section(s) above.

We recommend that you regularly review the explanation of benefits statement that you receive from [*us, your plan, your insurer*]. If you see any service that you believe you did not receive, please contact [*us, your plan, your 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 request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. You can order your reports from the three credit reporting agencies for free each year by calling 1-877-322-8228 or going to www.annualcreditreport.com.

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. For information on your medical privacy rights, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov.

If there is anything that [*name of organization*] can do to assist you, please call us at [*toll-free number*].

Appendix 3: California Law on Notice of Security Breach

Summary of Basic Breach Notice Law

California Civil Code Section 1798.29 applies to state government agencies and Sections 1798.82 and 1798.84 apply to any person or business doing business in California. The main provisions are summarized below.

Security Breach

- Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.

Type of Information

- Unencrypted computerized data including certain personal information.
- Personal information that triggers the notice requirement is name (first name or initial and last name) plus any of the following:
  - Social Security number,
  - Driver's license or California Identification Card number,
  - Financial account number, credit or debit card number (along with any PIN or other access code where required for access to account),
  - Medical information, as defined, or
  - Health insurance information, as defined.

Whom to Notify

- Notice must be given to any data subjects who are California residents.
- A sample copy of a notice sent to more than 500 California residents must be provided to the Caifornia Attorney General.

When to Notify

- Timing: "in the most expedient time possible and without unreasonable delay." Time may be allowed for the following:
  - Legitimate needs of law enforcement if notification would impede a criminal investigation.
  - Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system.

How to Notify

- Notice may be provided to individuals in writing, electronically (as consistent with provisions of 15 U.S. Code 7001), or by substitute notice.
- Substitute notice may be used if the cost of providing individual notice is more than $250,000, more than 500,000 people would have to be notified, or the organization does not have sufficent contact information for those affected.
- Substitute notice means all of the following:
  - E-mail when the e-mail address is available, AND
  - Conspicuous posting on web site, AND
  - Notification of major statewide media, AND
  - Notification by e-mail of the California

Office of Privacy Protection or, for state agencies, the California Office of Information Security.

- Alternatively, a business or agency may use its own notification procedures as part of an information security policy, if its procedures are consistent with the timing requirements of the law and if it notifies subjects in accordance with its policy.

Text of California Civil Code Sections 1798.29, 1798.82, and 1798.84

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that is required to issue a security breach notification pursuant to this section 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. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the

Government Code.

(f) For purposes of this section, "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.

(g) For purposes of this section, "personal information" means an individual's first name or first initial and 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:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, 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.

(4) Medical information.

(5) Health insurance information.

(h) (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.

(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.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Internet Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of Information Security within the California Technology Agency.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.82. (a) Any person or business that conducts business in California, and 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 whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following:

(i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) Any person or business that is required to issue a security breach notification pursuant to this section 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. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means an individual's first name or

first initial and 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:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, 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.

(4) Medical information.

(5) Health insurance information.

(i) (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.

(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.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media and the Office of Privacy Protection within the State and Consumer Services Agency.

(k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Appendix 4: California Law on Health Facilities Breach

Summary of Health Facilities Breach Notice Law

California Health and Safety Code Section 1280.15 requires certain licensed health facilities to prevent unlawful or unauthorized access to, or use or disclosure of, a patient's medical information. It sets fines and notification requirements for breaches of patient medical information and requires facilities to report such breaches to the California Department of Public Health.

Breach

- Unlawful or unauthorized access to, and use or disclosure of, patients' medical information, as defined in Civil Code section 56.05.

Type of Information

- Individually identifiable information in possession of or derived from a health care provider, plan or other specified entity, regarding a patient's medical history, mental or physical condition or treatment.

Whom to Notify

- California Department of Public Health.
- Affected patients or their representatives.

When to Notify

- Notify no later than five days after detection of the incident.

Text of California Health and Safety Code Section 1280.15

1280.15. (a) A clinic, health facility, home health agency, or hospice licensed pursuant to Section 1204, 1250, 1725, or 1745 shall prevent unlawful or unauthorized access to, and use or disclosure of, patients' medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code and consistent with Section 130203. For purposes of this section, internal paper records, electronic mail, or facsimile transmissions inadvertently misdirected within the same facility or health care system within the course of coordinating care or delivering services shall not constitute unauthorized access to, or use or disclosure of, a patient's medical information. The department, after investigation, may assess an administrative penalty for a violation of this section of up to twenty-five thousand dollars ($25,000) per patient whose medical information was unlawfully or without authorization accessed, used, or disclosed, and up to seventeen thousand five hundred dollars ($17,500) per subsequent occurrence of unlawful or unauthorized access, use, or disclosure of that patients' medical information. For purposes of the investigation, the department shall consider the clinic's, health facility's, agency's, or hospice's history of compliance with this section and other related state and federal statutes and regulations, the extent to which the facility detected violations and took preventative action to immediately correct and prevent past violations from recurring, and factors outside its control that restricted the facility's ability to comply with this section. The department shall have full discretion to consider all factors when determining the amount of an administrative penalty pursuant to this section.

(b) (1) A clinic, health facility, home health

agency, or hospice to which subdivision (a) applies shall report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the department no later than five business days after the unlawful or unauthorized access, use, or disclosure has been detected by the clinic, health facility, home health agency, or hospice.

(2) Subject to subdivision (c), a clinic, health facility, home health agency, or hospice shall also report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the affected patient or the patient's representative at the last known address, no later than five business days after the unlawful or unauthorized access, use, or disclosure has been detected by the clinic, health facility, home health agency, or hospice.

(c) (1) A clinic, health facility, home health agency, or hospice shall delay the reporting, as required pursuant to paragraph (2) of subdivision (b), of any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information beyond five business days if a law enforcement agency or official provides the clinic, health facility, home health agency, or hospice with a written or oral statement that compliance with the reporting requirements of paragraph (2) of subdivision (b) would likely impede the law enforcement agency's investigation that relates to the unlawful or unauthorized access to, and use or disclosure of, a patient's medical information and specifies a date upon which the delay shall end, not to exceed 60 days after a written request is made, or 30 days after an oral request is made. A law enforcement agency or official may request an extension of a delay based upon a written declaration that there exists a bona fide, ongoing, significant criminal investigation of serious wrongdoing relating to the unlawful or unauthorized access to, and use or disclosure of, a patient's medical information, that notification of patients will undermine the law enforcement agency's investigation, and that specifies a date upon which the delay shall end, not to exceed 60 days after the end of the original delay period.

(2) If the statement of the law enforcement agency or official is made orally, then the clinic, health facility, home health agency, or hospice shall do the following:

(A) Document the oral statement, including, but not limited to, the identity of the law enforcement agency or official making the oral statement and the date upon which the oral statement was made.

(B) Limit the delay in reporting the unlawful or unauthorized access to, or use or disclosure of, the patient's medical information to the date specified in the oral statement, not to exceed 30 calendar days from the date that the oral statement is made, unless a written statement that complies with the requirements of this subdivision is received during that time.

(3) A clinic, health facility, home health agency, or hospice shall submit a report that is delayed pursuant to this subdivision not later than five business days after the date designated as the end of the delay. (d) If a clinic, health facility, home health agency, or hospice to which subdivision (a) applies violates subdivision (b), the department may assess the licensee a penalty in the amount of one hundred dollars ($100) for each day that the unlawful or unauthorized access, use, or disclosure is not reported to the department or the affected patient, following the initial five-day period specified in subdivision (b). However, the total combined penalty assessed by the department under subdivision (a) and this subdivision shall not exceed two hundred fifty thousand dollars ($250,000) per reported event. For enforcement purposes, it shall be presumed that the facility did not notify the affected patient if the notification was not documented. This presumption may be rebutted by a licensee only if the licensee demonstrates, by a preponderance of the evidence, that the notification was made.

(e) In enforcing subdivisions (a) and (d), the department shall take into consideration the special circumstances of small and rural hospitals, as defined in Section 124840, and primary care clinics, as defined in subdivision (a) of Section 1204, in order to protect access to quality care in those hospitals and clinics. When assessing a penalty on a skilled nursing facility or other

facility subject to Section 1423, 1424, 1424.1, or 1424.5, the department shall issue only the higher of either a penalty for the violation of this section or a penalty for violation of Section 1423, 1424, 1424.1, or 1424.5, not both.

(f) All penalties collected by the department pursuant to this section, Sections 1280.1, 1280.3, and 1280.4, shall be deposited into the Internal Departmental Quality Improvement Account, which is hereby created within the Special Deposit Fund under Section 16370 of the Government Code. Upon appropriation by the Legislature, moneys in the account shall be expended for internal quality improvement activities in the Licensing and Certification Program.

(g) If the licensee disputes a determination by the department regarding a failure to prevent or failure to timely report unlawful or unauthorized access to, or use or disclosure of, patients' medical information, or the imposition of a penalty under this section, the licensee may, within 10 days of receipt of the penalty assessment, request a hearing pursuant to Section 131071. Penalties shall be paid when appeals have been exhausted and the penalty has been upheld.

(h) In lieu of disputing the determination of the department regarding a failure to prevent or failure to timely report unlawful or unauthorized access to, or use or disclosure of, patients' medical information, transmit to the department 75 percent of the total amount of the administrative penalty, for each violation, within 30 business days of receipt of the administrative penalty.

(i) Notwithstanding any other law, the department may refer violations of this section to the Office of Health Information Integrity for enforcement pursuant to Section 130303.

(j) For purposes of this section, the following definitions shall apply:

(1) "Reported event" means all breaches included in any single report that is made pursuant to subdivision (b), regardless of the number of breach events contained in the report.

(2) "Unauthorized" means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code) or any other statute or regulation governing the lawful access, use, or disclosure of medical information.

Text of California Civil Code Section 56.05

Civil Code 56.05...(g) "Medical information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

(h) "Patient" means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.

Appendix 5: Reporting to Law Enforcement

Law Enforcement Contacts for Computer Crimes

California High Technology Theft and Apprehension Program

This program funds five regional task forces staffed by investigators from local, state and federal law enforcement agencies who have received specialized training in the investigation of high technology crime and identity theft investigations. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or is the target of a criminal act.

Sacramento Valley Hi-Tech Crimes Task Force
Telephone: 916-874-3002
www.sachitechcops.org

Southern California High Tech Task Force
Telephone: 562-347-2601

Northern California Computer Crimes Task Force
Telephone: 707-253-4500
www.nc3tf.org

Rapid Enforcement Allied Computer Team (REACT)
Telephone: 408-282-2420
www.reacttf.org

Computer and Technology Crime High-Tech Response Team (CATCH)
Telephone: 858-737-7171
www.catchteam.org/

FBI

Field Offices: www.fbi.gov/contact-us/field
National Computer Crime Squad
Telephone: 202-324-9164
E-mail: nccs@fbi.gov
www.tscm.com/compcrim.html

U.S. Secret Service

Field Offices: www.secretservice.gov/field_offices.shtml

California Penal Code Definition of "Computer Crime"[1]

As defined by California Penal Code Section 502, subsection (c), a computer crime occurs when a person:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

[1]Other violations of California or federal law may also be involved in an incident of unauthorized acquisition of personal information. California laws that may be involved include identity theft (Penal Code § 530.5), theft (Penal Code § 484), and forgery (Penal Code § 470).

Appendix 6: Information Security Resources

Federal Trade Commission, "Financial Institutions and Customer Data: Complying with the Safeguards Rule," "Protecting Personal Information: A Guide for Business," and "Security Check: Reducing Risks to Your Computer Systems,"available at www.ftc.gov/bcp/menus/business/data.shtm.

U.S. Department of Health & Human Services, Office for Civil Rights, Summary of the HIPAA Security Rule, available at www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

ISO/IEC 27001, Information Technology - Security Techniques - Information Security Management systems - Requirements, available at www.iso.org.

ISO/IEC 27002, Information Technology - Security Techniques - Code of Practice for Information Security Management, available at www.iso.org.

National Institute for Standards and Technology (NIST) Computer Security Resource Center, available at www.csrc.nist.gov.

Payment Card Industry Data Security Standard, available at www.pcisecuritystandards.org.

SANS, "Top Cyber Security Risks," available at www.sans.org/top20.

U.S.-CERT, Cyber Security Tips, available at www.uscert.gov/cas/tips/index.html.