Tuesday, October 21
2:30 pm-4:00 pm

606 A Global Perspective on Data Security Breaches and Enforcement

Pamela Jones Harbour
Commissioner
Federal Trade Commission

Joanne McNabb
Chief, Office of Privacy Protection
California Office of Information Security & Privacy Protection

Lisa J. Sotto
Partner
Hunton & Williams

TJ Svensson
Assistant General Counsel, Global Privacy
Thomson Reuters

Law Enforcement Representative - TBA

Faculty Biographies

Pamela Jones Harbour

Pamela Jones Harbour was sworn in as a commissioner of the Federal Trade Commission on August 4, 2003. Her term expires in September 2009.

Ms. Harbour joined the FTC from Kaye Scholer LLP where she served as a partner in the litigation department handling antitrust matters. She counseled clients on Internet privacy, e-commerce, consumer protection, and a variety of competition-related matters. Prior to joining Kaye Scholer, Ms. Harbour was New York State deputy attorney general and chief of the office's 150-attorney Public Advocacy Division. During her term in the attorney general's office, she argued before the United States Supreme Court on behalf of 35 states in State Oil v. Khan, a landmark price-fixing case. She also successfully represented numerous states in New York v. Reebok, States v. Keds, and States v. Mitsubishi, each resulting in multimillion-dollar national consumer settlements. Among her most notable antitrust cases were New York v. May Department Stores, a successful anti-merger challenge, and States v. Primestar Partners, a consent judgment culminating a four-year multistate investigation of the cable television industry.

Ms. Harbour received her law degree from Indiana University School of Law, and a BM from Indiana University School of Music.

Joanne McNabb
Chief, Office of Privacy Protection
California Office of Information Security & Privacy Protection

Lisa J. Sotto

Lisa J. Sotto, a partner in the New York office of Hunton & Williams, LLP, heads the firm's privacy and information management practice. Ms. Sotto assists clients in identifying and managing risks associated with privacy and information security issues. She advises clients on GLB, HIPAA, COPPA, CAN-SPAM, and other US state and federal information privacy and security requirements (including state breach notification laws), as well as international data protection laws. During the past three years, Ms. Sotto has assisted clients on over 200 information security breaches, handling every aspect of the breach event including preparing individual notification letters, training call center personnel, and negotiating with state and federal regulatory agencies, credit card issuers, and credit reporting agencies.

Secretaries Ridge and Chertoff appointed Ms. Sotto as vice chair of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. She also serves as co-chair of the international privacy law committee of the New York State Bar Association and chair of the New York Privacy Officers Forum. Ms. Sotto has testified before Congress and Executive Branch agencies on privacy and data security issues. A routinely quoted source on the topic of privacy, Ms. Sotto has authored or been quoted in over 100 articles and publications. She was voted the world's leading privacy advisor in Computerworld's 2007 survey and was ranked "Band 1" by Chambers USA in the category of privacy and data security.

TJ Svensson

TJ Svensson works as assistant general counsel for the North American legal branch of Thomson Reuters' professional division. Among other duties, Mr. Svensson is responsible for matters concerning data privacy and he has served as chair of the company's executive privacy committee.

He joined the Thomson organization after spending twelve years as a litigator in private practice.

Mr. Svensson holds a dual law degree, from the University of Minnesota and the University of Uppsala, Sweden.

Federal Trade Commission

Association of Corporate Counsel Annual Meeting 2008
Session 606: A Global Perspective on
Data Security Breaches and Enforcement

October 21, 2008
Seattle, Washington

Pamela Jones Harbour, Commissioner
Federal Trade Commission

Protecting PERSONAL INFORMATION
A Guide for Business

FEDERAL TRADE COMMISSION

PROTECTING PERSONAL INFORMATION
A Guide for Business

Most companies keep sensitive personal information in their files—names, Social Security numbers, credit card, or other account data—that identifies customers or employees.

This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Given the cost of a security breach—losing your customers' trust and perhaps even defending yourself against a lawsuit—safeguarding personal information is just plain good business.

A sound data security plan is built on **5 key principles:**

1. **Take stock.** Know what personal information you have in your files and on your computers.
2. **Scale down.** Keep only what you need for your business.
3. **Lock it.** Protect the information that you keep.
4. **Pitch it.** Properly dispose of what you no longer need.
5. **Plan ahead.** Create a plan to respond to security incidents.

Use the checklists on the following pages to see how your company's practices measure up—and where changes are necessary.

1. TAKE STOCK. Know what personal information you have in your files and on your computers.

Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities. You can determine the best ways to secure the information only after you've traced how it flows.

- Inventory all computers, laptops, flash drives, disks, home computers, and other equipment to find out where your company stores sensitive data. Also inventory the information you have by type and location. Your file cabinets and computer systems are a start, but remember: your business receives personal information in a number of ways—through websites, from contractors, from call centers, and the like. What about information saved on laptops, employees' home computers, flash drives, and cell phones? No inventory is complete until you check everywhere sensitive data might be stored.
- Track personal information through your business by talking with your sales department, information technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of:
  - ***Who sends sensitive personal information to your business.*** Do you get it from customers? Credit card companies? Banks or other financial institutions? Credit bureaus? Other businesses?
  - ***How your business receives personal information.*** Does it come to your business through a website? By email? Through the mail? Is it transmitted through cash registers in stores?
  - ***What kind of information you collect at each entry point.*** Do you get credit card information online? Does your accounting department keep information about customers' checking accounts?
  - ***Where you keep the information you collect at each entry point.*** Is it in a central computer database? On individual laptops? On disks or tapes? In file cabinets? In branch offices? Do employees have files at home?
  - ***Who has—or could have—access to the information.*** Which of your employees has permission to access the information? Could anyone else get a hold of it? What about vendors who supply and update software you use to process credit card transactions? Contractors operating your call center?
- Different types of information present varying risks. Pay particular attention to how you keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft.

SECURITY CHECK

Question:

Are there laws that require my company to keep sensitive data secure?

Answer:

Yes. While you're taking stock of the data in your files, take stock of the law, too. Statutes like the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act may require you to provide reasonable security for sensitive information.

To find out more, visit ***www.ftc.gov/privacy***.

2. SCALE DOWN. Keep only what you need for your business.

If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it only as long as it's necessary.

- Use Social Security numbers only for required and lawful purposes—like reporting employee taxes. Don't use Social Security numbers unnecessarily—for example, as an employee or customer identification number, or because you've always done it.

SECURITY CHECK

Question:

We like to have accurate information about our customers, so we usually create a permanent file about all aspects of their transactions, including the information we collected from the magnetic stripe on their credit cards. Could this practice put their information at risk?

Answer:

Yes. Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not in your system, it can't be stolen by hackers. It's as simple as that.

- Don't keep customer credit card information unless you have a business need for it. For example, don't retain the account number and expiration date unless you have an essential business need to do so. Keeping this information—or keeping it longer than necessary—raises the risk that the information could be used to commit fraud or identity theft.
- Check the default settings on your software that reads customers' credit card numbers and processes the transactions. Sometimes it's preset to keep information permanently. Change the default setting to make sure you're not inadvertently keeping information you don't need.
- If you must keep information for business reasons or to comply with the law, develop a written records retention policy to identify what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when you no longer need it.

3. LOCK IT. Protect the information that you keep.

What's the best way to protect the sensitive personally identifying information you need to keep? It depends on the kind of information and how it's stored. The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers.

PHYSICAL SECURITY

Many data compromises happen the old-fashioned way—through lost or stolen paper documents. Often, the best defense is a locked door or an alert employee.

- Store paper documents or files, as well as CDs, floppy disks, zip drives, tapes, and backups containing personally identifiable information in a locked room or in a locked file cabinet. Limit access to employees with a legitimate business need. Control who has a key, and the number of keys.
- Require that files containing personally identifiable information be kept in locked file cabinets except when an employee is working on the file. Remind employees not to leave sensitive papers out on their desks when they are away from their workstations.
- Require employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building. Tell employees what to do and whom to call if they see an unfamiliar person on the premises.
- If you maintain offsite storage facilities, limit employee access to those with a legitimate business need. Know if and when someone accesses the storage site.
- If you ship sensitive information using outside carriers or contractors, encrypt the information and keep an inventory of the information being shipped. Also use an overnight shipping service that will allow you to track the delivery of your information.

ELECTRONIC SECURITY

Computer security isn't just the realm of your IT staff. Make it your business to understand the vulnerabilities of your computer system, and follow the advice of experts in the field.

General Network Security

- Identify the computers or servers where sensitive personal information is stored.
- Identify all connections to the computers where you store sensitive information. These may include the Internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, and wireless devices like inventory scanners or cell phones.

- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.
- Don't store sensitive consumer data on any computer with an Internet connection unless it's essential for conducting your business.
- Encrypt sensitive information that you send to third parties over public networks (like the Internet), and consider encrypting sensitive information that is stored on your computer network or on disks or portable storage devices used by your employees. Consider also encrypting email transmissions within your business if they contain personally identifying information.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on servers on your network.
- Check expert websites (such as ***www.sans.org***) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems.
- Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- When you receive or transmit credit card information or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.

Question:

We encrypt financial data customers submit on our website. But once we receive it, we decrypt it and email it over the Internet to our branch offices in regular text. Is there a safer practice?

Answer:

Yes. Regular email is not a secure method for sending sensitive data. The better practice is to encrypt any transmission that contains information that could be used by fraudsters or ID thieves.

- Pay particular attention to the security of your web applications—the software used to give information to visitors to your website and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks. In one variation called an "injection attack," a hacker inserts malicious commands into what looks like a legitimate request for information. Once in your system, hackers transfer sensitive information from your network to their computers. Relatively simple defenses against these attacks are available from a variety of sources.

Password Management

- Control access to sensitive information by requiring that employees use "strong" passwords. Tech security experts say the longer the password, the better. Because simple passwords—like common dictionary words—can be guessed easily, insist that employees choose passwords with a mix of letters, numbers, and characters. Require an employee's user name and password to be different, and require frequent changes in passwords.
- Explain to employees why it's against company policy to share their passwords or post them near their workstations.
- Use password-activated screen savers to lock employee computers after a period of inactivity.
- Lock out users who don't enter the correct password within a designated number of log-on attempts.

SECURITY CHECK

Question:

Our account staff needs access to our database of customer financial information. To make it easier to remember, we just use our company name as the password. Could that create a security problem?

Answer:

Yes. Hackers will first try words like "password," your company name, the software's default password, and other easy-to-guess choices. They'll also use programs that run through common English words and dates. To make it harder for them to crack your system, select strong passwords—the longer, the better—that use a combination of letters, symbols, and numbers. And change passwords often.

- Warn employees about possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.
- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
- Caution employees against transmitting sensitive personally identifying data—Social Security numbers, passwords, account information—via email. Unencrypted email is not a secure way to transmit any information.

Laptop Security

- Restrict the use of laptops to those employees who need them to perform their jobs.
- Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a "wiping" program that overwrites data on the laptop. Deleting files using standard keyboard commands isn't sufficient because data may remain on the laptop's hard drive. Wiping programs are available at most office supply stores.
- Require employees to store laptops in a secure place. Even when laptops are in use, consider using cords and locks to secure laptops to employees' desks.

- Consider allowing laptop users only to access sensitive information, but not to store the information on their laptops. Under this approach, the information is stored on a secure central computer and the laptops function as terminals that display information from the central computer, but do not store it. The information could be further protected by requiring the use of a token, "smart card," thumb print, or other biometric—as well as a password—to access the central computer.
- If a laptop contains sensitive data, encrypt it and configure it so users can't download any software or change the security settings without approval from your IT specialists. Consider adding an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet.
- Train employees to be mindful of security when they're on the road. They should never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security. If someone must leave a laptop in a car, it should be locked in a trunk. Everyone who goes through airport security should keep an eye on their laptop as it goes on the belt.

Firewalls

- Use a firewall to protect your computer from hacker attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.
- Determine whether you should install a "border" firewall where your network connects to the Internet. A border firewall separates your network from the Internet and may prevent an attacker from gaining access to a computer on the network where you store sensitive information. Set "access controls"—settings that determine who gets through the firewall and what they will be allowed to see—to allow only trusted employees with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, review them periodically.
- If some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information.

Wireless and Remote Access

- Determine if you use wireless devices like inventory scanners or cell phones to connect to your computer network or to transmit sensitive information.
- If you do, consider limiting who can use a wireless connection to access your computer network. You can make it harder for an intruder to access the network by limiting the wireless devices that can connect to your network.
- Better still, consider encryption to make it more difficult for an intruder to read the content. Encrypting transmissions from wireless devices to your computer network may prevent an intruder from gaining access through a process called "spoofing"—impersonating one of your computers to get access to your network.
- Consider using encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases.

Detecting Breaches

- To detect network breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.
- Maintain central log files of security-related information to monitor activity on your network so that you can spot and respond to attacks. If there is an attack on your network, the log will provide information that can identify the computers that have been compromised.

- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from your system to an unknown user. If large amounts of information are being transmitted from your network, investigate to make sure the transmission is authorized.
- Have in place and implement a breach response plan. See pages 22–23 for more information.

EMPLOYEE TRAINING

Your data security plan may look great on paper, but it's only as strong as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance you place on meaningful data security practices. A well-trained workforce is the best defense against identity theft and data breaches.

- Check references or do background checks before hiring employees who will have access to sensitive data.
- Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by your company's data security plan is an essential part of their duties. Regularly remind employees of your company's policy—and any legal requirement—to keep customer information secure and confidential.
- Know which employees have access to consumers' sensitive personally identifying information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a "need to know."
- Have a procedure in place for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out routine.

SECURITY CHECK

Question:

I'm not really a "tech" type. Are there steps our computer people can take to protect our system from common hack attacks?

Answer:

Yes. There are relatively simple fixes to protect your computers from some of the most common vulnerabilities. For example, a threat called an "SQL injection attack" can give fraudsters access to sensitive data on your system, but can be thwarted with a simple change to your computer. Bookmark the websites of groups like the Open Web Application Security Project, ***www.owasp.org***, or SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities, ***www.sans.org/top20***, for up-to-date information on the latest threats—and fixes. And check with your software vendors for patches that address new vulnerabilities.

- Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. Make sure training includes employees at satellite offices, temporary help, and seasonal workers. If employees don't attend, consider blocking their access to the network.
- Train employees to recognize security threats. Tell them how to report suspicious activity and publicly reward employees who alert you to vulnerabilities.

- Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate. Make sure your policies cover employees who telecommute or access sensitive data from home or an offsite location.
- Warn employees about phone phishing. Train them to be suspicious of unknown callers claiming to need account numbers to process an order or asking for customer or employee contact information. Make it office policy to double-check by contacting the company using a phone number you know is genuine.
- Require employees to notify you immediately if there is a potential security breach, such as a lost or stolen laptop.
- Impose disciplinary measures for security policy violations.
- For computer security tips, tutorials, and quizzes for everyone on your staff, visit ***www.OnGuardOnline.gov***.

SECURITY PRACTICES OF CONTRACTORS AND SERVICE PROVIDERS

Your company's security practices depend on the people who implement them, including contractors and service providers.

- Before you outsource any of your business functions—payroll, web hosting, customer call center operations, data processing, or the like—investigate the company's data security practices and compare their standards to yours. If possible, visit their facilities.
- Address security issues for the type of data your service providers handle in your contract with them.
- Insist that your service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of your data.

4. PITCH IT. Properly dispose of what you no longer need.

What looks like a sack of trash to you can be a gold mine for an identity thief. Leaving credit card receipts or papers or CDs with personally identifying information in a dumpster facilitates fraud and exposes consumers to the risk of identity theft. By properly disposing of sensitive information, you ensure that it cannot be read or reconstructed.

- Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to—or use of—personally identifying information. Reasonable measures for your operation are based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

SECURITY CHECK

Question:

My company collects credit applications from customers. The form requires them to give us lots of financial information. Once we're finished with the applications, we're careful to throw them away. Is that sufficient?

Answer:

No. Have a policy in place to ensure that sensitive paperwork is unreadable before you throw it away. Burn it, shred it, or pulverize it to make sure identity thieves can't steal it from your trash.

- Effectively dispose of paper records by shredding, burning, or pulverizing them before discarding. Make shredders available throughout the workplace, including next to the photocopier.
- When disposing of old computers and portable storage devices, use wipe utility programs. They're inexpensive and can provide better results by overwriting the entire hard drive so that the files are no longer recoverable. Deleting files using the keyboard or mouse commands usually isn't sufficient because the files may continue to exist on the computer's hard drive and could be retrieved easily.
- Make sure employees who work from home follow the same procedures for disposing of sensitive documents and old computers and portable storage devices.
- If you use consumer credit reports for a business purpose, you may be subject to the FTC's Disposal Rule. For more information, see *Disposing of Consumer Report Information? New Rule Tells How* at ***www.ftc.gov/privacy*** (click on Credit Reporting, Business Guidance).

SECURITY CHECK

Question:

I own a small business. Aren't these precautions going to cost me a mint to implement?

Answer:

No. There's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers. Some of the most effective security measures—using strong passwords, locking up sensitive paperwork, training your staff, etc.—will cost you next to nothing and you'll find free or low-cost security tools at non-profit websites dedicated to data security. Furthermore, it's cheaper in the long run to invest in better data security than to lose the goodwill of your customers, defend yourself in legal actions, and face other possible consequences of a data breach.

5. PLAN AHEAD. Create a plan for responding to security incidents.

Taking steps to protect data in your possession can go a long way toward preventing a security breach. Nevertheless, breaches can happen. Here's how you can reduce the impact on your business, your employees, and your customers:

- Have a plan in place to respond to security incidents. Designate a senior member of your staff to coordinate and implement the response plan.
- If a computer is compromised, disconnect it immediately from the Internet.
- Investigate security incidents immediately and take steps to close off existing vulnerabilities or threats to personal information.
- Consider whom to notify in the event of an incident, both inside and outside your organization. You may need to notify consumers, law enforcement, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, many states and the federal bank regulatory agencies have laws or guidelines addressing data breaches. Consult your attorney.

ADDITIONAL RESOURCES

These websites and publications have more information on securing sensitive data:

- **National Institute of Standards and Technology (NIST)'s Computer Security Resource Center**
  www.csrc.nist.gov
- **NIST's Risk Management Guide for Information Technology Systems**
  www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- **Department of Homeland Security's National Strategy to Secure Cyberspace**
  www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
- **SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities**
  www.sans.org/top20
- **United States Computer Emergency Readiness Team (US-CERT)**
  www.us-cert.gov
- **Carnegie Mellon Software Engineering Institute's CERT Coordination Center**
  www.cert.org/other_sources
- **Center for Internet Security (CIS)**
  www.cisecurity.org
- **The Open Web Application Security Project**
  www.owasp.org
- **Institute for Security Technology Studies**
  www.ists.dartmouth.edu
- **OnGuard Online**
  www.OnGuardOnline.gov

ACC Association of Corporate Counsel

ACC Annual Meeting

Information Security Breaches

By in-house counsel for in-house counsel℠

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-22 | Seattle, WA | am.acc.com

ACC Association of Corporate Counsel

Information Security Breaches

- In the U.S., 2005 was the year of the security breach
  - Followed by 2006, 2007 and 2008 . . .
- Since 2005, over 1,000 information security breaches
  - ChoicePoint
  - Bank of America
  - Lexis Nexis
  - DSW
  - Card Systems
  - Boston Globe
  - Veterans Administration
  - TJX
- Over 236 million records potentially affected
- Over 40 U.S. jurisdictions have security breach notification laws
  - California SB 1386 started the trend
- Numerous federal bills

Information Security Breaches

- The term "security breach" defines a broad range of activities
  - Lost and stolen laptops
  - Unintentional employee misuse of data
  - Employee espionage
  - Vendor unauthorized use of data
  - External intrusions
    - Small attacks
    - Massive, organized attacks

Recent FTC Enforcement Actions

- FTC enforcement authority: Section 5 of the FTC Act
- Most FTC privacy enforcement actions result from security breaches
  - Card Systems
  - ChoicePoint
  - DSW
  - BJ's Wholesale Club
  - Petco
  - Tower Records
  - Barnes & Noble.com
  - Guess.com, Inc.
- Division of Privacy and Identity Protection
- Enforcement trends

U.S. Requirements: State Security Breach Notification Laws

- Generally, the duty to notify arises when unencrypted computerized "personal information" was acquired or accessed by an unauthorized person
- "Personal information" typically is an individual's name, combined with:
  - SSN
  - driver's license or state ID card number
  - account, credit or debit card number, along with password or access code
- But state laws differ:
  - Computerized v. paper data
  - Definition of PI
  - Notification to state agencies
  - Notification to CRAs
  - Timing of individual notification
  - Harm threshold
  - Content of notification letter

What if a Breach Occurs?

- Critical Question: Does the event trigger notification to individuals?
  - State breach notification laws generally mandate disclosure if PI was "acquired" or "accessed" by "unauthorized" person
  - Is expert evaluation needed to answer this question?
- Service provider obligations

Who are the Stakeholders?

- Recognize the potential stakeholders
  - Board of Directors/senior management
  - Law enforcement
  - Financial markets
  - Affected individuals
  - Employees
  - Shareholders
  - Regulators
  - Auditors
  - Public

Notification

- Individual notification - Letters must be written with five primary constituencies in mind:
  - Regulators
  - Plaintiffs' lawyers
  - Impacted individuals
  - Public at large/media
  - Employees
- If you notify in one jurisdiction, notify in all jurisdictions (including foreign)
  - Overseas notification standards
- Standard offerings to affected individuals

Timing of Notification

- If breach notification laws are triggered, when do you notify?
  - As soon as possible
    - Except in some states
  - Exceptions
    - Investigation and restoration
    - Law enforcement delay
  - If you rely on exceptions, document the basis for delay

The Notice

- Plain language notice – describe:
  - The event (but not in MA)
  - Personal information involved
  - Steps taken to protect against further unauthorized acquisition
  - How company will assist affected individuals
  - Guidance on how individuals can protect themselves from identity theft or account fraud
- Need substantial pre-mailing plan
  - Press statement and related PR
  - Call center set-up, scripts/FAQs and training, then monitoring
  - Website materials
  - Credit monitoring arrangement
  - Investor relations

Other Interested Parties

- Consumer reporting agencies
- Payment card companies
  - Consider contractual obligations
  - File an incident report
  - Conduct an audit
- Regulatory agencies
  - FTC and other relevant federal regulators
  - State agencies – HI, MA, MD, ME, NC, NH, NJ, NY, PR, SC, VA
  - Non-U.S. regulators

EU Data Breach Notification

- Under the Directive, data controllers must ensure appropriate security of personal data they maintain
- But there is no general legal obligation (yet) to report breaches to EU residents or regulators
- UK's ICO "believes serious breaches should be brought to the attention of his Office"

Recent UK Data Breaches

- UK government department (HMCR) lost 2 CDs with unencrypted data on 25 million UK child benefit recipients
- U.S. contractor lost data on 3 million U.K. learner drivers
- FSA fined Norwich Union $2.5 million for poor security screening that allowed fraudsters to divert funds
- UK's ICO was notified of over 100 breaches in less than one year – and there is no legal requirement to notify of breaches

Proposed Breach Notification Revisions to EU's E-Privacy Directive

- European Commission published a proposal to amend the E-Privacy Directive to create a duty to notify of data breaches
- As proposed, the notification obligation would apply primarily to ISP and network operators
- Notification would be required where there is a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data"
- Notification would need to be made "without undue delay" to:
  - "Subscribers" of the relevant electronic communication service, and
  - The appropriate national regulatory authority (e.g., DPA or other competent agency)

Canada

- Ontario's health privacy law contains a breach notification requirement
- There is no other breach notification law in Canada
- But there is a pending proposal to amend PIPEDA to include a breach notification requirement
- In addition, the OPC has issued federal data breach guidelines
- Investigations by the Canadian DPA's (federal and provincial) are rampant

Breach Notification Around the Globe

- Japan
- New Zealand
  - Guidelines "encourage" voluntary notification to affected individuals
- South Korea
  - New omnibus privacy law coming later this year will include breach notification requirements

Lessons Learned

- Prevention is the primary goal, but proactive planning can minimize impact if breach occurs
- Concern and focus on data security must come from the top
- Data breaches often must involve the CEO, CFO, CPO, CIO and GC
- Re-evaluate security systems and policies on an ongoing basis
- Integrate the concern for information security as a core value and train often

New York Law Journal
INVESTIGATIONS
&
COMPUTER FORENSICS

Tuesday, May 29, 2007

ALM

Data Breach!

Correct Response Crucial

BY LISA J. SOTTO,
JOHN W. WOODS JR.
AND JOHN J. DELIONADO

THE THREAT TO CORPORATE networks, and the information contained on those networks, has never been greater. While 15, or even five, years ago the compromise of computer data would likely have been the work of a lone hacker or disgruntled insider, there are increasing signs that these events are often the work of complex criminal organizations. The need for sophisticated professionals knowledgeable in the legal issues surrounding these events has increased.

Most individuals familiar with these events understand that a breach involving the compromise of personal data will trigger state laws requiring notification to affected individuals. For lawyers, however, these events pose a myriad of additional competing and important legal issues. Of critical importance is how a company handles a compromise event. The actions it takes in the first days after learning of an event can have a profound effect, including the possibility of litigation, government scrutiny, negative public attention and the erosion of the organization's customer base.

Lisa J. Sotto *is a partner in the New York office of Hunton & Williams,* **John W. Woods, Jr.** *is a partner in the firm's Washington, D.C. and Richmond, Va. offices, and* **John J. Delionado** *is an associate in the firm's Miami office.*

ART BY NEWSCOM

The threat to corporate networks, and the information they contain, has never been greater.

Companies must recognize that a data breach requires actions that go well beyond simple compliance with state breach notification laws. Some of the issues about which a business may need legal advice are:

(1) conducting an investigation into the event;

(2) notifying auditors and the securities regulators;

(3) notifying law enforcement authorities;

(4) notifying contracting parties (such as payment card issuers);

(5) notifying regulatory agencies with oversight authority or consumer regulatory bodies; and

(6) notifying the public.

Investigating the Event

Given the issues that can arise, understanding the factual contours of the event are critically important. Most importantly, companies must recognize that upon discovery of an issue, the event should not be handled like just another problem for the Information Technology (IT) department.

Ignoring the threat is not an option, but it may be equally dangerous to engage the problem with inadequate resources. The most important step is for a company to retain a qualified network security consultant to conduct an investigation overseen by legal counsel. The structure of the engagement of outside experts in these events is critical, and these experts must be focused on conducting the investigation in a way that will best assist the company.

Many businesses have sophisticated counsel who are well versed in the litigation process and may have the ability to direct consultants and determine the source of the compromise. A word of caution, however.

Corporate counsel generally engage in a variety of functions within a company and often make or assist in its business decisions. This dual role of corporate counsel may serve to unravel what might have been a privileged internal investigation. Engaging and obtaining the advice of litigation counsel will best serve a company in such a situation since it provides to it the best chance to preserve available privileges. Legal privileges are hard to come by, and easy to lose.

Privilege extends to communications between a company and outside legal counsel. Courts also protect as "work product" any material prepared by a party or its attorneys or other representatives in anticipation of litigation.[1] Where an internal investigation is undertaken and experts are used, *United States v. Kovel*[2] provides the benchmark standard and must be considered by counsel. Courts have routinely applied the *Kovel* test to third party consultants ranging from accountants to patent consultants.[3] Where privilege has been properly protected, the work-product doctrine will extend to materials prepared for counsel by the consultants.[4]

A company must keep in mind that whatever is determined in the investigation, even where privilege is successfully protected, privilege "only protects disclosure of communications; [not] underlying facts[.]"[5] What will be protected by privilege in the event it is preserved are the judgments, strategy and recommendations by counsel and counsel's agent, the expert consultants.

Devoting proper attention to a breach event is a company's best chance to limit or, in some instances, avoid entirely any damage to itself. Taking all reasonably possible steps to preserve the privilege is fundamental when dealing with a breach, regardless of whether there was a compromise of personal information. How forensic experts are retained to go about the task at hand and who directs them can mean the difference between creating a valuable privileged engagement that can benefit a company versus a road map to would-be litigants and government regulators that documents a company's darkest hour.

After taking all prudent steps to best preserve privilege, the internal investigation must focus first on the nature of the compromise and how it occurred. Given that the response must begin immediately to determine the source and scope of the compromise, it is often necessary, or at least expedient, to have the outside consultant obtain information from a trusted internal IT professional within the company. As with any highly confidential and significant event, it is prudent to keep the circle of people circumscribed.

Inform Senior Management

The compromise of personal data has become a boardroom event.

The scope of the breach and the effect that it can have on a company may be an event that affects the corporate public profile and possibly its stock price in the event the company is publicly traded. Since a data compromise can have such a wide-ranging and significant impact, company management must be kept abreast of the information developed during the investigation, and particularly any significant revelations.

What the decision-makers in the organization must be informed of immediately is the security posture of the network and whether there has been compliance with relevant industry standards. In addition, a company needs to review whether it has followed its own information security policies and procedures.

Where an event is significant enough that the business' independent auditors must be informed, the auditors will undoubtedly seek answers to many hard questions. Auditors will focus on the findings resulting from the investigation as well as the methodology used in evaluating the event. They will also scrutinize the quality of the investigation and what it revealed.

For a publicly traded company, the decision-makers will need to evaluate whether a disclosure is warranted. Trusted securities counsel is essential to this process and should be engaged from the outset of the investigation to assist in making this critical determination.

Involving Law Enforcement

A compromise event is very often the work of criminals and not simply the result of negligence. Federal law enforcement has become increasing sophisticated and has developed the tools to identify and arrest those who commit criminal acts against a victim company.

The U.S. Secret Service has had great success with the Electronic Crimes Task Force that has been developed and flourished in many of the Service's large field offices and headquarters in Washington, D.C. This task force allies itself with state and local law enforcement as well to ensure that the best resources are brought to bear. Similarly, the Federal Bureau of Investigation has grown its crack Computer Analysis and Response Team and has had significant success combating computer crime.

Along with the Secret Service and the FBI, the U.S. Department of Justice (DOJ) now has a group of experienced and knowledgeable prosecutors to combat computer crime. At DOJ headquarters, there is now a group of trial attorneys in the Computer Crimes and Intellectual Property Section devoted to investigating and prosecuting computer crimes throughout the country. Further, many of the large U.S. Attorney's offices have sophisticated

Assistant U.S. Attorneys designated as computer and telecommunications coordinators experienced in investigating and litigating complex computer crimes.

The Computer Fraud and Abuse Act (CFAA) is the primary federal criminal statute that addresses computer crimes.[6] Potential criminal liability attaches when someone intentionally accesses a computer without authorization, typically known as an outside hack, or when someone exceeds authorized access.

In investigating crimes, law enforcement has the power and ability to go beyond the limitations of an internal investigation. Investigative techniques can include grand jury subpoenas, search warrants, Pen Registers (surveillance devices), Electronic Communications and Privacy Act warrants (which are essentially search warrants aimed at a user's account with an Internet service provider), and even Title III wire interceptions. Generally, any hope of catching the individual or group responsible for criminal conduct against a company depends on allowing law enforcement the time and ability to use the techniques available to it.

The state breach notification laws actually encourage companies to notify law enforcement by allowing a cooperating company to delay public notification in order to allow law enforcement to conduct a confidential investigation (assuming law enforcement agrees that a delay in notification would assist in its investigation). At least one state, New Jersey, has made notification to law enforcement a condition precedent to notifying affected individuals.

Notifying Contracting Parties

A company must evaluate whether it has contractual obligations to notify significant business partners of the compromise event.

Where payment cards are involved, the terms of the contract often require consultation with the card issuers in the event of a security breach. Where such obligation exists, the notification should be accomplished as soon as possible. Typically, a company will reveal the relevant facts discovered through its investigation, but not the privileged opinions of counsel or the experts.

Depending on the contract, the notice may need to take the form of a formal incident report filed with the card company. Further, card companies may require an independent audit by a data security firm conducted on their behalf and funded by the company that experienced the breach.

Contacting Regulators

Any company that is within a regulated industry will need to consult counsel about whether the entity regulating it must be informed.

There are strict guidelines, for instance, where a federally insured financial institution is involved since there is oversight by Federal Depository Insurance Company, the Office of the Comptroller of Currency, or the Federal Reserve. Compromise events, however, draw regulatory scrutiny even where a company is not federally regulated.

The Federal Trade Commission (FTC) has enforcement authority in the privacy arena pursuant to Section 5 of the FTC Act,[7] which prohibits unfair or deceptive trade practices. The FTC has demonstrated its commitment to investigate data breach events as it recently established a new division of Privacy and Identity Protection. The FTC looks to whether a company has failed to take appropriate action to protect personal information of individuals and, thus, constitutes an unfair or deceptive trade practice.

The FTC has focused its enforcement actions pursuant to Section 5 on security breaches. Notifying the FTC of the event and framing the circumstances can greatly assist a company in avoiding an enforcement action, rather than taking a more passive approach whereby the FTC may learn of the event through information in the public realm that may be rife with inaccuracies and hearsay.

Letting the Public Know

California was the first state to pass a law requiring organizations to notify affected citizens where their personal information was compromised.

As these compromise events came to light with some frequency in 2005 and garnered significant attention from the media and lawmakers, approximately 35 other states, plus New York City, Washington, D.C. and Puerto Rico, have enacted similar notification laws. At the state level, the duty to notify individuals affected by a breach generally arises when there is a reasonable belief that computerized sensitive personal information has been acquired or accessed by an unauthorized person in an accessible form.

State laws typically define "personal information" to include an individual's first name or first initial and last name, combined with one of the following: (a) a Social Security number; (b) a driver's license or state identification card number; or (c) a financial account, credit or debit card number, along with a required password or access code.

Where notification is required, it generally must be done in the most expedient time possible and without unreasonable delay. Companies are generally given time to investigate the event and, as discussed above, may be able to delay notification where they have notified law enforcement. In several states, however, including Florida, Ohio and Wisconsin, notification is required within 45 days of the date the incident was discovered.

Conclusion

Companies that are afflicted with a data breach cannot give such an event short shrift. As these events have become more widespread, public and government scrutiny over a company's handling of a breach event have increased. It is essential that victim companies take all prudent steps to prevent becoming further victimized in the legal courts or the courts of public opinion.

A company so afflicted must prepare to address the problem in a well-organized and meticulous manner, led by a team of sophisticated professionals able to recognize the myriad issues confronting the company. Recognizing that such a situation is front page news and not a back room event is the first step toward surviving the crisis and getting back to (successful) business as usual.

1. See generally *Hickman v. Taylor*, 329 U.S. 495 (1947).
2. *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).
3. See, e.g., *In re Grand Jury Proceedings Under Seal*, 947 F. 2d 1188 (4th Cir. 1991) (finding privilege applied to communication with accountant where communication was "made for the purpose of facilitating the rendition of legal services covered by the privilege").
4. See *United States v. Nobles*, 422 U.S. 225, 239 (1975).
5. *Upjohn Co. v. United States*, 449 U.S. 383, 395 (1981).
6. 18 U.S.C. §1030.
7. 15 U.S.C. §45.

BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Since 2005, there have been reports of over 500 U.S. security breaches. Proactive incident response planning can help minimize the impact when and if a breach occurs. The authors provide advice on responding to and managing a data breach, including information on state law variations, relevant stakeholders, and tips on actual notification.

A How-To Guide to Information Security Breaches

By Lisa J. Sotto and Aaron P. Simpson

Contrary to what the headlines suggest, information security breaches are not a new phenomena. What is new is that we are hearing about them in record numbers. While consumers are newly focused on information security due to the emergence of e-commerce, the reason security breaches now seem ubiquitous is a result of the development of a body of state laws requiring companies to notify affected individuals in the event of a breach. The differing requirements of over 35 state security breach notification laws make legal compliance a challenge for organizations operating on a national level.

Lisa Sotto heads the Privacy and Information Management Practice at Hunton & Williams LLP and is a partner in the New York office. She is also vice chairperson of the DHS Data Privacy and Integrity Advisory Committee. Sotto may be contacted at lsotto@hunton.com. Aaron P. Simpson is an associate in the Privacy and Information Management Practice at Hunton & Williams, New York. He may be contacted at asimpson@hunton.com.

Background

Since 2005, there have been reports of over 500 security breaches, many of which have involved the most respected organizations in the United States.[1] In fact, the number of reported incidents does not begin to define the actual number of breaches that have occurred in the United States during the past two years. From universities to government agencies to Fortune 500 companies, no industry sector has been spared. These breaches have run the gamut from lost backup tapes and laptops, to hacking incidents, to organized crime. The reported breaches are estimated to have exposed personal information contained in over 100 million records. Consequently, a significant percentage of the American public has received notification that the security of their personal information has been breached. Indeed, it seems that hardly a day goes by without a new press report of a significant security breach.

[1] *See* Privacy Rights Clearinghouse, "A Chronology of Data Breaches," available at http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited March 27, 2007).

 ISSN 1538-3423

State Security Breach Notification Laws

Public awareness was not focused in earnest on security breaches until 2005, fully two years after California enacted a law requiring organizations to notify affected Californians of a security breach.[2] At the time of enactment, few understood the enormous implications of that law. Since 2005, 35 other states, as well as New York City, Washington, D.C. and Puerto Rico, have jumped on the bandwagon and enacted breach notification laws of their own. In addition, numerous federal security breach bills have been proposed. With no clear frontrunner, it is hard to predict when a federal law might be passed, thought a federal preemptive law appears likely.

At the state level, the duty to notify individuals affected by a breach generally arises when there is a reasonable belief that unencrypted, computerized sensitive personal information has been acquired or accessed by an unauthorized person. Typically, the state laws define ''personal information'' to include an individual's first name or first initial and last name, combined with one of the three following data elements:

- Social Security number;
- driver's license or state identification card number, or
- financial account, credit or debit card number, along with a required password or access code.

Unfortunately, entities struggling with a potential breach must look beyond the language of the ''typical'' state law in the event of a national, or even multi-state, incident. The variations among state breach notification laws greatly complicates the legal analysis as to whether the breach laws are triggered with respect to a particular event. Because most breaches impact individuals in multiple jurisdictions, companies often must take a ''highest common denominator'' approach to achieve legal compliance.

Key areas of variation among state breach notification laws include:

- *Affected Media*: Under most state breach laws, notification is required only if ''computerized'' data has been accessed or acquired by an unauthorized individual. In some states, however, including North Carolina, Hawaii, Indiana and Wisconsin, organizations that suffer breaches involving paper records are required to notify affected individuals.
- *Definition of ''Personal Information''*: Breach notification laws in some states expand the definition of personal information to include data elements such as medical information (Arkansas, Puerto Rico), biometric data (Nebraska, North Carolina, Wisconsin), digital signatures (North Carolina, North Dakota), date of birth (North Dakota), employee identification number (North Dakota), mother's maiden name (North Dakota), and tribal identification card numbers (Wyoming).
- *Notification to State Agencies*: Many states require entities that have suffered a breach to notify state agencies. Currently, the states that require such notification include Hawaii, Maine, New Hampshire, New Jersey, New York, North Carolina and Puerto Rico. In Puerto Rico, organizations must notify the state government within ten days of detecting a breach. In New Jersey, the breach notification law requires entities to notify the state police prior to notifying affected individuals.
- *Notification to Credit Reporting Agencies*: While the threshold for notification differs among the state laws, many states require organizations that suffer a breach to notify the three national consumer reporting agencies (Equifax, Experian and Transunion). Among the states with this requirement, the state with the lowest threshold requires notification to the credit reporting agencies in the event 500 state residents must be notified in accordance with the notification requirement.
- *Timing of Notification to Affected Individuals*: Most state notification laws require notification to affected individuals within ''the most expedient time possible and without unreasonable delay.'' Some states, such as Ohio, Florida and Wisconsin, require notification within 45 days of discovering the breach.
- *Harm Threshold*: Some states (*e.g.*, Indiana, Michigan, Ohio, Rhode Island, Utah and Wisconsin) require notification of affected individuals only if there is a reasonable possibility of identity theft. Other states (*e.g.*, Colorado, Idaho, Kansas, Maine, New Hampshire, New Jersey and Vermont) do not require notification unless it has been determined that misuse of the information has occurred or is reasonably likely to occur. And in other states (*e.g.*, Arkansas, Florida, Hawaii and Louisiana) notification is not required unless there is a reasonable likelihood of harm to customers. For organizations that suffer multi-state security breaches, any harm threshold is irrelevant as a practical matter because many state breach notification laws do not contain such a threshold.

Federal Enforcement

In addition to the compliance maze at the state level, the Federal Trade Commission (FTC) has enforcement authority in the privacy arena pursuant to Section 5 of the FTC Act.[3] Section 5 of the FTC Act prohibits unfair or deceptive trade practices. The FTC recently has brought a number of enforcement actions pursuant to Section 5 stemming from security breaches. In fact, most of the enforcement actions brought by the FTC in the privacy arena have resulted from security issues. Some of the more noteworthy FTC enforcement actions stemming from security breaches have included those against BJ's Wholesale Club, CardSystems, ChoicePoint and DSW.

The CardSystems case highlights the significant reputational risk associated with privacy events generally, and security breaches in particular. In this case, over 40 million credit and debit card holders' information was accessed by hackers leading to millions of dollars in fraudulent purchases. In its enforcement action, the FTC alleged that the company's failure to take appropriate action to protect personal information about millions of consumers was tantamount to an unfair trade practice. As part of its settlement with the FTC, CardSystems agreed to implement a comprehensive information security program and conduct audits of the program biennially for 20 years. The real punishment, however, was the reputational damage the company suffered in the wake of the breach. Both Visa and Discover severed their relationship with CardSystems and the company ultimately was sold to an electronic payment company in Silicon Valley.

As our society becomes increasingly information-dependent, it is likely that there will be an increase in FTC enforcement associated with security breaches. In fact, in response to heightened consumer concern and an increased need for regulatory oversight in this arena, the FTC recently established a new division of Privacy and Identity Protection. This signals a new FTC focus on data privacy and security, along with what will likely be a concomitant increase in enforcement.

Managing a Data Breach

If a possible breach occurs, it is critical to determine as quickly as possible whether the event triggers a requirement to notify affected individuals. To make this determination, organizations must be able to answer the following questions:

1. *What information was involved?* Does the compromised information meet the definition of ''personal information'' under any of the state breach notification laws? As discussed above, certain states have adopted expansive definitions of ''personal information'' for purposes of their breach notification laws. These broader definitions must be considered in analyzing the information involved in the event.
2. *Was the information computerized?* In most states, only incidents involving computerized information require individual notification. But special attention should be paid to the laws in those states in which notification is required for incidents involving personal information in any form, including paper.
3. *Was the information encrypted?* Encryption is available as a safe harbor under every extant state security breach notification law. Importantly, all of the relevant laws are technology-neutral, meaning they do not prescribe specific encryption technology. If the information is maintained in an unreadable format, then it may be considered encrypted for purposes of the state breach laws. Encryption does not, however, include password-protection on equipment such as desktop computers, laptop computers and portable storage devices. As a result, many organizations have been required to notify affected individuals when laptop computers subject to password-protection have been lost or stolen.
4. *Is there a reasonable belief that personal information was accessed or acquired by an unauthorized person?* If an entity has a reasonable belief that the information was compromised by an unauthorized person, notification is required. Note that a number of state breach notification laws contain a harm threshold whereby notification is not required unless there is reasonable possibility of harm, misuse or identity theft (*see above*). Organizations should be wary of relying on harm thresholds, however, because they are not included in many state breach laws and thus may not be available in the event of a multi-state breach.

Because breaches come in all shapes and sizes, many of them require significant technical analysis to answer these questions. Organizations often must enlist the assistance of highly skilled forensic investigators to assist with the evaluation of their systems.

Recognize the Stakeholders

Once an organization has determined that the breach notification laws have been triggered, it is important to understand the panoply of stakeholders throughout the breach process. Depending on the type of organization involved, the potential universe of stakeholders is extensive and may include:

- *Affected individuals*: Individuals affected by a security breach are the primary focus for every organization during the notification process. Although the breach may not have occurred as a result of any misdeeds by the organization suffering the breach, in the eyes of consumers, employees and other affected individuals, the organization is responsible for the data it collects and maintains. As a result, regardless of the circumstances, an organization suffering a security breach should be appropriately helpful and respectful to individuals whose data may have been compromised.
- *Board of Directors/Senior Management*: Information security is no longer an area of a company that is relegated to the dusty basement. Front-page headlines and stock drops stemming from early security breaches made sure of that. It is often advisable to involve the Board of Directors (or its equivalent) and senior management soon after learning of a security breach affecting the organization.
- *Law Enforcement*: Depending on the nature of the event, it may be important to report the security breach to law enforcement authorities for purposes of conducting an investigation. The state security breach laws allow organizations to delay notifying affected individuals pending a law enforcement investigation. New Jersey's breach notification law makes it a legal requirement to notify law enforcement prior to notifying affected individuals.
- *State and Federal Regulators*: In addition to the laws' requirements to notify state regulators, organizations should give serious consideration to notifying the FTC in the event of a significant security breach. Proactively notifying the FTC, while not a legal requirement, provides an organization with the opportunity to frame the circumstances of the breach and provide appropriate context. Because the FTC will undoubtedly learn about every significant security breach, organizations are well-advised to tell the story themselves rather than have the FTC learn about the breach from unfavorable media reports.
- *Financial Markets*: For publicly-traded companies, some security breaches rise to the level of reportable events. In these cases, it may be necessary to notify the Securities and Exchange Commission and the relevant exchange of the breach.
- *Payment Card Issuers*: To the extent payment cards are involved, it is often essential to consult the card issuers as early as possible in the process. Organizations should review their contractual obligations with the card issuers because there are likely to be provisions relevant to a security breach. In addition, the card issuers may require organizations suffering breaches to file formal incident reports. Depending on the scope of the breach, the card issuers also may require that an

[2] Cal. Civ. Code § 1798.82 (2006).

[3] 15 U.S.C. § 45 (2005).

independent audit be conducted by their own auditors.

- *Employees*: In some cases, employees of the organization should be notified of an incident affecting customers. Many employees care deeply about the entity for which they work. To the extent the organization's reputation may be tarnished by the event, employees will not want to be left in the dark about the incident.
- *Shareholders*: Public companies that suffer breaches must consider their shareholders in the aftermath of a breach. The investor relations department should be mobilized in the event of a significant breach to respond to investors' concerns.
- *Auditors*: In some cases, security breaches may need to be reported to a company's auditors.
- *Public*: Security breaches often ignite the passions of the public at-large. In managing the process of notification, organizations should give careful consideration to the anticipated public response to the incident. In many cases, it is helpful to work with experienced public relations consultants. The risk to an organization's reputation stemming from a security breach far exceeds the risk associated with legal compliance. Thus, it is imperative in responding to a security breach to consider measures that will mitigate the harm to an organization's reputation.

Timing of Notification

Once the extent and scope of the incident have been defined and it is determined that notification is required, the next step is to notify affected individuals. Most state security breach laws require organizations that suffer a breach to notify affected individuals ''in the most expedient time possible and without unreasonable delay.'' In several states, notification is required within 45 days of the date the incident was discovered. Under both timeframes, the date of actual notification may be delayed by the exceptions available in most states for law enforcement investigations and restoring system security.

Pursuant to the law enforcement exception, notification may be delayed if a law enforcement agency determines that notification would impede a criminal investigation. Thus, if law enforcement has requested such a delay, the clock does not start ticking on notification until after the agency determines that notification will not compromise the investigation.

As to the exception for restoring system security, notification to affected individuals may be delayed to provide the affected organization time to take any security measures that are necessary to determine the scope of the breach and to restore the ''reasonable integrity of the system.'' Organizations should not take this exception lightly—notification to consumers of a system vulnerability may tip off copycat fraudsters to a system weakness they can exploit. Thus, prior to notifying affected individuals, it is essential for organizations suffering security breaches to restore the integrity of their systems.

Entities that rely on either the law enforcement or system security exception should document such reliance. In Hawaii, such documentation is a legal requirement.

Notification to Individuals

Letters to individuals notifying them of a possible compromise of their personal information should be simple, free of jargon and written in plain English. Entities would be well-advised to avoid legalistic phrases and any attempt to pin blame elsewhere. Organizations that have been most favorably reviewed by individuals following a breach are those that have accepted responsibility and provided useful information to recipients. (A breach notification letter is not the place for marketing!)

Organizations should keep in mind that, in addition to impacted individuals, the notification letter will likely be scrutinized by numerous interested parties, including regulators, plaintiffs' lawyers and the media. As a result, it is essential to strike the appropriate tone while at the same time providing a meaningful amount of substance.

There is a growing de facto standard, depending on the information breached, for the types of ''offerings'' companies are making to affected individuals in their notice letters. These offerings typically include:

- *Credit Monitoring*: In the event a Social Security number or some other form of identification that may contain a Social Security number (such as a driver's license number or a military identification card number) has been compromised, it has become standard to offer affected individuals one year of credit monitoring services. Depending on the size of the breach, this can be a significant cost for companies.
- *Free Credit Report*: Separate and apart from credit monitoring, organizations should inform affected U.S. individuals that they are entitled to one free credit report annually from each of the three national credit reporting agencies.
- *Fraud Alert*: Organizations also may want to recommend that affected individuals place a fraud alert on their credit file for additional protection. There is no charge for this service. Because fraud alerts can have a significant impact on a consumer's day-to-day purchase habits, most organizations simply suggest to consumers that this is an option rather than insist they take such action.

In addition to the standard offerings, the letter should describe the details of the security breach. For obvious reasons, these details should never include the specific affected payment card or Social Security numbers impacted by the breach. Instead of providing this detail, it is most effective to explain what happened and what the organization is doing to help individuals affected by the breach. In many cases, this means providing the individual with information about credit monitoring and other information about how they may protect themselves. Also, it may be necessary to establish a call center (with trained agents) to handle consumer response to the incident.

As a general rule, if an organization is required to notify in a few jurisdictions, it is recommended that it notify in all jurisdictions (often this includes foreign countries). With few exceptions, this has become standard in the privacy realm. A few companies that suffered early security breaches after California passed its law were torched by the media and subjected to severe criticism by irate state attorneys general for notifying affected Californians but not affected residents of other states without breach notification laws. The collective experience of these companies highlights an important, but often misunderstood, concept: technical compliance with law is necessary but not sufficient in the privacy arena. Privacy events are hot button social issues that often transcend mere legal compliance. Indeed, the risk to an organization's reputation and revenues often far exceeds the risk associated with non-compliance with breach laws. As a result, organizations responding to a breach should focus on doing the right thing as opposed to doing only those things that are required by law.

  PVLR ISSN 1538-3423

Lessons Learned

Security breach notification laws have brought information security issues into the spotlight. While no information security is perfect, proactive incident response planning can help minimize the impact when and if a breach occurs. Such planning includes inventorying the entity's databases that contain sensitive personal information, understanding how sensitive personal information flows through the organization, conducting ongoing risk assessments for internal and external risk to the data and responding to reasonably foreseeable risks, maintaining a comprehensive written information security program, and developing a breach response procedure. Given that a recent survey of 31 breaches ranging in size from 2,500 records to 263,000 records conducted by the Ponemon Institute found that the average cost of responding to a security breach was $182 per lost customer record with an average total cost of $4.8 million, the stakes are higher than ever for companies to focus on their information security programs.[4] Most importantly, concern and respect for information security should be integrated into the organization's core values. A breach response plan alone, without demonstrable organizational concern for information security generally, exposes the organization to significant risk. With the stakes as high as they are, all organizations should be taking a closer look at their information security practices.

[4] *See* Ponemon Institute, ''2006 Annual Study: Cost of a Data Breach'' (October 2006).

ACC Association of Corporate Counsel

ACC Annual Meeting

Data Security Breaches – The View from California

By in-house counsel, for in-house counsel℠

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-21 | Seattle, WA | am.acc.com

ACC Association of Corporate Counsel

Outline of Presentation

- California Office of Privacy Protection
- Making key decisions in responding to a data breach
- New California provision on breaches of medical information

ACC Association of Corporate Counsel

California Office of Privacy Protection

- CA is 1st state agency dedicated to consumer privacy – opened 2001.
- Mission – Identifying consumer privacy problems and promoting fair information practices.

ACC Association of Corporate Counsel

Office of Privacy Protection Functions

- Information and assistance
- Education
- Coordination with law enforcement
- Best practice recommendations

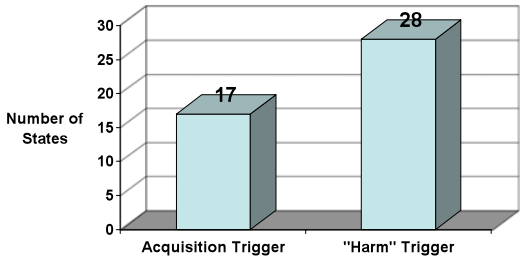
Making the Call on a Breach

- To notify or not to notify?

Factors in Assessing Risk of Harm

- Lost vs. stolen data
- Nature of data
  - Individual's ability to protect single account
  - Longevity of SSN's utility
  - Medical info and possible discrimination (HIV/AIDS, STDs, mental health, etc.)

"Risk-Based" Notification Trigger



Factors in Assessing "Unauthorized Acquisition"

- Case 1: Stolen laptop with unencrypted SSNs
- Case 2: Lost back-up tape with unencrypted SSNs
- Case 3: Hacked POS terminal with unencrypted credit/debit card numbers
- Case 4: Hacked server with database containing unencrypted SSNs

California Law on Breach of Medical Info

- Effective 1/1/08, new notice-triggering information in CA law.
  - Medical information or health insurance information – very broadly defined.
- AR and DE have similar provisions, but also harm trigger.

Our Recommended Practices

- Developed with advisory group of stakeholders.
- Attempted modeling on consumer credit reporting redress procedures.
  - But similar systems not in place in health care.

Our Recommended Practices: Health Plans & Insurers

- Provide patients with regular explanation of benefit statements: prompt, easy to understand.
- Be prepared to give individuals new member/subscriber number if breached.

Our Recommended Practices: All Organizations

- As part of data inventory, identify medical/ health insurance information.
- Update breach response plan to include medical information.
  - Be sure all staff are aware of change.

What to Say in Notice of Breach of Medical Information

- Aim is to provide *helpful* information on how individuals can protect themselves.
- If the breach does not include SSN, DL number or financial account numbers, say so.
- If it does, then also include the information on what to do from the appropriate section(s) [in sample letter].

What to Say in Notice of Breach of Medical Information

- Recommend regular review of explanation of benefits statements.
- Suggest consider ordering copies of your credit reports and checking for any medical bills that you do not recognize.

What to Say in Notice of Breach of Medical Information

- 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 to serve as a baseline.

CALIFORNIA
OFFICE OF
PRIVACY
PROTECTION

Recommended Practices on Notice of Security Breach Involving Personal Information

May 2008

October 2003
Rev. April 2006
Rev. February 2007
Rev. May 2008

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

Contents

Introduction

Identity Theft

Identity theft has been called the crime of the 21st century, favored, according to law enforcement, for its low risk and high reward. Not only do identity theft victims sometimes have to spend money out of pocket to clear up their records, but they also must devote their time – up to hundreds of hours in some cases – to doing so. 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, over eight million Americans were victims of identity theft in 2007. The same survey estimated the total cost of identity theft in the U.S. at $45 billion.[1]

Precisely how most identity theft occurs and the role of information security breaches is not clear. The major nationwide surveys have found that more than 60 percent of victims do not know how their personal information was acquired by a thief.[2] Consumers can often protect their personal information from some types of data theft, such as stolen mail or wallets and "phishing" emails. Other risks, however, are beyond consumer control. One academic study of identity theft cases found that in over half of the crimes, insiders in organizations were involved.[3]

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.[4]

Information Security

Security has always been an essential component of information privacy. It is one of the basic principles of fair information practice: Organizations that collect or manage individuals' personal information should use security safeguards to protect that information against unauthorized access, use, disclosure, modification, or destruction.[5]

Implementing an effective information security program is essential for an organization to fulfill its responsibilities towards the individuals who entrust it with their personal information. It is the best way to reduce the risk of exposing individuals to the possibility of identity theft. It is also the best way to reduce the risk of an information security breach and the resultant cost to an organization's reputation and finances.

Many organizations in the United States are legally required to protect the security of personal information. The two major federal laws on privacy enacted in recent years - the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act - include security regulations that apply to a broad range of financial services companies and health care organizations.[6] A California law also requires businesses to use reasonable and appropriate security measures to protect specified personal information of California residents.[7] Another California law imposes a similar requirement on state government agencies.[8]

Security Breach Notification

One of the most significant privacy laws in recent years is the California law intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to 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 to the addition of medical and health insurance information as "notice-triggering" in 2008.

Since the California law took effect in 2003, news reports of breaches have brought the issue of information security to public attention. Notifying affected individuals in such cases has become a standard practice, and at least 43 states have enacted notification laws based on California's.

The breach notice law has done more than give individuals notice. It has also resulted in improved privacy and security practices in many organizations. While the law does not require entities experiencing a breach to notify the California Office of Privacy Protection, many individuals, companies, and agencies have contacted the Office with questions about notification. In an effort to identify and spread best practices, the Office has studied these breach notifications and has synthesized many lessons learned from them.

One lesson is made clear by the significant share of breaches resulting from lost or stolen laptops and other portable devices, about 45 percent of the publicly known breaches.[9] Organizations have begun to pay more attention to protecting personal information on portable devices. Some organizations are doing this by using encryption. Others have adopted new procedures to safeguard the information, such as cabling PCs to desks, not allowing the downloading of Social Security numbers from mainframes onto PCs or laptops, and tightly restricting the number of people who are permitted to carry sensitive personal information on portable devices.

Another lesson is the ubiquity of Social Security numbers in databases and other records. Three quarters of the publicly known breaches involved Social Security numbers.[10] Individuals face the greatest risk of serious identity theft problems when their Social Security numbers fall into the wrong hands. Recovering from these types of identity theft can take hundreds of hours and thousands of dollars, making early discovery critical.

Some organizations that have experienced breaches of Social Security numbers have revised their data retention policies. After a breach that exposed 15-year-old data, a university reviewed its policies and decided to shorten the retention period for 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. A 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.

The California Office of Privacy Protection's Recommended Practices

California law obligates the Office of Privacy Protection to protect the privacy of individuals' 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 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 higher-risk 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 4 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. 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]

10. 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.

11. 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.

12. 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.

13. 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.

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.

Whom to Notify

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.
4. Avoid false positives. A false positive occurs when the required notice of a security breach is sent to individuals who should not receive it because their personal information was not acquired as part of the breach. Consider the following when identifying the group that will be notified.
   - Before sending individual notices, make reasonable efforts to include only those individuals whose notice-triggering information was acquired.
   - Implement procedures for determining who gets included in the notice and who does not. Check the mailing list before sending the notice to be sure it is not over-inclusive.
   - Document your process for determining inclusion in the group to be notified.

Contact Credit Reporting Agencies on Large Breaches of Financial-Related Information

A breach involving a large number of individuals can potentially have a significant impact on consumer reporting agencies and their ability to respond efficiently. High volumes of calls could impede access to the agencies. 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 relevant for breaches of Social Security numbers, driver's license or California ID numbers, or financial account numbers - not for breaches 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. Organizations should contact the consumer credit reporting agencies as follows.
   - Experian: Send an e-mail to BusinessRecordVictimAssistance @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.

Contents of Notice

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

1. A general description of what happened.
2. The specific type of personal information that was involved.
   - In breaches of financial-related information, specify whether Social Security number, driver's license or California ID number, or financial account number was involved.
   - In breaches of medical or health insurance information, be as specific as possible about the nature of the information involved. Specify that Social Security numbers, driver's license numbers and financial account numbers were not involved, when that is the case.
3. What you have done to protect the individual's personal information from further unauthorized acquisition.
4. What your organization will do to assist individuals, including providing your toll-free contact telephone number for more information and assistance.
5. 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.

6. 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 clear, simple language, guiding subheads, and plenty of white space in the layout.
2. Avoid jargon or technical language.
3. Avoid using a standardized format, which could result in making the public complacent about the process and thus undercut the purpose of the notice.

Means of Notification

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.
3. 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.
   - Post the notice conspicuously on your Web site, AND
   - Notify through major statewide media (television, radio, print), AND
   - Send the notice by e-mail to any affected party whose e-mail adddress

Notes

you have.

[1]Javelin Strategy & Research's "2008 Identity Fraud Survey Report," published February 2008. An abbreviated version is available for free and the full survey reports may be purchased online at www.javelinstrategy.com.

[2]According to the data in the 2008 Javelin survey report cited above, 65% of the victims surveyed did not know how their information was acquired by identity thieves. In addition, 20% said their information was in lost or stolen mail, wallet, or credit card; 8% said it was stolen during a transaction; 4% online; 2% in a data breach; and 1% other.

[3]"Identity Theft: Predator Profiles," Collins, J.M. and Hoffman, S.K. (2004). Available from Judith Collins, School of Criminal Justice, Michigan State University.

[4]The World Privacy Forum's research on medical identity theft is available at www.worldprivacyforum.org.

[5]This formulation of the security safeguards principle is from the Organisation for Economic Cooperation and Development (OECD)'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at www.oecd.org. The U.S. participated in the development of these principles and reaffirmed their viability as recently as 1998, in the *Declaration on the Protection of Privacy in Global Networks*. In that work, the U.S. committed to respecting individual privacy rights as an essential component to building and retaining public confidence in a marketplace that is increasingly global and increasingly online. The Principles form the foundation of most privacy laws in the U.S. and elsewhere.

[6]The Gramm-Leach-Bliley Act, 15 U.S.C 6801-6827, includes the Safeguards Rule, "Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information," 16 C.F.R. Part 314. The Health Insurance Portability and Accountability Act, PL 104-191, includes "Health Insurance Reform: Security Standards," 45 C.F.R. Parts 160, 162, and 164.

[7]California Civil Code § 1798.81.5 requires companies that collect specified personal information (name plus Social Security number, driver's license or state ID number, financial account number, or medical information) on California residents to use reasonable and appropriate security safeguards to protect it. It also requires such companies to contractually obligate service providers to the same standards.

[8]California Civil Code § 1798.21. The Information Practices Act, Civil Code § 1798 et seq., imposes specific responsibilities for protecting the security and confidentiality of records containing personal information.

[9]The Privacy Rights Clearinghouse maintains a list of publicly known breach notifications at www.privacyrights.org. While this list does not represent all breaches or even all notifications, it is the most comprehensive list available.

[10]In a May 2008 revew of 880 breach notifications on the Privacy Rights Clearinghouse list cited above, 45% of the incidents resulted from a lost or stolen computer, thumb drive, back-up tape or other medium. Eighteen percent were due to hacking, 14% to inadvertant Web exposure, 6% to improper disposal, 5% to insider fraud, and the remaining 12% to mailing or emailing errors, lost mail, and other causes.

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

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

[13]The internationally recognized information security standard is ISO/IEC 27001, a comprehensive set of controls comprising best practices in information security. For more information on the principles and practices of information security, see Appendix 5: Information Security Resources.

[14]The State of California has adopted a policy requiring State agencies to encrypt "notice-triggering" and medical information on portable computing devices or portable storage media. See BL05-32, available on the Policy page at www.infosecurity.ca.gov.

[15]See California Civil Code § 1798.81.5.

[16]Effective May 26, 2002, 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*, published in February 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 14 above, includes practices related to responding to and reporting security incidents and malfunctions "as quickly as possible" (§ 6.3).

[19]See Appendix 4 for suggestions on computer security incident response from the California Highway Patrol's Computer Crimes Investigations Unit and the FBI's National Computer Crime Squad.

[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

Dear :

We are writing to you because of a recent incident at [*name of organization*]. *Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response.*

Tell people what to 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 for Social Security numbers.

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 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.

When to Notify

- Timing: "in the most expedient time ossible 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 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.
- 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) 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.

(e) 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.

(f) (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 athe individual, or any information in an individual's applicaton and claims history, including any appeals records.

(g) 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 Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), 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) 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.

(e) 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.

(f) (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 athe individual, or any information in an individual's applicaton and claims history, including any appeals records.

(g) 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 Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), 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.

1798.84. (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable. (b) Any customer injured by a violation of this title may institute a civil action to recover damages. (c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.

(d) Unless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively.

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(f) A prevailing plaintiff in any action commenced under Section 1798.83 shall also be entitled to recover his or her reasonable attorney's fees and costs.

(g) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

Appendix 4: 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: 408-494-7186
http://reacttf.org

Computer and Technology Crime High-Tech Response Team (CATCH)
Telephone: 619-531-3660
http://www.catchteam.org/

FBI
Local Office: http://www.fbi.gov/contact/fo/fo.htm
National Computer Crime Squad
Telephone: 202-324-9164
E-mail: nccs@fbi.gov
www.emergency.com/fbi-nccs.htm

U.S. Secret Service
Local Office: www.treas.gov/usss/index.shtml
Cyber Threat/Network Incident Report: www.treas.gov/usss/net_intrusion_forms.shtml

Procedures the Computer User Should Institute Both Prior to Becoming a Computer Crime Victim and After a Violation Has Occurred

Guidance from the FBI National Computer Crime Squad
www.emergency.com/fbi-nccs.htm

- Place a login banner to ensure that unauthorized users are warned that they may be subject to monitoring.
- Turn audit trails on.
- Consider keystroke level monitoring if adequate banner is displayed.
- Request trap and tracing from your local telephone company.
- Consider installing caller identification.
- Make backups of damaged or altered files.
- Maintain old backups to show the status of the original.
- Designate one person to secure potential evidence
- Evidence can consist of tape backups and printouts. These should be initialed by the person obtaining the evidence. Evidence should be retained in a locked cabinet with access limited to one person.
- Keep a record of resources used to reestablish the system and locate the perpetrator.

Reporting a Computer Crime to Law Enforcement

Guidance from the California Highway Patrol Computer Crimes Investigation Unit
www.chp.ca.gov/programs/ccrime-incident.html#do

When reporting a computer crime be prepared to provide the following information:

- Name and address of the reporting agency.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.).
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- Make/model of the affected computer(s).
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).

- Operating System of the affected computer(s).
- Location of the affected computer(s).

Incident Response DOs and DON'Ts

DOs

1. Immediately isolate the affected system to prevent further intrusion, release of data, damage, etc.
2. Use the telephone to communicate. Attackers may be capable of monitoring E-mail traffic.
3. Immediately notify an appropriate law enforcement agency.
4. Activate all auditing software, if not already activated.
5. Preserve all pertinent system logs, e.g., firewall, router, and intrusion detection system.
6. Make backup copies of damaged or altered files, and keep these backups in a secure location.
7. Identify where the affected system resides within the network topology.
8. Identify all systems and agencies that connect to the affected system.
9. Identify the programs and processes that operate on the affected system(s), the impact of the disruption, and the maximum allowable outage time.
10. In the event the affected system is collected as evidence, make arrangements to provide for the continuity of services, i.e., prepare redundant system and obtain data back-ups. To assist with your operational recovery of the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

DON'Ts

1. Delete, move, or alter files on the affected systems.
2. Contact the suspected perpetrator.
3. Conduct a forensic analysis.

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 docu-

mentation, 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), or forgery (Penal Code § 470).

Appendix 5: Information Security Resources

Federal Trade Commission, "Financial Institutions and Customer Data: Complying with the Safeguards Rule," available at www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

Federal Trade Commission, "Security Check: Reducing Risks to Your Computer Systems," available at www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

"Health Insurance Reform: Security Standards; Final Rule," 45 CFR Parts 160, 162 and 164, available at www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp.

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.visa.ca/ais and https://sdp.mastercardintl.com.

SANS, "Top 20 Security Risks" (updated annually) and "Best Practices for Preventing Top 20 Risks", available at www.sans.org/top20/.

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