INFORMATION SECURITY AND SECURITY BREACH NOTIFICATION GUIDANCE

Preventing, Preparing for, and Responding to Breaches of Information Security

LISA MADIGAN
ILLINOIS ATTORNEY GENERAL

INFORMATION SECURITY AND SECURITY BREACH NOTIFICATION GUIDANCE

Preventing, Preparing for, and Responding to Breaches of Information Security

The Office of Illinois Attorney General Lisa Madigan has created this guide for businesses and governmental agencies in Illinois subject to the Personal Information Protection Act. The Illinois Personal Information Protection Act requires notification to Illinois residents in the event of an unauthorized acquisition of their personal information.

Entities that collect, maintain, store, use, and ultimately dispose of personal information should take steps to protect that information and reduce the risk of suffering a security breach. Although it may be impossible to prevent every breach, good data security can reduce the likelihood of some breaches, thereby helping entities to avoid the costly notification process.

This guide is meant to provide guidance, and not to provide legal advice. It is also important to recognize that due to the ever-changing aspect of information security and technology, more may be required of businesses and governmental agencies than is explained in this guide.

Businesses and governmental agencies are encouraged to stay abreast of industry best practices for data security and prevention of data breaches.

This guide begins by providing guidance for strong data security practices. Because not all prevention is foolproof, it then provides information on how to plan ahead so that a response plan can be implemented immediately upon discovery of a breach. It then provides guidance for responding to breaches and complying with the Personal Information Protection Act.

PREVENTING SECURITY BREACHES

Safeguarding sensitive data in files and on computers makes good business sense. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on the following five key principles: (1) take stock; (2) scale down; (3) lock it; (4) pitch it; and (5) plan ahead.

TAKE STOCK

Know what personal information you have in your files and on your computers. 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. Conduct a thorough information assessment of all departments and divisions within your business or governmental agency.

When conducting the information assessment, you should follow these steps:

- Review human resources and personnel records and files and determine what personal employee information is collected, used, maintained, and stored.
- Review internal forms and computer systems that are used by employees for expense reports, trainings, reimbursement requests, and other administrative functions.
- Review all requests for personal information from clients, customers, vendors, and the general public.

SCALE DOWN

Keep only what you need for your business. If you don't have a legitimate business need for sensitive personally identifiable information, don't keep it. Maintaining Social Security numbers (SSNs) on personnel records is required for tax purposes and may be required for other purposes. Other uses may not be required and can be phased out as appropriate.

In order to reduce unnecessary reliance on personal information, especially SSNs, consider phasing out the use of personal information, especially SSNs, for administrative purposes and internal identification; explore the feasibility of replacing the SSN with a unique identification number; and if you determine that you do not need an SSN from clients, customers, vendors, or the general public with which you do business or interact, change your forms so that the SSN is not being requested.

LOCK IT

Protect the information that you keep. This includes physical and electronic security, and employee training regarding the handling of the information.

Physical and Electronic Security

- Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:
  - Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.
  - Store records in a room or cabinet that is locked when unattended.
- When customer information is stored on a server or other computer, ensure that the computer is accessible only with a strong password and is kept in a physically secure area.
- Change default passwords on all software.
- Where possible, avoid storing sensitive customer data on a computer with an Internet connection.
- Implement strong access controls. For example:
  - Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
  - Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. Strong passwords are a minimum of eight characters in length, and contain numeric characters, symbols, and a mixture of upper- and lower-case alphabetic characters. An employee's username and password should never be the same.
- Develop policies for employees who telecommute or travel often.
  - Consider whether or how employees should be allowed to keep or access customer data at home.
  - Require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
  - Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.
- Maintain secure backup records and keep archived data secure by storing it off-line and in a physically secure area.
- Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.
- Encrypt, using National Institute of Standards and Technology (NIST) certified cryptographic modules, all data on mobile computers/devices carrying sensitive data and all data that is transmitted via public networks.
- Use a "time-out" function for all internal computers that house sensitive information, remote access, and mobile devices. Time-out functions require users to re-authenticate after periods of inactivity.
- Log all computer-readable data extracts from databases holding sensitive information and verify each extract. Logs should be reviewed and inappropriate data extracts should be further investigated.
- Ensure all individuals with authorized access to personally identifiable information and their supervisors sign a document clearly describing their responsibilities.
- Maintain current updates to all software.
- Maintain strong firewalls, anti-virus, and anti-spyware protections.
- Do not allow employees to download and utilize peer-to-peer (P2P) software.
- Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices.

Security for Transmission of Payment Information

The Payment Card Industry (PCI) standards require businesses to maintain secure networks and dictate the proper storage and destruction of transmittable payment information. By complying with the PCI Data Security Standards, merchants and service providers not only meet their obligations to the payment system, but also build a culture of security that benefits everyone. The PCI Data Security Standards consist of twelve basic requirements categorized as follows:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

Employee Training

Employees with access to sensitive personal information must be trusted to maintain that information without taking advantage of their position. By some accounts, employee theft is a major cause of security breaches and subsequent identity theft. It is important to take the following steps to keep information out of the hands of rogue employees who steal or sell information:

- Check references or order background checks before hiring employees who will have access to customer information.
- Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.
- Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
    - Lock rooms and file cabinets where records are kept;
    - Do not share or openly post employee passwords in work areas;
    - Protect laptops, PDAs, cell phones, and other mobile devices according to policy;
    - Refer calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
    - Report suspicious attempts to obtain customer information to designated personnel.
- Regularly remind all employees of your company's policy—and the legal requirement—to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.
- Impose disciplinary measures for security policy violations.

- Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

PITCH IT

Dispose of customer information in a secure way. For example:

- Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
- Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.
- Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.

Proper Disposal

As of January 1, 2012, the Illinois Personal Information Protection Act requires the proper disposal of materials containing personal information. Proper disposal of material that contains personal information is a necessary step in protecting individuals against identity theft and financial fraud. Incidents of identity theft occur when "dumpster divers" find troves of valuable personal information in publicly available garbage bins. In addition, personal information left on computers and other electronic media can be accessed and misused with relative ease.

- A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following:
    - Paper documents containing personal information may be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.
    - Electronic media and other non-paper media containing personal information may be destroyed or erased so that personal information cannot practicably be read or reconstructed.
- "Person" means: a natural person; a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.
- Any person disposing of materials containing personal information may contract with a third party to dispose of such materials in accordance with this Section. Any third party that contracts with a person to dispose of materials containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to, acquisition of, or use of personal information during the collection, transportation, and disposal of materials containing personal information.

PREPARING FOR SECURITY BREACHES

Even entities that take all appropriate precautions against security breaches may find themselves in the unenviable position of learning that sensitive personal information has been lost, stolen, or otherwise accessed inappropriately. A company or agency should not be caught off guard when a breach is discovered. In order to ensure compliance with breach notification laws, and to provide all affected individuals an opportunity to protect against identity theft, it is important that all entities establish a plan for responding to breaches. For that reason, the Federal Trade Commission (FTC) identifies "plan ahead" as the fifth key principle for a strong data security plan. Planning ahead can be part of a larger information security program.

INFORMATION SECURITY PROGRAMS

Federal law imposes data storage and destruction requirements on financial institutions and creditors who access consumer credit reports. As part of its implementation of the Gramm-Leach-Bliley (GLB) Act and the Fair Credit Reporting Act (FCRA), the FTC issued the Safeguards Rule, which requires financial institutions and users of credit reports under FTC jurisdiction to have measures in place to keep customer information secure.

The Safeguards Rule requires entities to establish, maintain, and update individual Information Security Programs. The Safeguards Rule can be used as a model for all businesses and governmental agencies. In creating an Information Security Program, consideration should be paid to the following steps:

- Designate an employee or employees to coordinate the information security program.
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each area of operations, including:
    - Employee training and management;
    - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and
    - Detecting, preventing, and responding to attacks, intrusions, or other systems failures.
- Design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Oversee service providers, by:
    - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
    - Requiring service providers by contract to implement and maintain such safeguards.
- Evaluate and adjust the information security program in light of the results of testing and monitoring; any material changes to business operations or business arrangements; or any other circumstances that may have a material impact on the information security program.

- **PLAN AHEAD.** Create a plan to respond to security incidents. The Government Accountability Office recommends that government agencies develop a plan to respond to security breaches. Private entities should establish plans in line with these same recommendations:
    - Develop a uniform response policy and standard operating procedures for data breach response capabilities.
    - Identify a core response group that can be convened in the event of a breach to evaluate the situation and help guide further response.
- Train employees to notify the appropriate personnel in the event of lost or compromised data. If a problem has been detected, it must be reported to the appropriate member of the response group so that a response can be implemented.
    - Conduct risk analyses to determine when to offer credit monitoring and when to contract for an alternative form of monitoring.
- Credit monitoring may not be appropriate in all breach situations. Many consumers have come to expect some offer of free credit monitoring, though. Before a breach occurs, talk to private companies that offer credit monitoring to discuss your options.
    - Implement an announcement strategy in preparing for inquiries about the incident by considering a call center staffed with individuals prepared to answer the most frequently asked questions.
- A call center may be appropriate where large amounts of data are compromised and notification is sent nationwide. Many businesses and agencies do not have the capability to respond to thousands of inquiries.
    - Require service providers and business partners who handle personal information for the agency to follow the agency's security policies and procedures.

RESPONDING TO SECURITY BREACHES

Businesses and government agencies learn of security breaches in a variety of ways. For example, an employee may notify his supervisor that a laptop containing sensitive customer data was lost or stolen. Information technology, properly monitoring its intrusion detection systems, may learn that an unauthorized individual has accessed the computer network. The business or agency may learn that a rogue employee has been selling data to identity thieves. There are many different ways that sensitive personal information belonging to employees, clients, customers, or consumers can be compromised. Regardless of the type of breach, the following steps should be taken upon discovery of a breach.

1. Implement the appropriate incident response plan.
    a. Notify the appropriate internal response team of the nature of the breach.

        ***Note: It is important that every employee understands what security incidents need to be reported, and to whom they should be reported. A response plan cannot be implemented without the proper individuals first having sufficient knowledge of a problem.

    b. Assess what happened and follow your pre-set plan.

        ***Note: Following the pre-set plan may include setting up a call center and establishing credit monitoring service for affected individuals. It may also include notifying the three major credit reporting agencies of the breach.

2. Secure the data immediately.
    a. Contact your information technology department and determine how to secure the data so that the minimum amount of data is compromised.
    b. Take all appropriate measures to secure the data.
3. Involve law enforcement immediately.
    a. Once the data is secure and isolated, if necessary, contact your local police, the FBI, or the U.S. Secret Service.

        ***Note: It might be prudent to notify law enforcement first, if an intruder has hacked into your computer network and you suspect that the intruder is still present in the system. Although you do not want additional information to be compromised, you also want to give law enforcement an opportunity to learn more about the thief while he is actively stealing data.

    b. Cooperate in any law enforcement investigation.
4. Consider hiring an outside forensic analyst to determine the extent of the breach and the individuals affected.
5. If you are handling the data for another entity, immediately contact that entity and any other entities from which you may have obtained the data.
    a. The Illinois law requires the entity that owns or licenses the data to notify affected individuals. The entity that maintains the data must report any breach to the owner/licenser of the data, which in turn will notify affected individuals.
6. Notify consumers about the breach without unreasonable delay.
    a. Notification can be delayed upon request by law enforcement.
7. Consider notifying the Illinois Attorney General's Identity Theft Hotline.
    a. Although notification to the Office of the Attorney General is not required, it may help affected individuals to know that they can turn to the Identity Theft Hotline for assistance. Notifying the Attorney General's Office before giving out the Identity Theft Hotline number will help us better prepare for the influx of calls.

ILLINOIS LAW REQUIRING NOTIFICATION IN THE EVENT OF A SECURITY BREACH

Personal Information Protection Act
815 ILCS 530/

Security Breach
"Breach of the security of the system data" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

Type of Information
"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 or redacted:

1. Social Security number.
2. Driver's license number or State identification card number.
3. Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

****Note:* If the breach involves the unauthorized acquisition of protected health information, notification may be required under the federal Health Insurance Portability and Accountability Act (HIPAA).

Whom to Notify
Any Illinois resident whose personal information has been breached. Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach.

*** *Note:* State agencies that collect personal information concerning an Illinois resident must notify the resident where there has been a breach of written material in addition to computerized data. There is a distinction here between data collectors and State agencies.

Any State agency that collects personal data and has had a breach of security of the system data or written material shall submit a report within 5 business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any State agency that has submitted a report under this Section shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.

When to Notify
The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

The notification may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

How to Notify

Notice to consumers 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 for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or
3. Substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) e-mail notice if the data collector has an e-mail address for the subject persons; (ii) conspicuous posting of the notice on the data collector's Web site if the data collector maintains one; and (iii) notification to major statewide media.

Other Legal Requirements

Any State agency that collects personal data and has had a breach of security of the system data or written material shall submit a report within 5 business days of the discovery or notification of the breach to the General Assembly listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any State agency that has submitted a report under this Section shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.

Any Illinois State agency that collects personal data that is no longer needed or stored at the agency shall dispose of the personal data or written material it has collected in such a manner as to ensure the security and confidentiality of the material.

A data collector that does not own or license the data shall provide such notification of the breach to the owner or licensee. In addition, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach.

Practical Considerations for Notification of the Breach

- What does the law require the letter to include? The disclosure notification to an Illinois resident shall include, but need not be limited to:
  - The toll-free numbers and addresses for consumer reporting agencies:
    - ✓ Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
    - ✓ Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
    - ✓ TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Fullerton, CA 19016-2000
  - The toll-free number, address, and Web site address for the Federal Trade Commission.
  - A statement that the individual can obtain information from these sources about fraud alerts and security freezes.

- What other information could be helpful to include in the letter? Entities sending notification letters should also consider including the following information:
  - What happened;
  - What information was believed to be accessed;
  - Whether law enforcement has been notified and the status of any criminal investigation, including whether any arrests have been made;
  - How consumers can protect themselves against identity theft;
  - What consumers should look for to determine if they have become victims, including:
    - Receiving credit cards you did not apply for;
    - Being denied credit, or offered credit at less favorable terms for no apparent reason;
    - Receiving calls or letters from debt collectors or businesses about merchandise or services you did not buy;
    - Missing bills and other pieces of mail.
  - What steps consumers should take if they become victims of identity theft, including:
    - Contact the Attorney General's Identity Theft Hotline at 1-866-999-5630 for further advice on protecting yourself from identity theft.
    - Check with your creditors. Work with your credit card companies, banks, and other lenders to determine if any suspicious or unauthorized activity has occurred on your accounts.
    - Cancel credit cards whose numbers may have been compromised.
    - Place an initial fraud alert on your credit report. Order your free copy of your credit report and review it for problems.
      - ✓ Contact any of the three consumer reporting companies to place a fraud alert on your credit report. You only need to contact one of the three companies because that company is required to contact the other two.
      - ✓ Once you place a fraud alert on your file, you are entitled to a free copy of your credit report. The credit reporting agencies will send you a letter telling you how to order your free report. When you receive your credit reports, review them carefully and look for any suspicious activity.
    - Remain alert. This is always a good idea, but especially in the first year following a security breach notification. Take advantage of your right to one free copy of your credit report from each of the three consumer reporting companies per year. Request a report from one of the reporting companies every four months and carefully review this report for suspicious activity. To obtain the free reports, consumers can call 1-877-322-8228 or order online at www.annualcreditreport.com.
  - How consumers can get further information; and
  - How consumers can sign up for credit monitoring (if you are offering it).
- Do we need to set up a call center?
  - This may depend on the number of breach notification letters that are going out. If your regular customer service line can handle the influx of calls, you may not need a separate call center.
- Should we stagger breach notification letters?
  - If you have a lot of letters to send out and are worried about call volume, you should consider staggering the mailing of notification letters.
- How can we ensure accurate information is reaching affected consumers?
  - Employee training is essential. Fact sheets can be utilized to provide quick, easy information to all employees. Anticipate where calls might come in and make sure that those employees are briefed.
- Should we offer credit monitoring?
  - Offering credit monitoring to consumers is not required under the Personal Information Protection Act. Nonetheless, many entities that suffer breaches offer 12 or 24 months of free credit monitoring to affected consumers.

- o Credit monitoring services may be inappropriate where credit or debit account information was accessed. In those cases, the thieves may make unauthorized charges on existing accounts, but they probably do not have the requisite information to open new lines of credit. Credit monitoring will not prevent the thief from spending to the limit on cards that already exist.

- Do we need to notify anyone else?
  - o Unless you are a state agency, the law does not require that you notify anyone other than the affected Illinois residents.
  - o The Illinois Attorney General's Office provides an Identity Theft Hotline to assist consumers. If you want to include the Hotline number on your breach notification letter, you should contact our office so that we can be prepared for the calls.
- How can we prevent this from happening in the future?
  - o The first step is to determine how it happened. Each situation requires a different response. For example:
    - If you had a rogue employee access the data without permission, address whether that employee should have had access to personal information in the first place, and whether increased or different training would have helped to protect the information.
    - If an honest employee misplaced a laptop, thumb drive, or list of personnel files, address whether it was proper for that employee to be permitted to take that information out of the office. Consider increased security on laptops and other portable devices to better protect the information.
    - If a hacker found his way into your network system, address whether IT security is up to date. Assess the storage, maintenance, and destruction of personal information and make a determination about whether information is being mishandled at any point in the process.

---

[i] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (March 2007).

[ii] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Office of Management and Budget, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES M-07-16 (May 22, 2007). These requirements are derived from existing federal security policy and National Institute of Standards and Technology (NIST) guidance.

[iii] See NIST's Web site at http://csrc.nist.gov/cryptval/ for a discussion of the certified encryption products.

[iv] Adapted from Lessons Learned about Data Breach Notification, Report to Congressional Requestors, GAO-07-657 Privacy (April 2007).