

The New York State Consumer Protection Board's Business Privacy Guide:

*How to Handle Personal
Identifiable Information and
Limit the Prospects of Identity Theft*



**New York State
Consumer Protection Board**
Advocating for and Empowering NY Consumers
1-800-697-1220
www.nysconsumer.gov

David A. Paterson
Governor

Mindy A. Bockstein
Chairperson and Executive Director

This brochure is for informational purposes only and should not be construed as legal advice or as policy of the State of New York. It is recommended that you speak with a privacy professional and an attorney for further advice.

This Guide may be copied if
(1) the meaning of the copied text is not changed or misrepresented;
(2) credit is given to the New York State Consumer Protection Board; and
(3) all copies are distributed free of charge.

October 2008

New York State Consumer Protection Board

<http://www.nysconsumer.gov>

Introduction

The New York Consumer Protection Board (CPB) is the State's top consumer watchdog and "think tank." The Agency's core mission is to protect the residents of New York by publicizing unscrupulous and questionable business practices; conducting investigations and hearings; researching issues; developing legislation and creating consumer education programs and materials.

This Guide has been developed by the CPB to help New York businesses better understand the importance of protecting customer and employee personal information and to address the growing problem of data breach and identity theft. It will also help build your reputation in the marketplace and avoid potential liability.

It is important for your company to have written policies to protect the personal information of employees and customers. These policies should be reviewed and updated regularly. You should refer to this Guide as a resource outlining principles and best practices for privacy protection. Furthermore, it is highly recommended that you consult a privacy professional and an attorney to ensure legal compliance with applicable State and federal laws and regulations.

Background: *The Core Principles.*

Identity theft is a growing problem. After California, New York leads the nation in the number of data breach incidents each year.¹ And, New York is 6th per-capita in identity theft complaints. In 2007, identity theft alone cost businesses over 40 billion.² The average data breach today will cost your business \$192 per-incident.³ According to a Ponemon Institute study, almost 33% of customers surveyed stated that they would cut ties with a company that had a data breach.⁴ It is not only good business sense for your organization to safeguard personal information, but it should be a core value to promote and retain business. A business plan might not stop data breach and identity theft, but good privacy practice will help to limit its adverse effects and to protect your business from potential liability.

Businesses collect and retain personal identifiable information⁵ in their records such as employee and customer names, residential addresses, Social Security numbers, credit cards and bank information. As a result, it is vital to properly safeguard personal information and to comply with both New York and federal law.

¹ Jay Cline, Computerworld, September 8, 2008.

² Javelin Strategy and Research survey reported in February 2008. <http://www.javelinstrategy.com/>

³ Ponemon Institute 2007 Annual Study: Cost of Data Breach. <http://www.ponemon.org/index.html>

⁴ Ibid.

⁵ For purposes of this guide, Personal Identifiable Information (PII) is defined as name combined with address, Social Security number, credit and or debit card numbers, individual account or bank numbers. Personal Identifiable Information will have the same meaning as Personal Information or Sensitive Information.

Business should adhere to the following four core principles in protecting personal information and in formulating written policies and procedures for privacy:

- Identify
- Secure
- Educate
- Plan

I. IDENTIFY

It is fundamental to understand how data is collected, transferred and transmitted in and out of your organization. To achieve that understanding, conduct a privacy audit of your business. Speak with all departments in your organization to obtain a complete picture of where data comes into your organization, where it goes, and who has possession, access and/or control over it. Create a chart of the data flows within your hierarchy. Examine all electronic equipment, computers, laptops, servers, any and all devices containing personal information.

Understand exactly the type of personal information that is maintained or recorded in your paper files and on your business computers. Ask: how? what? who? where? and why?

- **How?** It is vital to understand how your business collects personal information. Is information collected on a website? Does information come through postal mail? Is data collected via e-mail?
- **What?** Does the information that you receive and collect contain personal information? Is it names, addresses, Social Security numbers?
- **Who?** Which employees collect data of any kind? Which employees have access to sensitive data? Do you have contractors accessing personal information?
- **Where?** Where is personal information stored? On-site or off-site? Do you have individual computers containing personal information? Do employees have personal information on laptops?
- **Why?** Is it necessary to collect and store all the personal information your business collects? Is there a legitimate business purpose for collecting personal information? Is there some personal information that can be limited or eliminated from collection?

To ensure that you are compliant with best business practices, you should also study State and federal statutory prohibitions on data retention and collection. Best business practice is to limit both collection and access to personal information.

KEY POINTS

- ✓ Do not collect and or retain any personal information that does not have a legitimate business purpose.
- ✓ Best Practice: Social Security numbers. Limit the collection and the use of Social Security numbers. This will help prevent the unauthorized exposure of personal information in the event of a data breach.

Key New York Laws

The New York Social Security Number Protection Law⁶ became effective January 1, 2008. It prohibits your business from:

- making a Social Security number available to the general public whether intentionally or not.
- printing Social Security numbers on any card or tag required for an individual to access products, services, or benefits provided by the company.
- requiring an individual to transmit his/her Social Security number over the Internet, unless the connection is secure or the number is encrypted.
- requiring an individual to use his/her Social Security number to access an Internet website, unless a password, PIN, or other type of authenticating device is also required for the individual to access the website.
- printing an individual's Social Security number on any materials that are mailed to the individual, unless a State or federal law requires the number to be on the document being mailed.

The prohibitions highlighted below become effective January 3, 2009:

- Encoding or embedding a Social Security number in or on a card or document, including but not limited to, using a bar code, magnetic strip, or other technology, in place of removing the Social Security number.
- Filing any document available for public inspection with any State agency, political subdivision, or in any court that contains a Social Security account number of any other person, unless such other is a dependent child or has consented to such filing, except as required by federal or State law or regulation, or by court rule.

⁶ New York General Business Law Section 399-dd.

The New York Employee Personal Identifying Law will become effective January 3, 2009⁷. This law requires the creation of policies and procedures to prevent the prohibited practices outlined below, as well as employee notification of these policies and procedures.

Employers are prohibited from the following actions:

- Publicly posting an employee's Social Security number.
- Visibly printing a Social Security number on any identification badge or card, including any time cards.
- Placing a Social Security number in files with unrestricted access.
- Communicating an employee's personal identifying information to the general public. Personal identifying information is defined as a Social Security number, home address or telephone number, e-mail address, Internet identification name or password, parent's surname prior to marriage or driver's license number.

Does your business collect receipts?

- ✓ All businesses accepting payment by credit card must remove the expiration date and all but the last five digits of the credit card number from customer receipts.⁸

Key Federal Laws

The federal Health Information Insurance Portability and Accountability Act Privacy and Security Rules (HIPAA) apply to health care providers, health plans and health care clearinghouses and describe rules to maintain privacy. See www.hhs.gov/ocr/hipaa.

The federal Gramm-Leach-Bliley Act's Privacy and Safeguards Rules (GLBA) apply to a broad spectrum of financial institutions and list privacy requirements for these types of businesses. See www.ftc.gov/privacy/privacyinitiatives/glbact.html.

II. SECURE

Physically protect the personal information that your company has in its possession. This includes both physical and electronic protection. Proper security measures include the adoption of administrative, physical and technological safeguards for personal information.

⁷ New York Labor Law Section 203-d (effective January 3, 2009).

⁸ New York State General Business Law Section 520-a.

Physical Security

Prepare a written information security policy. Elements of this policy should include the principles of Lock, Limit and Learn.

- ✓ **LOCK** papers, documents, disks and files containing personal identifiable information. Files containing personal information should always be kept in a locked cabinet or locked room.
- ✓ **LIMIT** access to secure rooms to those employees who have a legitimate business need. This is also true of any personal information that is kept at a remote location. Only those with a legitimate business need should have access to off-site secure locations.
- ✓ **LEARN** about the best ways to educate your employees on the proper methods to physically secure personal information. It is vital to continually educate and train your employees on the importance of the protection of personal information. Stay informed of best practices to secure sensitive data.

Electronic Security

Implement technological safeguards to protect personal information.

Electronic Data

- Sensitive data should always be encrypted on laptops.
- Credit card or sensitive financial information should be sent from your business using Secure Sockets Layer (SSL), the standard language for transmitting sensitive information.

Computers and Networks

- Install firewalls, anti-virus and anti-spyware software to secure both networks and computers.
- Monitor software for regular updates and issues relating to viruses, spam and other threats.
- Limit access and laptop use to those who have a legitimate business purpose.
- Password protect laptops and encrypt sensitive information.
- Consider using an intrusion detection system to prevent hacking of your network and to detect network breaches.

- Use encryption for wireless transmissions to your network.

Passwords

- Require employees to have passwords on their desktop computers, laptops and wireless devices. Passwords must be kept private and not easily guessed. For example, the use of an employee's own name would be improper. You should advise your employees to make passwords long using a combination of symbols, numbers and letters.
- Ensure that passwords are kept in a safe place. Employees should not store them in a front drawer of a desk or on a computer's keyboard. They should be changed regularly and not be shared with others.
- Password protect all laptops.
 - Lost or stolen laptops or other portable devices are leading causes of data breach incidents.⁹

Record Disposal

- Dispose of paper and electronic data containing personal information in a safe and secure manner.
- Consider shredding paper records that are not required to be retained. Be sure to use a micro shredder.
- Use "wipe utility" software to permanently delete computer data.

Contractors

- Investigate your contractors' security policies and procedures and ensure that they are as strong as your own, if not stronger.
- Require your contractors to follow the same practices your business follows. Insist that your contractors notify you promptly of any security lapses or incidents.
- Make sure there is adequate physical security for paper records and encryption for electronic data shipped to and from vendors.

⁹ Ponemon Institute 2007 Annual Study: Cost of Data Breach.

KEY POINTS

- ✓ Limit access to personal information to those who need it for a legitimate business purpose.
- ✓ Secure physical and electronic access to sensitive information by developing reasonable safeguards.
- ✓ Best Practice: Never store personal information in a physical or electronic form when it is not needed for legitimate business use.

Key New York Laws

- Employees should only have access to Social Security numbers for legitimate business purposes and safeguards should be used to prevent unauthorized access to Social Security numbers.¹⁰

Does your business destroy records?

Ensure that you are compliant with New York General Business Law Section 399-h, which governs disposal of records containing personal information.

1. Shred the record before disposal; or
2. Destroy personal information contained in the record; or
3. Modify the record to make the personal information unreadable; or
4. Take action consistent with commonly accepted industry practices to ensure that no unauthorized person will have access to the personal information contained in the record.

Ensure compliance with the Federal Trade Commission's Disposal Rule, 16 CFR (Code of Federal Regulations) Part 682. This rule requires any individual or business that uses a consumer report, such as a credit check, for a business purpose to dispose of the report or information derived from such report to prevent "unauthorized access to or use of the information."

Other Relevant Laws:

Also see New York City Administration Code Sec. 20-117(g) which codifies requirements for the destruction of documents in the City of New York.

¹⁰See New York General Business Law Section 399-dd;
New York Labor Law Section 203-d (effective January 3, 2009).

III. EDUCATE

Education of both customers and employees is an important part of any information privacy plan. Clients need to be educated on why and what your organization collects and how it handles and uses personal information. Employees need to be regularly trained to handle personal information properly. A well-trained staff can also detect breaches and help to prevent identity theft.

Customers/Clients

Let clients know that privacy is an important core value of your business. If your company has a website, then it should have a conspicuously posted and easily understandable privacy policy that adheres to the following fundamentals:

- Describe how you collect personal information.
- Inform your customers of the types of personal information that your business collects, to whom it is shared and for how long it is retained.
- Explain how you protect personal information from unauthorized access.
- Provide a mechanism for a customer to review his or her personal information that is collected and for whom to contact at your company.
- Give customers a choice on how their personal information is to be used and disclosed.
- Train employees how to respond to customer questions and requests regarding the use of their personal data.
- Always comply with the terms of your privacy notice and immediately notify clients of any changes.
 - Special considerations for children and your website.
 - The Children’s Online Privacy Protection Act of 1998 (“COPPA”), imposes restrictions on commercial websites from collecting information about or from children age thirteen (13) and under without first obtaining parental consent.

- ✓ Consider using a privacy seal on your Website such as TRUSTe or BBBOnline. See www.truste.org and www.bbbonline.org.

Employees

The training of company employees in the protection of personal information must be an integral part of your privacy plan. Ensure that employees know and understand your company's privacy policy. Highlight the importance of protecting personal information through regular security and privacy trainings.

- Require new employees to read and understand your written privacy plan. Make sure remote employees adhere to the same data security and privacy rules as other employees.
- Utilize regular training sessions. Consider the use of posters to emphasize the importance of privacy. Train employees about pretext calling and phishing schemes. Require employees to notify managers immediately of any lost or stolen data, remote devices and or laptops.
- Monitor new privacy and security laws and regulations and update your privacy plan and training materials accordingly. Advise employees on new security risks.

KEY POINTS

- ✓ Staff training should be regularly scheduled to ensure that you have made the protection of personal information a priority within your company.
- ✓ Best Practice: Stay informed of changing laws and model procedures in information privacy and security; share the knowledge with your employees.

IV. PLAN

Every business must be prepared to respond to a data breach. The best medicine is an ounce of prevention. A protocol for the inevitable should include:

- A response team to coordinate and implement your businesses data breach plan.
- A team consisting of security, privacy and legal experts who know how to contain the breach, notify the appropriate law enforcement and regulatory bodies, and properly inform customers and clients.

- A response team that stays up-to-date and informed on the changing landscape regarding data breach and identity theft risks and laws. Your business plan should be regularly checked against new laws and issues. More than forty states (40) have diverse data breach laws, including the State of New York.

KEY POINTS

- ✓ Be ready for the inevitable data breach by planning and staying prepared. Take steps to close off risks or vulnerabilities. A data breach could trigger an investigation of your company's privacy and information practices by the Federal Trade Commission.
- ✓ Know who to notify in case of a data security breach.
- ✓ Best Practice: Become familiar with New York law and the laws of other states if you are doing business beyond New York borders. Always be prepared to show any regulatory body your written privacy policy.

Key New York Law

New York has a security breach information law known as The Information Security Breach and Notification Act.¹¹

In the event that an unauthorized party has accessed "private information", defined as a name in combination with a Social Security, driver's license or an account or credit card number, New York law requires your business to notify affected customers and inform appropriate authorities. Disclosure must be made "in the most expedient time possible and without reasonable delay but subject and consistent with legitimate needs of law enforcement." In addition, if there are more than five thousand (5,000) New York residents affected by the security breach at one time, your business must notify consumer reporting agencies as to the timing, content and distribution of the notices.

¹¹ New York General Business Law Section 899-aa.

Key Federal Regulation

➤ FTC Red Flag Rules

The Red Flag Rules¹² effective May 1, 2009, require any financial institution or creditor with “covered accounts” or other account for which there is a reasonably foreseeable risk of identity theft, to formulate and implement an identity theft program. Each institution’s program must include policies and procedures for detecting, preventing and mitigating identity theft. Further, the program must set forth a list of red flag activities that signal possible identity theft, and a response plan for when a flag is raised. In addition, each financial institution or creditor must update its program periodically to reflect changes in risks from identity theft.

V. CONCLUSION

It is good business sense for your company to have written policies and procedures to protect the personal information of employees and customers. A business plan might not stop data breach and identity theft, but good privacy practice will help to limit its adverse effects and help protect your business from potential liability and negative publicity. You should ensure that your policies are reviewed and updated regularly. Your business should use this Guide as a resource outlining principles and best practices for privacy protection, but it is highly recommended that you continually consult a privacy professional and an attorney to ensure legal compliance with applicable State and federal laws and regulations.

¹² FTC Business Alert, New Red Flag Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft, <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>. The enforcement of these rules has been delayed to May 1, 2009.

NEW YORK STATE SECURITY BREACH REPORTING FORM
Pursuant to the Information Security Breach and Notification Act
(General Business Law §899-aa; State Technology Law §208)

Name of Entity:

Street Address:

City: _____ State: _____ Zip Code: _____

Sector (please select one): Local Government State Government Federal Government
 Not-for-profit Commercial Educational

Type of Business (please select one): Biotech/Pharm Education Financial Services
 Health Care Insurance Retail/Internet Telecom. Transportation
 Other _____

Persons Affected: Total: _____ **Dates:** Breach Occurred: _____
NY residents: _____ Breach Discovered: _____
Consumer Notification: _____

Reason for delay, if any, in sending notice: _____

Description of Breach (please select all that apply): Hacking incident; Inadvertent disclosure;
 Stolen computer, CD, tape, etc; Lost computer, CD, tape, etc; Insider wrongdoing;
 Other (specify): _____

[Attach additional description if necessary]

Information Acquired (please select all that apply): Name; SSN; Driver's license no.;
 Account number; Credit or Debit card number; Other (specify): _____

Manner of Notification to Affected Persons (Attach Copy): Written; Electronic (email);
 Telephone; Substitute notice (provide justification). List dates of any previous (within 12
months) breach notifications:

Credit Monitoring or Other Service Offered: [] Yes; [] No; Duration: _____
Service: _____ Provider: _____

Submitted by: _____ Title: _____

Firm Name (if other than entity): _____

Telephone: _____ Email: _____

Dated: _____

**PLEASE COMPLETE AND SUBMIT THIS FORM TO
EACH OF THE THREE STATE AGENCIES LISTED BELOW:**

Fax or E-mail this form to:

New York State Attorney General's Office (OAG):

SECURITY BREACH NOTIFICATION
Consumer Frauds & Protection Bureau
120 Broadway - 3rd Floor
New York, NY 10271
Fax: 212-416-6003
E-mail: breach.security@oag.state.ny.us

**New York State Office of Cyber Security & Critical Infrastructure
Coordination (CSCIC):**

SECURITY BREACH NOTIFICATION
30 South Pearl Street, Floor P2
Albany, NY 12207
Fax: 518-474-9090
E-mail: info@cscic.state.ny.us

New York State Consumer Protection Board (CPB):

SECURITY BREACH NOTIFICATION
1740 Broadway, 15th floor
New York, NY 10019
Fax: 212-459-8855
E-mail: security_breach_notification@consumer.state.ny.us

VI. ADDITIONAL RESOURCES

Privacy Principles

The Privacy Rights Clearinghouse www.privacyrights.org

Organization for Economic Cooperation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data www.oecd.org

Protecting Personal Information: A Guide for Business from the Federal Trade Commission www.ftc.gov/bcpmenus/business/data.shtm

A California Business Privacy Handbook, California Office of Privacy Protection, April 2008 www.oispp.ca.gov

Security Information

Payment Card Industry Security Standard www.pcisecuritystandards.org

California Office of Information and Security & Privacy Protection www.oispp.ca.gov

General Information

International Association of Privacy Professionals www.iapp.com

Federal Trade Commission's Interactive Tutorial www.ftc.gov/infosecurity

New York City Department of Consumer Affairs www.nyc.gov/consumers

New York State Consumer Protection Board www.nysconsumer.gov

NYS Office of Cyber Security & Critical Infrastructure Coordination
www.cscic.state.ny.us

New York State Attorney General's Office www.oag.state.ny.us