



Dechert  
LLP

PRIMER ON SELECTED FEDERAL, CONNECTICUT, NEW  
JERSEY AND NEW YORK PRIVACY, IDENTITY THEFT AND  
INFORMATION SECURITY LAWS RELEVANT TO CHARITABLE  
AND OTHER NONPROFIT ORGANIZATIONS

REVISED JUNE 2010

This publication is available online at  
[www.probonopartnership.org/publications.htm](http://www.probonopartnership.org/publications.htm)

## TABLE OF CONTENTS

<b>INTRODUCTION.....</b>	<b>1</b>
<b>I. CONNECTICUT, NEW JERSEY AND NEW YORK STATE LAWS .....</b>	<b>2</b>
1. Who Must Pay Attention to Identity Theft Laws?.....	2
2. What Information Is Protected? .....	2
3. What Steps Must a Business Take to Protect This Information?.....	3
4. When Protective Measures Fail: What Constitutes A Breach? .....	5
5. What Must a Business Do When a Breach Occurs?.....	6
6. What are the Penalties for Violations?.....	8
7. Additional Restrictions When Accepting Payment in New York .....	9
8. Steps A Business Can Take to Protect Itself.....	10
<b>II. FEDERAL LAWS.....</b>	<b>10</b>
1. Health Insurance Portability and Accountability Act .....	11
2. Fair Credit Reporting Act .....	12
3. FTC Red Flags Rule.....	14
4. Gramm-Leach-Bliley Act .....	15
<b>III. RECENT FEDERAL LEGISLATIVE PROPOSALS AND EMERGING TRENDS .....</b>	<b>17</b>
1. Massachusetts Standards for the Protection of Personal Information .....	17
2. Proposed Federal Data Breach Notification Act.....	17
3. Proposed Federal Data Accountability & Trust Act.....	18
<b>IV. PRACTICAL SUGGESTIONS.....</b>	<b>19</b>
1. Conduct a Privacy and Security Audit.....	19
2. Prepare a Privacy and Security Policy .....	21
3. Prepare an Action Plan in the Event of a Security Breach .....	21
4. Helpful Resources.....	22
<b>APPENDIX A: RELEVANT TRI-STATE LAWS .....</b>	<b>24</b>

## INTRODUCTION

Identity theft in the United States is a problem that affects millions of Americans each year.<sup>1</sup> The federal government and most state governments have enacted laws to regulate the way businesses and other entities handle, maintain and protect certain personal and identifying information. This Primer is a summary of significant statutes and regulations in the area of privacy, identity theft and information security.<sup>2</sup> It focuses on the main topics that will likely be relevant to charitable and other nonprofit organizations.

The Primer concentrates on federal law and the laws of three states: Connecticut, New Jersey and New York. It is intended to be only a general summary to facilitate awareness among nonprofits of their potential obligations in this area. The Primer is not, and is not intended to be, a complete review of all laws relating to this topic or to all potential factual situations. Moreover, the laws relating to the issues covered in this Primer are rapidly changing. Should you have specific questions about how federal or state laws apply to your organization, you should seek legal advice.

The Primer is divided into four sections. Sections I and II review the main tri-state and federal laws relating to privacy and identity theft. Section III reviews a leading Massachusetts law and two pending federal bills. Finally, Section IV offers some practical suggestions for addressing privacy and identity theft issues within nonprofit organizations.

While reading the following outline, the following questions may be helpful to consider with respect to your organization's compliance needs in this area:

- What type of personal information does your organization collect (*e.g.*, names, addresses, social security numbers)? Is the collection of this information necessary for the purposes of your organization?
- How does your organization collect this information (*e.g.*, through a website or other electronic means, hand-written documents, mass mailings)?
- Once the personal information is collected, how does your organization store it? Who has access to it? How does the organization control access to this information (*e.g.*, if stored on a computer, is the information accessible only by certain users with passwords)? How does the organization destroy the information (*e.g.*, how is information destroyed or deleted from the hard drive of a computer prior to its disposal)?

In general, businesses (including nonprofits) that collect personal information from their customers or employees, including social security numbers and other identifying information, are required to protect the security of that information. They are also required to notify such individuals if the security of their information is breached. To protect the information from unauthorized use, businesses must destroy personal information before disposing of records containing such information (*i.e.*, shredding paper records, deleting electronic records or using other means to ensure that the content to be protected is unreadable). In addition, the application of certain federal laws and regulations in this area depend on whether your organization is an entity that provides health care services, obtains credit reports for the purpose of evaluating prospective or current employees or is engaged in the business of providing credit or financial products or services.

---

<sup>1</sup> *Identity Theft: Victims Bill of Rights: Hearing Before the Subcommittee on Information Policy, Census, and National Archives of the House Committee on Oversight and Government Reform*, 111th Cong. (2009) (statement of Federal Trade Commission).

<sup>2</sup> Although the law in this area has privacy and information security aspects, this Primer will refer to it as the law of "identity theft."

## I. CONNECTICUT, NEW JERSEY AND NEW YORK STATE LAWS

The relevant state-level identity theft laws for Connecticut, New Jersey and New York are very similar. For this reason, Section I of this Primer follows this format: **legal requirements common to all three states are described in the opening paragraphs under each subsection, and distinctions applicable to a specific state are discussed in subsequent paragraphs, denoted by the relevant state's name.**

In general, an organization's obligation to comply with a state's statutory requirements regarding identity theft may be triggered by where the business conducts its services or offers its products, including where its customers or donors reside. To the extent that a business conducts its services or offers its products, or has customers or donors, in states other than Connecticut, New Jersey or New York, the business may be subject to the privacy laws of such other states. This Primer does not discuss the privacy laws of states other than Connecticut, New Jersey or New York.

This Section will discuss: (i) how an entity may become subject to identify theft laws; (ii) what types of information are protected; (iii) how a business can protect this information; (iv) what constitutes a breach of the security of electronic data; (v) what to do if there is a breach; (vi) penalties for breach of these privacy laws; (vii) additional considerations when accepting payment in New York; and (viii) steps a business can take to protect itself. For statutory references to the relevant provisions of the Connecticut, New Jersey and New York laws relating to identity theft, please see Appendix A.

### 1. Who Must Pay Attention to Identity Theft Laws?

Connecticut, New Jersey and New York all require individuals or businesses – the latter of which include sole proprietorships, partnerships, corporations, associations or other entities, however organized and whether or not organized to operate at a profit (hereinafter, a “Business”) – to protect the security of private information and to provide notice of a breach of such protection to those individuals whose private information was or may have been compromised while in the Business' possession. The laws of each of these states apply to any Business (with one exception in Connecticut only, noted below) that (i) conducts business in the state and (ii) either (a) owns or licenses computerized data that include private information or (b) maintains data, electronic or paper, that include private information.

Although the statutory privacy and security requirements in these three states apply in certain situations only to social security numbers (“SSNs”) or only to electronic data, nonprofit organizations should consider applying similar privacy and security protections to all paper and electronic records that contain personal information. Such a practice would bolster the organization's defenses to identity theft. For the same reason, even though the laws in these three states differ somewhat, nonprofit organizations in a state with a less demanding privacy or security requirement should consider applying the broader protections found in other state schemes.

In Connecticut, there is an exception from the breach notification law for a Business that, in the “ordinary course”<sup>3</sup> of business, **does not** own or license computerized private information, and/or maintain computerized private information that the business does not own.

### 2. What Information Is Protected?

In general, the law broadly protects virtually all personally identifying data or information of a private nature (“Personal Information”) that a Business collects, such as through employment applications

---

<sup>3</sup> The relevant Connecticut statute does not define “ordinary course” of business.

and other employment-related materials, among other sources. Personal Information includes an individual's first name or first initial and last name linked with any one or more of the following data elements, whether or not encrypted (*i.e.*, modified so that the information is unreadable or unusable to an unauthorized user): (i) SSN; (ii) driver's license number or state identification number; or (iii) account number, credit card number or debit card number, in combination with any required security code or access code that would permit access to an individual's financial account. Publicly available information that is lawfully made available to the general public from federal, state or local government records, or from widely distributed media, is not protected.

### **3. What Steps Must a Business Take to Protect This Information?**

Laws in Connecticut, New Jersey and New York require that Businesses take reasonable measures to protect the confidentiality of Personal Information. The laws generally require that Businesses safeguard Personal Information against misuse by third parties, and adequately destroy Personal Information before disposing of records in which it is contained. This must be done by shredding, erasing or otherwise modifying the Personal Information to make the contents unreadable, indecipherable or incapable of being re-constructed through generally available means. Merely discarding paper documents or deleting electronic records is unlikely to satisfy the legal requirements.

In addition to the above, the laws of Connecticut, New Jersey and New York have requirements specifically relating to the protection of SSNs, as discussed below. Businesses should not use any portion of an individual's SSN as part of the individual's account, membership or employee number.

It is permissible for a Business to require individuals to include their SSNs on written applications that individuals fill out in order to receive services, employment or benefits. However, SSNs should not be requested unless there is a strong business necessity for the information.

Connecticut. Connecticut law requires Businesses that collect SSNs to adopt and publicly display a privacy protection policy that ensures the confidentiality of SSNs. For this purpose, a "public display" may include posting a policy on the Business' website. Unlike similar statutes in other states, however, in Connecticut, "unintentional" or merely negligent violations of this policy display requirement are not subject to civil penalties.<sup>4</sup>

Connecticut law imposes restrictions on Businesses from "publicly displaying" SSNs, but does not prohibit the use or disclosure of an SSN pursuant to state or federal law. It also does not prohibit the use of SSNs solely for internal verification or administrative purposes.

Connecticut law prohibits: (i) intentionally making an SSN available to the general public; (ii) printing an SSN on any card required for an individual to access the Business' products or services; (iii) requiring an individual to transmit his/her SSN over the Internet (except where the Business provides a secure connection or encrypts the SSN); or (iv) requiring an individual to use his/her SSN to access a website (except where a password or unique personal identification number is required to access the Business' website).

New Jersey. In New Jersey, the law prohibits certain conduct in connection with the collection and use of SSNs. A Business may not: (i) publicly post or display either an individual's SSN or any four or more consecutive numbers taken from the individual's SSN; (ii) print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires the SSN to be on the document to be mailed; (iii) print an individual's SSN on any card required for the individual to access products or services provided by the Business; (iv) intentionally communicate or otherwise make available to the general public an individual's SSN; (v) require an individual to transmit his/her SSN over

---

<sup>4</sup> Penalties for statutory violations are discussed further in Section I.6 below.

the Internet, unless the connection is secure or the SSN is encrypted; or (vi) require an individual to use his/her SSN to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the Internet website. New Jersey permits employers to use an individual's SSN for internal verification purposes and administrative purposes – such as to confirm representations in employment or membership applications – that do not result in unauthorized access to the protected information.

New York. In New York, Businesses are prohibited from: (i) intentionally communicating or making available to the general public an individual's SSN (or any number derived from an individual's SSN), except where the number has been encrypted; (ii) printing an individual's SSN on any card or tag required for the individual to access products, services or benefits; (iii) requiring an individual to transmit his/her SSN over the Internet, unless the connection is secure or the SSN is encrypted; (iv) requiring an individual to use his/her SSN to access an Internet website, unless a password or personal identification number or other authentication device is also required to access the website; (v) printing an individual's SSN on any materials mailed to the individual unless state or federal law requires the SSN to be on the document; (vi) encoding or embedding an SSN 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 SSN; and (vii) filing any document with any state agency, political subdivision or in any court, where such document is available for public inspection and contains the SSN of any other person, unless such other person is a dependent child or has consented to such filing, except as required by federal or state law or regulation, or by court rule.

New York employers may not, unless otherwise required by law: (i) publicly post or display an employee's SSN; (ii) visibly print an SSN on any identification badge or card, including a time card; (iii) place an SSN in files with unrestricted access; or (iv) communicate an employee's personal identifying information to the general public. The law also prohibits the use of SSNs as identification numbers for the purposes of any occupational licensing.

**Illustration.** ABC Nonprofit is a nonprofit organization that is subject to the laws of Connecticut. In addition, due to the scope of its operations, it may also be subject to the laws of New Jersey and New York. ABC requires employees to write their SSNs on forms that are used for payroll purposes, and requires members to list their SSNs on membership forms. In addition, during its annual open enrollment period for benefits, ABC requires employees to write down their SSNs and the SSNs of their family members who opt for health coverage, and then ABC passes that information on to the applicable group health insurance carrier, group life insurance carrier or pension plan administrator. The information is saved to electronic files and all paper records are discarded. ABC mails its employees their payroll stubs and mails annual reports to members. It also has a website that individuals can use to register for membership and make donations.

Because ABC is subject to Connecticut law and may be subject to the laws of New Jersey and New York, it decides to comply with the identity theft laws of all three states with respect to all of its activities. To satisfy these states' requirements, ABC must:

(i) ensure that the computer files are password protected and that only those employees who need to access the SSNs for legitimate business reasons know the password;

(ii) shred the paper forms and not simply discard the forms after the information is transferred to the computer;

(iii) ensure that no SSNs are printed on the payroll stubs, other mailings or membership cards;

(iv) ensure that any information collected through the website is encrypted and secure;

(v) not use a member's SSN as a website access ID or password, unless the member also is required to use an additional password that is not derived from the SSN; and

(vi) display a privacy protection policy ensuring the confidentiality of SSNs.

ABC should not print any part of an SSN on any membership lists or other materials that it may use internally. It should not use any portion of an SSN as an employee or member ID number.

In general, for all personal information collected, but particularly when handling SSNs and credit/debit card numbers, employees of ABC must not discuss such information when unauthorized individuals (including other employees) are present. For example, if there is a fundraiser or other such gathering, it is important that lists of attendees with their addresses, phone numbers and SSNs, if applicable, are not sitting on a table in an open area, or that if paper membership forms are collected, they are secure, so that an unauthorized person cannot gain access. It is difficult to envision a situation where an organization would need to have at its fundraiser an attendance list that includes attendees' SSNs and, thus, this should be avoided.

#### **4. When Protective Measures Fail: What Constitutes A Breach?**

A security breach occurs when there is unauthorized access to **electronic** files containing Personal Information that compromises the security, confidentiality, integrity or availability of Personal Information. Good faith acquisition of Personal Information by an employee or agent of the Business for the purposes of the Business is not a breach of the security of the system, provided that the Personal Information is not used or disclosed without authorization.

**Illustration.** Although ABC Nonprofit has appropriately authorized only necessary employees to access the Personal Information of its employees, members and donors, the following events give rise to a breach (or, in the third example, a potential breach):

1) An outside third party accesses ABC's computer system by breaching the security of ABC's website and downloading copies of SSNs or credit cards numbers of employees, donors or members.

2) One of ABC's authorized employees leaves his computer on. An unauthorized employee, *i.e.*, one acting without legitimate business reason, accesses Personal Information from that computer and prints a copy of the information for his own personal use. (Note: If the unauthorized employee saw the information on the computer screen but did not copy or use it, it would likely not constitute a breach. However, steps should be taken to reduce the risk of such a situation from occurring.)

3) ABC has a stack of new paper membership forms. Two authorized employees are loading data from the membership forms into an ABC computer. One of them is reading the information aloud and the other is typing the information into the computer. Also present in the room, within earshot of the two authorized employees, are other ABC employees who are not authorized to access the membership data. Even if the unauthorized employees do not use the information, the fact that they hear it could constitute public communication and constitute a breach.

## 5. What Must a Business Do When a Breach Occurs?

A Business that collects Personal Information must disclose any breach of: (i) the security of its electronic system for maintaining Personal Information; or (ii) the confidentiality of electronic Personal Information – such as an unauthorized copying or downloading of Personal Information from a computer.<sup>5</sup> The disclosure must be made to any in-state resident<sup>6</sup> whose Personal Information was, or is reasonably believed to have been, acquired by a person without valid authorization.

In addition, a Business that maintains computerized data licensed from a third party is required to notify the owner or licensor of that information of any breach of the data's security immediately following discovery of the breach, if there is reason to believe that an unauthorized person obtained Personal Information contained in the accessed data.

Notice may be provided by the following methods: (i) in writing; (ii) by telephone, provided a log is kept of each notification; (iii) "electronically," pursuant to specific statutory requirements;<sup>7</sup> or, in certain cases, (iv) by substitute notice. Substitute notice may be provided under any of the following conditions: (a) the person giving notice can demonstrate that the cost of providing notice in writing, by telephone, or electronically would exceed \$250,000; (b) notice must be given to over 500,000 affected persons; or (c) the person giving notice has insufficient contact information for the affected persons.

<sup>5</sup> The Connecticut, New Jersey and New York breach notification laws currently apply only to breaches related to electronically stored or transmitted data. Businesses should consider similar notification practices for security breaches with respect to Personal Information that is maintained in paper form.

<sup>6</sup> In New York, only state agencies are required to notify victims of a breach who are non-residents. *Although the laws in Connecticut, New Jersey and New York (as to Businesses) require disclosure of a breach only to in-state residents, it would be prudent for a Business that experiences a breach to consider also notifying affected non-residents, in view of the potential detrimental public relations consequences if such disclosure is not made.*

<sup>7</sup> Electronic notice must comply with the provisions regarding electronic records and signatures set forth in section 101 of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001, available at [www.law.cornell.edu/uscode/uscode15/usc\\_sec\\_15\\_00007001---000-.html](http://www.law.cornell.edu/uscode/uscode15/usc_sec_15_00007001---000-.html). This statute has numerous requirements, including, among others: (1) that the consumer has affirmatively consented to receiving the electronic notice and has not withdrawn the consent; and (2) that the consumer, prior to consenting, is provided with a clear and conspicuous statement that informs her of the right to receive the record in non-electronic form, of the right to withdraw consent, and of any conditions, consequences or fees that would apply should the consumer withdraw consent.

Substitute notice may consist of the following: (1) email notice, not necessarily pursuant to the electronic notice provision mentioned above, if email addresses are available; (2) conspicuous posting on the Business' website; or (3) notification to major state-wide media, including newspapers, radio, or television.

A nonprofit that experiences a security breach should consider seeking immediate assistance from legal counsel.

Connecticut. Connecticut applies a "reasonableness standard" for determining the likelihood of a breach and timing of the required notification. Notification is required: (i) of a confirmed breach of Personal Information; and (ii) where a Business reasonably believes that Personal Information has been breached (regardless of whether an actual breach occurred). The relevant statute does not elaborate on what must be done to determine whether a breach has occurred, or what type of evidence supports a reasonable belief that a breach occurred.

Connecticut does not *require* a Business to notify law enforcement authorities of a breach. However, if the Business *does* notify law enforcement officials and later determines that the breach is unlikely to result in harm to the individuals whose Personal Information was accessed, then the Business is relieved of the duty to notify those individuals. The Business may delay its notification to the affected individuals for a reasonable period, if so requested by a law enforcement agency in furtherance of a criminal investigation. Under these circumstances, the Business must await instruction from the law enforcement agency before notifying the affected individuals.

Notice is not required, despite the existence of a confirmed breach or a Business' reasonable determination that a breach has likely occurred, in any of the following situations: (i) the affected individuals are not Connecticut residents; (ii) prior to the breach, the Personal Information was made unreadable or unusable to an unauthorized user; or (iii) after an appropriate investigation and consultation with relevant federal, state and local law enforcement agencies, the Business reasonably determines that the breach will not likely result in harm to the affected individuals.

If notification is required (*i.e.*, there is a confirmed security breach, or a Business reasonably determines that such a breach likely occurred and none of the exceptions apply), then the Business must do so without unreasonable delay. The law allows time for the Business to complete an investigation to determine the nature and scope of the breach, to identify the affected Connecticut residents and to restore the reasonable integrity of the data system, before issuing its notifications.

New Jersey. If a Business believes that there has been a breach of the security of Personal Information, triggering the duty to disclose such breach, a Business ***must first notify the State Police***, which may also refer the matter to other law enforcement agencies. Depending on the outcome of an inquiry by law enforcement officials, the Business may be subject to a criminal or civil investigation. After the law enforcement agency has determined that disclosure of the security breach will not compromise its investigation and so informs the Business, the Business must notify affected individuals as soon as possible. The Business also must document the findings of any investigation relating to a security breach – regardless of whether it determines that a breach occurred – and retain a written record of the findings for five years.<sup>8</sup> In circumstances requiring notice to more than 1,000 people at the same time, a Business must notify all consumer reporting agencies that compile or maintain files on consumers at the same time.

---

<sup>8</sup> A Business that holds Personal Information for third parties and does not use that Personal Information for its own purpose must immediately notify the third party entity for which it is maintaining the information of any security breach. In that situation, the third party – not the Business holding the Personal Information – is responsible for complying with the breach notification requirements. If, in contrast, a Business holding Personal Information for a third party uses the information in furtherance of its business, then it is subject to the breach notification requirements.

New York. A Business must notify New York residents of a security breach regarding their Personal Information. The Business must also report to the State Attorney General, State Consumer Protection Board and State Office of Cyber Security and Critical Infrastructure Coordination regarding the timing, content and distribution of these notices and the approximate number of affected persons. If the breach affects more than 5,000 New York residents, then the Business also must report this information to New York consumer reporting agencies.

The statute defines a “consumer reporting agency” to be any agency that engages in the practice of assembling consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. Examples of consumer reporting agencies include Equifax, Experian and TransUnion. The New York Attorney General’s office will provide a complete list of all New York consumer reporting agencies upon request.

Regardless of the method of notifying the affected persons, the notice must include contact information for the Business and specify what Personal Information was affected. The notification must be made without delay, unless a law enforcement agency requests that notification be delayed to prevent interference with a criminal investigation. In that situation, notification must be made once the law enforcement agency lifts its delay request.

**Illustration.** An unauthorized third party hacked into the website of ABC Nonprofit and downloaded SSNs (or credit card numbers) that had been provided by the organization’s donors. While running a security check on its website, ABC discovers the unauthorized access and reasonably believes that the breach could result in harm to approximately 2,000 donors. ABC has sufficient contact information from each of the donors to allow it to notify them of the breach. Because ABC is subject to Connecticut law and may be subject also to New Jersey and New York law due to the scope of its operations, ABC decides to comply with the identity theft laws of all three states, with respect to all of its activities.

ABC first *must* notify the New Jersey State Police; however, it would also be advisable for ABC to notify state police in each of the other states. ABC must also notify the New York State Attorney General, the New York State Consumer Protection Board and the New York State Office of Cyber Security and Critical Infrastructure Coordination, and provide them with the details, as discussed above. Depending on the outcome of the initial investigation by such law enforcement officials, ABC may delay disclosure of the breach to its donors until otherwise instructed. Once so instructed, ABC must promptly notify each of the affected individuals. Because ABC has sufficient contact information, it decides to notify each donor by written letter.

## **6. What are the Penalties for Violations?**

Connecticut. Intentional failure to safeguard Personal Information in Connecticut is deemed an unfair trade practice that is subject to legal action by the Attorney General. Intentional failure to protect Personal Information, including intentional failure to destroy, erase or make unreadable Personal Information during the disposal of records, carries a civil penalty of \$500 for every violation and a maximum civil penalty of \$500,000 for any single event. Willful public display of SSNs is punishable by fines up to \$100 for a first violation, \$500 for a second violation and \$1,000 and/or imprisonment for up to six months for every subsequent violation.

New Jersey. A Business could be subject to civil penalties up to \$20,000 per offense (more if senior citizens are involved) if it “willfully, knowingly, or recklessly”: (i) discloses Personal Information; (ii) fails to notify affected individuals of a security breach; or (iii) does not appropriately destroy Personal Information. In addition, a Business may be found liable for triple damages and attorneys’ fees in a civil action by a victim.

New York. Whenever the New York Attorney General believes, based on evidence satisfactory to the Attorney General, that there has been, or there is, a continuing violation of the relevant laws, the Attorney General may bring an action in the name and on behalf of the people of the state of New York. Such an action may seek an injunction against continued violation of the New York laws, including those laws governing the destruction of Personal Information. In addition, in such an action, the court may award money damages for the victim's actual costs or financial losses if the Business did not provide notice in accordance with New York law. Knowing or reckless conduct may also give rise to such a civil penalty. Violators may be subject to fines of \$5,000 per violation. A Business may defend itself by showing that it used due diligence in properly disposing of such records.

In addition, a Business' knowing unauthorized use of employee Personal Information carries a civil penalty of up to \$500 per violation. A violation will be presumed to be "knowing" if the Business previously failed to establish any policies or procedures to safeguard against such a violation, including by informing its employees of the applicable law.

## **7. Additional Restrictions When Accepting Payment in New York**

New York imposes additional restrictions on Businesses that collect Personal Information from customers when accepting payment in a sales transaction. Generally, Businesses in sales transactions in New York may not record on a personal check, traveler's check, gift certificate, money order or other similar form of payment, the purchaser's SSN. If a Business requires a purchaser to present a credit card as a condition to accepting such a form of payment (*e.g.*, as a means of identification or as an indication of credit worthiness), then the Business may record the type of credit or debit card presented. The Business may not, however, record the card number on the form of payment. It also may not print either the expiration date or more than the last five digits of the card number on any receipt provided to the purchaser.

In addition, Businesses which accept payment by credit or debit card may not record on the credit or debit card transaction form any personal identification information (such as the purchaser's address or telephone number) that is not required to complete the credit or debit card transaction. Exceptions are for information required: (i) for shipping, delivery or installation purposes or for special orders; or (ii) where the Business processes credit or debit card transactions by mailing transaction forms to a designated bankcard center for settlement.

With some exceptions (including for shipping, delivery or installment related to the purchase), transaction forms must: (i) be carbonless; and (ii) not render a separate piece of paper that readily identifies the cardholder by name or number, unless doing so is necessary to complete the transaction. The laws applying to credit card transactions only apply to receipts that are electronically printed. They do not apply to transactions in which the sole means of recording the purchaser's charge, credit or debit card number is by handwriting or by an imprint or copy of the credit card.

Violation of the law prohibiting the recording of SSNs on payment instruments is punishable by a civil fine not to exceed \$100 for a first violation or \$250 for a subsequent violation. Violations of the credit card transaction laws are subject to a civil penalty of \$500, and must be corrected within one week. Failure timely and fully to correct a violation is punishable by a civil penalty of \$1,000 per week, not to exceed \$4,500.

**Illustration.** XYZ is a nonprofit operating in New York only. For its annual fundraiser, XYZ sells candy and accepts credit cards as a payment method. XYZ also accepts personal checks, but asks to see a credit card as one form of identification. XYZ is prohibited under New York law from requiring a customer who pays by credit card to also write down the customer's SSN, address or telephone number. XYZ is also prohibited from creating a record of the credit card number of any customer who displays his or her credit card as identification. In New York, a Business is not prohibited from requiring that a personal check have a pre-printed street address on it.

## **8. Steps A Business Can Take to Protect Itself**

In addition to becoming familiar with the principles discussed in this Primer and complying with applicable laws relating to protections against identity theft, all businesses in the tri-state area are encouraged to develop a comprehensive written information security program to protect the Personal Information they possess. Incorporating a written information security program is not only a good business practice, but also enhances customer loyalty, and protects against possible regulatory enforcement actions should a breach occur.

The Primer's introductory questions and practical suggestions (see Section IV, below) may be helpful for a Business to consider when designing a written information security program. Such a program would include appropriate safeguards for the specific type of information possessed, the risks associated with that information, how that information is received and maintained, and the Businesses' particular needs and uses of Personal Information in its possession.<sup>9</sup>

Nonprofit organizations should avoid the practice of requiring employees, members, donors or other individuals associated with their organization to record their SSNs or credit/debit card numbers on various forms when such information is not needed. For example, employers should not use employee SSNs, or portions of SSNs, as "employee numbers."

## **II. FEDERAL LAWS**

The major federal laws in the area of identity theft are the Health Insurance Portability and Accountability Act, which is enforced by the U.S. Department of Health and Human Services ("DHHS"), the Fair Credit Reporting Act, which is enforced by the Federal Trade Commission ("FTC") and the Gramm-Leach Bliley Act, which is also enforced by the FTC. Whether one of these statutes applies to an entity depends on the entity's classification (*e.g.*, whether the entity is a "financial institution" or a "creditor" with "covered accounts") and the type of information that the entity receives (*e.g.*, information that is "protected health information"). An organization that collects information that falls within the purview of any of these statutes is restricted in its use, transfer and storage of that information. This section summarizes these federal laws.

---

<sup>9</sup> As of October 2009, New Jersey has proposed a rule that would require a Business to create a comprehensive written information security program that includes appropriate safeguards for the protection of the Personal Information and for the prevention and detection of a breach of security with respect to this Personal Information. The proposed New Jersey regulation, N.J.A.C. 13:45F-3.2(a), gives specific examples of the types of provisions that could be included in the procedures, and suggested actions that a business can take to manage risk. According to the proposed regulations, a well-designed program will: (i) ensure the security and confidentiality of Personal Information; (ii) protect against any anticipated threats or hazards to the security or integrity of the Personal Information; and (iii) protect against unauthorized access to or use of Personal Information that could result in substantial harm or inconvenience to any customer. It is not certain that this rule, or a similar rule, will become effective.

## 1. Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996<sup>10</sup> (“HIPAA”) authorizes DHHS to issue rules addressing the privacy and security of “individually identifiable health information.” DHHS has issued two such rules – one for privacy (“HIPAA Privacy Rule”) and one for security (“HIPAA Security Rule”).

Generally, the HIPAA Privacy Rule requires “covered entities”<sup>11</sup> to:

- notify patients about their privacy rights and how their information can be used;
- adopt and implement privacy procedures for their practice, hospital or plan;
- train employees so that they understand the privacy procedures;
- designate individuals to be responsible for seeing that the privacy procedures are adopted and followed; and
- secure patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

The HIPAA Privacy Rule prohibits covered entities from using or disclosing “protected health information”<sup>12</sup> (“PHI”) except in certain circumstances. Among permissible uses and disclosures of PHI are those that are: (i) authorized in writing in advance by the affected individual; (ii) for treatment, payment for medical treatment or health care operations (such as for management and administrative activities); and (iii) required by law. Upon request by the individual (or the person’s representative), a covered entity must disclose an individual’s PHI (subject to certain exceptions) or account for past authorized disclosures of an individual’s PHI. A covered entity also must establish policies and procedures regarding its privacy practices under the HIPAA Privacy Rule, and generally provide notice of these privacy practices at first contact with the individual while making a good faith effort to obtain written acknowledgement of receipt of such notice.

Any disclosure of PHI must be limited to what is reasonably necessary under the circumstances. Covered entities must implement reasonable and appropriate safeguards (administrative, technical and physical in nature) to prevent the unauthorized use or disclosure of PHI. Controls must be in place to prevent public access to, or unintentional disclosures of, PHI, as they must be for secure disposal of PHI.

In this respect, the HIPAA Privacy Rule overlaps with the HIPAA Security Rule, which prescribes standards for protecting the confidentiality, integrity and availability of electronic PHI (“E PHI”).<sup>13</sup> The HIPAA Security Rule provides that covered entities that possess or transmit E PHI must

---

<sup>10</sup> Pub. L. No. 104-191 (1996).

<sup>11</sup> “Covered entities” are “health plans,” health care clearinghouses and health care providers that transmit health information in electronic form in connection with transactions involving health care claims, benefits, payments or medical referrals. Health plans are generally any individual or group plan that provides or pays the cost of medical care.

<sup>12</sup> “Protected health information” is any “individually identifiable health information” transmitted or maintained by a covered entity.

“Individually identifiable health information” is information that: (i) relates to an individual’s past, present or future physical or mental health or condition, the provision of health care to the individual or the past, present or future payment for the provision of health care to the individual; and (ii) identifies or provides a reasonable basis to identify an individual. So defined, individually identifiable health information includes many common identifiers, such as an individual’s name, address, birth date and social security number. *Employment information maintained by a covered entity in its capacity as an employer is excluded from the definition of protected health information.*

<sup>13</sup> E PHI is PHI transmitted or maintained in electronic form.

protect against reasonably anticipated prohibited uses or disclosures. The Rule also sets forth standards for administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of EPHI.

Covered entities must ensure employee compliance with the HIPAA Security Rule's requirements, but may tailor their security measures depending on the entity's size, complexity and capabilities, as well as on the particular sensitivity of the EPHI. Some of the required safeguards include: (i) conducting a risk analysis involving consideration of all risks relating to the entity's EPHI; (ii) implementing security measures to manage the risks found during the risk analysis; (iii) implementing policies and procedures to detect, contain and remedy security violations; (iv) designating a security official to develop and implement such policies and procedures; (v) managing access to the EPHI; and (vi) ensuring that "business associates"<sup>14</sup> are contractually held to the requirements of the HIPAA Security Rule.

As required by the American Recovery and Reinvestment Act of 2009, DHHS issued an interim final rule implementing breach notification requirements ("Breach Notification Regulations"), which require covered entities, business associates and personal health record vendors to report breaches of "unsecured PHI" to the affected individuals or entities. "Unsecured PHI" includes any decipherable PHI, non-encrypted EPHI or EPHI that has not been destroyed per DHHS regulation. A breach requires notification unless: (i) the unauthorized person to whom the information was available would not reasonably have been able to retain such information; or (ii) the information disclosed would not pose a significant risk of financial, reputation or other harm to the individual. Covered entities and business associates are required to implement policies and procedures to enable them to perform risk assessments to determine whether a breach requires notification because the breach posed a significant risk of financial, reputation or other harm and the unauthorized person could have retained the information.

Under the Breach Notification Regulations, notice to the affected individual is required no later than 60 calendar days after the breach is discovered, and requires, among other things, a description of the incident, the PHI involved and the actions that the covered entity is taking to investigate the breach, mitigate losses and protect against further breaches. If a business associate of a covered entity maintains PHI for the covered entity, the business associate is required to provide similar notification to the covered entity within 60 calendar days of the breach, and, upon notification, the covered entity would have 60 calendar days to notify the affected individuals *if* the business associate is considered an "independent contractor" of the covered entity. If the business associate is an "agent" of the covered entity, the covered entity would have to provide notification within 60 calendar days of the date the *business associate* discovered the breach.<sup>15</sup>

A more detailed review of HIPAA's requirements is set forth in *HIPAA Primer for Nonprofit Social Services Agencies*, available at [www.probonopartnership.org/publications.htm](http://www.probonopartnership.org/publications.htm).

## **2. Fair Credit Reporting Act**

The Fair Credit Reporting Act ("FCRA"),<sup>16</sup> as amended by, among other laws, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), is enforced by the FTC and establishes requirements and procedures for the collection, use and protection of information used to assess consumer credit, employment and insurance eligibility. The FCRA provides protections for "consumers" and

---

<sup>14</sup> A business associate for these purposes is a person or organization that performs certain functions or activities on behalf of, or provides services to, a covered entity that involve the use or disclosure of EPHI.

<sup>15</sup> Generally speaking, an entity would be an "independent contractor" of another entity if the relationship between the entities is solely contractual and they were not affiliated in some other way.

<sup>16</sup> Codified at 15 USC § 1681 *et seq.* Information about the FCRA is available at [www.ftc.gov/os/statutes/fcrajump.shtm](http://www.ftc.gov/os/statutes/fcrajump.shtm).

regulates the uses and contents of “consumer reports,” but generally applies only to entities that are a “consumer reporting agency” or that use (such as some employers) or resell consumer reports.

A “consumer reporting agency” (“CRA”)<sup>17</sup> generally may disclose consumer reports only to third party businesses for consumer purposes (including background checks by employers) or to government officials acting in their official capacities. CRAs must make reasonable efforts to verify the identity of prospective users of their consumer reports and provide notices both to persons who regularly furnish it with consumer information and who receive the CRAs’ consumer reports. In addition, CRAs must maintain reasonable procedures to ensure that information in their consumer reports: (i) will be used and reported only for permissible purposes; (ii) is accurate; and (iii) is not more than seven or ten years old for certain categories of information (such as civil judgments or bankruptcies). CRAs must also dispose of consumer information in a safe manner (*i.e.*, in a way that is not accessible or legible to unauthorized persons, such as by shredding paper copies).

The FCRA also imposes obligations on employers who obtain consumer reports from CRAs to evaluate prospective and current employees.<sup>18</sup> The employer must:

- provide prior written notice to and obtain written consent from the prospective or current employee regarding the consumer report;<sup>19</sup>
- provide the prospective or current employee with a copy of the consumer report and a description of his or her rights under the FCRA if contemplating certain “adverse actions” (*e.g.*, denying or terminating employment) based on the information contained in the consumer report (a “pre-adverse action notice”); and
- notify the prospective or current employee orally or in writing if, based in whole or in part on the information obtained from the CRA, any adverse action has been taken (an “adverse action notice”),<sup>20</sup> which must include:
  - the name, address and phone number of the CRA that supplied the report;
  - a statement that the CRA that supplied the report did not make the decision to take the adverse action and cannot give specific reasons for it; and
  - a notice of the individual's right to dispute the accuracy or completeness of any information the agency furnished, and his or her right to an additional free consumer report from the CRA upon request within 60 days.

Under the FTC’s “Disposal Rule,” any person subject to the FTC’s jurisdiction that maintains or otherwise possesses “consumer information” (which includes any consumer report and information derived from it) for a business purpose must properly dispose of such information by taking “reasonable measures” to protect against unauthorized access to or use of the information. This would include an

---

<sup>17</sup> A consumer reporting agency is any person (including a corporation or association) that regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing “consumer reports” to third parties. A consumer report includes any information collected by a consumer reporting agency with regard to a consumer’s creditworthiness or eligibility for extensions of personal credit, insurance or employment purposes. Information about an individual collected for a consumer purpose (such as extensions of credit or insurance) may also constitute a consumer report.

<sup>18</sup> If a Business retains an outside party, such as a lawyer or a human resources consultant, to conduct an internal investigation into workplace misconduct, the FCRA may apply to the report generated by the investigator. Before having a third party conduct such an investigation, confer with legal counsel for guidance.

<sup>19</sup> The prior written notice and consent may be in the same document, but the document cannot contain anything else.

<sup>20</sup> The FCRA adverse action notification provisions have been interpreted to require that a period of time elapse between the pre-adverse action and adverse action notices. The FTC has indicated in informal guidance that five business days may be appropriate, depending on the nature of the employer’s business.

employer's possession of a consumer report obtained for employment purposes. Reasonable measures would include implementing and monitoring compliance with policies and procedures that require shredding paper copies and erasing electronic media containing the consumer information so that such information "cannot practicably be read or reconstructed."

In addition, users of consumer reports are required, upon receiving notice from the CRA that a substantial discrepancy exists between the address the user (*i.e.*, the employer) provided and the address listed in the consumer report, to attempt to verify the address based on information in the user records or with the consumer about whom the report relates and to notify the CRA of the verified address.

The FCRA also prohibits any person that accepts credit or debit cards for a "transaction of business" from printing more than the last five digits and the expiration date of the credit or debit card. This does not apply to card imprints or handwritten receipts.

**Illustration.** ABC Nonprofit receives multiple applications for an open position. ABC provides notice to, and obtains written consents to receive credit reports from, all applicants. ABC rejects some applicants due to their negative credit histories, although the lack of relevant experience carries more weight in ABC's decisions not to hire.<sup>21</sup>

ABC was required to provide pre-adverse action disclosures before rejecting the applicants and notices of adverse action once the decisions not to hire the applicants were finalized, even though the information in the credit reports was not the only factor in the decisions not to hire.

Upon a consumer's request, a CRA must disclose all information in that consumer's "file,"<sup>22</sup> along with a summary of consumer rights under the FCRA that the FTC has published. If a consumer disputes the completeness or accuracy of information in such a consumer report, then upon notice from the consumer the CRA must reasonably investigate the charge – unless the consumer fails to provide sufficient information upon which to verify the disputed information. If a consumer contacts a CRA and identifies himself or herself as a victim of fraud or identity theft, then the CRA is required to provide the consumer with a special notice and summary of rights that the FTC has published.

### 3. FTC Red Flags Rule

The Red Flags Rule (the "Rule") is a regulation that the FTC and federal banking agencies jointly issued that requires financial institutions and "creditors" to develop a written Identity Theft Prevention Program ("Program") to protect consumer personal information.<sup>23</sup>

The Rule applies to every financial institution and "creditor" that holds any consumer account or any other account for which there is a reasonably foreseeable risk of identity theft. The Rule defines "creditor" broadly and captures anyone who provides for payment in arrears (*i.e.*, any entity that accepts payment *after* the good or service has been provided). Acceptance of credit card payment does not – without more – subject an entity to the Rule.

<sup>21</sup> Please note that the use of credit histories in employment decisions may give rise to claims of employment discrimination. *See, e.g.*, U.S. Equal Employment Opportunity Commission Informal Discussion Letter, February 14, 2005, available at [www.eeoc.gov/foia/letters/2005/titlevii\\_credit\\_reports.html](http://www.eeoc.gov/foia/letters/2005/titlevii_credit_reports.html).

<sup>22</sup> A consumer's "file" is all of the information pertaining to the consumer that is recorded and retained by a CRA.

<sup>23</sup> Under FACTA, the FTC, Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation, Department of the Treasury (Office of Thrift Supervision) and National Credit Union Administration are all charged with promulgating identity theft regulations. Each agency is responsible for administering the Rule with regard to entities that fall within its jurisdiction.

Thus, financial institutions and creditors that offer or maintain “covered accounts” must develop and implement an identity theft prevention program. A “covered account” is: (i) an account primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions; or (ii) any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.

The Rule requires a financial institution or creditor to implement a written Program approved by its board of directors that allow the entity to:

- identify relevant patterns, practices, and specific forms of activity that are “red flags” signaling possible identity theft and incorporate those red flags into the Program;
- detect red flags that have been incorporated into the Program;
- respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- make sure that the Program is updated periodically to reflect changes in risks of identity theft.

Additionally, financial institutions and creditors must exercise “appropriate and effective” oversight over service providers.<sup>24</sup> Thus, companies must ensure service providers follow “reasonable policies and procedures” to detect, prevent and mitigate risk of identify theft.

The FTC’s original compliance deadline was November 1, 2008. However, the FTC changed the enforcement date to January 1, 2011. **Thus, enforcement of the Red Flags Rule will not commence until January 1, 2011, unless Congress passes legislation that limits the applicability of the Red Flags Rule and that legislation becomes effective prior to January 1, 2011.**

#### **4. Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act<sup>25</sup> (“GLBA”) applies to “financial institutions,” which generally includes any entity that significantly engages in any financial or nonfinancial activities customarily conducted by banks or other entities in the financial services industry. GLBA was enacted to increase competition in the financial services industry, by removing restrictions on affiliations among banks, securities firms, and insurance companies. These affiliations raise privacy concerns with regard to the quantity and nature of the “nonpublic personal information” that is regularly available to “financial institutions.”

Accordingly, the GLBA protects nonpublic personal information that financial institutions hold with regard to “consumers.” The GLBA, and regulations that implement it, impose two primary requirements on these entities: (i) notice obligations and restrictions on disclosure of consumer nonpublic personal information to nonaffiliated third parties (the “Privacy Rule”); and (ii) procedures to ensure confidentiality and protect against unauthorized access (the “Safeguards Rule”).

---

<sup>24</sup> A “service provider” is defined as “a person that provides a service directly to the financial institution or creditor.”

<sup>25</sup> Pub. L. No. 106-102, 113 Stat. 1338 (1999), codified at 15 USC § 6801 *et seq.* Information about the GLBA and related regulations is available at [www.ftc.gov/privacy/privacyinitiatives/glbact.html](http://www.ftc.gov/privacy/privacyinitiatives/glbact.html).

**Illustration.** MNOP Company is engaged in the business of providing “pay day” lending and check cashing services. XYZ Nonprofit is engaged in the business of providing credit counseling and tax preparation services. 123 Company sells retail goods and services and accepts payment in the form of cash, checks or credit cards that it did not issue, and allows purchasers to write a check for a higher amount than the goods or services are worth and obtain cash in return.

MNOP and XYZ are “financial institutions” within the meaning of the GLBA and are thus subject to the GLBA and its implementing regulations. 123 is not a “financial institution” and is not subject to the GLBA.

Privacy Rule compliance depends on the nature of the individual’s relationship with the financial institution. Generally, compliance is less onerous with respect to “consumers”<sup>26</sup> than “customers.”<sup>27</sup> The Privacy Rule requires financial institutions to provide notice of their privacy policies and practices to customers, once the customer relationship is established, and to consumers, before disclosing “nonpublic personal information”<sup>28</sup> (“NPI”) to a non-affiliated third party (except in certain situations). For the length of a customer relationship, a financial institution must provide customers with annual notice of its privacy policies and practices.

Privacy notices must state, among other things: (i) the categories of NPI collected and disclosed; (ii) the categories of affiliates and non-affiliated third parties with which NPI is shared; (iii) the consumer’s right to opt out of sharing certain NPI with non-affiliated third parties; and (iv) the financial institution’s policies and practices to protect NPI confidentiality and security. The Privacy Rule restricts the disclosure of NPI about consumers to non-affiliated third parties, as well as the use and disclosure of NPI received from non-affiliated financial institutions by those third parties. Specifically, a person or Business, regardless of whether it is a financial institution, can only use or disclose the NPI received from non-affiliated financial institutions in the ordinary course of business to carry out the purpose for which it was received, which may include disclosing the NPI to its affiliates.

The Safeguards Rule generally incorporates the Privacy Rule’s definitions, and applies to all customer-NPI in a financial institution’s possession. The Safeguards Rule requires financial institutions to develop, implement and maintain a comprehensive information security program. The program must contain administrative, technical and physical safeguards that are appropriate to the financial institution’s size and complexity, to the nature and scope of its activities, and to the sensitivity of NPI in its possession.

The Safeguards Rule also requires financial institutions to designate one or more employees to coordinate the information security program. Such employee(s) must also identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in its unauthorized disclosure, misuse, alteration or destruction. This risk assessment must also consider the risks associated with employee training and management and the financial institution’s means of information storage, transmission and disposal. Financial institutions must impose contractual

---

<sup>26</sup> A “consumer” is any individual (or the individual’s legal representative) who obtains a financial product or service from a financial institution that is to be used primarily for personal, family or household purposes (such as a home equity loan).

<sup>27</sup> A “customer” is a “consumer” with a “customer relationship” with the financial institution, which is a continuing or ongoing relationship between a consumer and a financial institution (such as a personal savings or checking account).

<sup>28</sup> “Nonpublic personal information” includes any “personally identifiable financial information” (broadly defined as any information provided by or otherwise obtained from a consumer) that is not “publicly available information.”

“Publicly available information” includes any information that a financial institution has a reasonable basis to believe is lawfully made available to the general public from federal, state or local government records, widely distributed media or public disclosures required to be made under federal, state or local law.

obligations on service providers to implement and maintain similar safeguards with respect to the customer NPI that they receive from the financial institution.

### **III. RECENT FEDERAL LEGISLATIVE PROPOSALS AND EMERGING TRENDS**

Below are summaries of the influential Massachusetts Standards for the Protection of Personal Information and two proposed bills for data privacy currently pending in the U.S. Congress. These developments illustrate an evolving shift away from static post-breach legislation to a fluid regulatory environment in which entities must be pro-active and take affirmative steps to limit the risk of security breaches.

#### **1. Massachusetts Standards for the Protection of Personal Information**

The Massachusetts Standards for the Protection of Personal Information (the “Massachusetts Standards”),<sup>29</sup> apply to individuals, corporations, associations and any other entity that owns or licenses “Personal Information” about a Massachusetts resident, whether in paper or electronic form. Consequently, the Massachusetts Standards also apply outside of Massachusetts, and the Massachusetts Attorney General’s office may pursue enforcement actions regardless of where an entity is located.

The Massachusetts Standards require entities to “develop, implement, maintain, and monitor a comprehensive, written information security program” that incorporates administrative, technical and physical safeguards to protect Massachusetts residents’ personal information. The Massachusetts Standards establish specific administrative, technical and physical safeguards that must be implemented. All entities that possess personal information relevant to a Massachusetts resident should therefore review the specific requirements to ensure compliance before the March 1, 2010 deadline.

The written information security program (the “Program”) must be reasonably consistent with industry standards and also with the safeguards for protection of personal information set forth in any state or federal regulations by which the covered entity may be regulated. Compliance is evaluated by taking into account: (i) the size, scope and type of business; (ii) the amount of resources available; (iii) the amount of stored data; and (iv) the need for security and confidentiality of both consumer and employee information. A covered entity’s Program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

#### **2. Proposed Federal Data Breach Notification Act**

The Data Breach Notification Act (“Notification Act”)<sup>30</sup> would be the first of its kind at the federal level. Currently, forty-four states have breach notification laws,<sup>31</sup> but no uniform federal law exists. As proposed, the Notification Act would require any business entity engaged in interstate commerce that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information in electronic or digital form to notify, after the discovery of a security breach, any U.S. resident whose information has been, or is reasonably believed to have been, accessed or acquired. An entity that does not own or license such information, but possesses it, must notify the owner or licensee of the information upon discovery of a breach. In all instances, notice must be provided without unreasonable delay.

---

<sup>29</sup> The Massachusetts Standards are codified at 201 C.M.R. 17, *et. seq.*, and implement M.G.L. ch. 93H.

<sup>30</sup> S. 139, 111<sup>th</sup> Congress (2009). As of September 2009, the bill remained in the Subcommittee on the Judiciary, where it was sent on January 6, 2009.

<sup>31</sup> As discussed in Section I, above, Connecticut, New Jersey and New York have breach notification laws.

The Notification Act defines “sensitive personally identifiable information” as any information, or compilation of information, in electronic form that includes:

- an individual’s first and last name or first initial and last name in combination with any one of the following:
  - o a non-truncated SSN, driver’s license number, passport number or alien registration number
  - o any two of:
    - home address or telephone number
    - mother’s maiden name (if identified as such)
    - month, day and year of birth
  - o unique biometric data (*e.g.*, finger or voice prints)
  - o a unique account identifier, electronic identification number, user name or routing code in combination with the access code or password that is required for an individual to obtain money, goods, services or any other thing of value; or
- a bank or credit card number in combination with the access code or password that is required for an individual to obtain credit, withdraw funds or engage in a financial transaction.<sup>32</sup>

The Notification Act would not require notification if a risk-assessment investigation finds that the security breach did not, or will not, result in a significant risk of harm to the affected individual. The risk assessment must be submitted to the U.S. Secret Service and, unless the Secret Service responds that notice is necessary, no further action is required. Another exception to notification exists if the business determines, and certifies in writing, that notification reasonably could be expected to cause damage to the national security or hinder a law enforcement investigation. The Notification Act presumes that a significant risk does not exist if the personally identifiable information is encrypted.

Violation of the Notification Act may result in a civil penalty of up to \$1,000 per day per affected individual. The penalty may increase for intentional or willful violations. No private right of action is provided. Instead, the Attorney General, a state attorney general, or a designated representative of a state attorney general is granted exclusive jurisdiction to enjoin and prosecute violations.

The Notification Act would preempt state breach notification laws and provide a national, uniform standard if it becomes law. Under the national standard, notice must include a description of the type of sensitive personally identifiable information that was breached, a toll-free number of the entity providing notification, and the toll-free numbers and addresses for the major credit reporting agencies. Individual States may require that notice also include information regarding victim assistance provided for by that State.

### **3. Proposed Federal Data Accountability & Trust Act**

The Data Accountability & Trust Act (“DATA”)<sup>33</sup> would direct the FTC to issue regulations that require businesses to establish security policies to protect consumers’ personal information maintained in

---

<sup>32</sup> Please note that the definition of “sensitive personally identifiable information” is similar to the definition of “Personal Information” subject to the laws of Connecticut, New Jersey and New York, discussed in Section I.2, above, and the definition of “personal information” in Section III.3, below.

<sup>33</sup> H.R. 2221, 111<sup>th</sup> Congress (2009).

electronic form. As proposed on April 30, 2009, DATA would create a national data privacy standard that preempts the patchwork of state laws in this area.

The FTC regulations would apply to any entity engaged in interstate commerce that owns or possesses electronic data containing personal information and requires establishment of security policies and procedures. Entities that contract for third party service providers to maintain such information are not exempt from the statutory requirements.

The FTC regulations would require covered entities to enact procedures to protect personal information, including by: (i) creating a security policy that applies to the collection, use, sale, dissemination and maintenance of personal information; (ii) identifying a head information security officer; (iii) creating procedures to identify and reasonably access foreseeable vulnerabilities and regularly monitor for security breaches; (iv) adopting measures to mitigate vulnerabilities; and (v) establishing methods to destroy obsolete electronic data. The construction of a security system must take into account the size, nature, scope and complexity of the entity's business activities, as well as the current state of the art in administrative, technical and physical safeguards for protecting such information, and the cost of implementing such safeguards.

DATA also contains notification provisions similar to those set forth in the Notification Act. DATA defines "personal information" broadly, and includes an individual's first name or initial and last name, or address, or phone number in combination with any one or more of the following data elements for the same individual:

- social security number;
- driver's license number or State identification number; or
- any financial account number, or credit or debit card number, and any required security code, access code or password that is necessary to permit access to an individual's financial account.

Exclusive enforcement authority is vested in government actors, thus barring private rights of action. Violations are enforced by the FTC or a state attorney general and may result in injunction against infringing practices, compliance orders or civil monetary penalties of up to \$11,000 per violation per day, with maximum damages of \$5,000,000.

#### **IV. PRACTICAL SUGGESTIONS**

This section of the Primer sets out a few practical suggestions a Business can consider during its preparations to comply with the laws discussed in Sections I and II above.<sup>34</sup>

##### **1. Conduct a Privacy and Security Audit**

A privacy and security audit can help a Business to understand the type of Personal Information the Business collects and how the Personal Information is collected, used and discarded. The audit will identify areas where the Business is not in compliance with the laws discussed in Sections I and II above.

---

<sup>34</sup> For specific suggestions relating to complying with HIPAA's requirements, please see *HIPAA Primer for Nonprofit Social Services Agencies*, available at [www.probonopartnership.org/publications.htm](http://www.probonopartnership.org/publications.htm).

There is no effective “one size fits all” audit design. Rather, an audit should be tailored according to the Business’ particular scope of operations and organizational structure. In designing and conducting an audit, the following factors and questions normally should be considered:

Information Collection:

- What information is collected and by whom?
- Is this information required for a legitimate business need?
- Is this information used for any other purposes? Are these other uses authorized and legally permissible?

Information Storage and Disposal:

- Once the information has been collected, how is it stored? Is it secure?
- Once it is stored, who has access to that information and how do those people get access?
- Once the information is no longer required, what happens to the records?
- Is there someone who is responsible for managing this process and keeping track of the information that is stored and destroyed? Does your organization need a privacy and security officer?

Risk Assessment:

- Review and analyze all past security breaches and risks of security breaches.
- Analyze, assess and respond to any potential security vulnerabilities.
- Conduct a technical security audit. What are the technical safeguards in place? Are they consistent with industry standards? How could they be improved?
- Does your organization engage any third-party providers? If so, analyze third-party vendors’ abilities to comply with your privacy and security policy.
- Analyze employee training.
- Analyze employee disciplinary procedures.
- Create a system for documenting, analyzing and responding to all breaches.
- Create procedures for annual review of the privacy and security policy.
- Does your organization have a plan for responding to breaches of Personal Information?

Other Activities:

- Does your organization transmit Personal Information or PHI electronically, or contract with a third party to electronically transmit PHI? If so, is it encrypted?
- Does your organization use reports from CRAs in evaluating applicants for employment or current employees for promotions?
- Does your organization allow customers to defer payment for goods and services?
- If the answer to the last question is yes, does your organization have “covered accounts”?
- Does your organization engage in financial activities?
- Does your organization receive NPI from financial institutions?

## **2. Prepare a Privacy and Security Policy**

Once the Business has completed the privacy and security audit, it should use this information to prepare a privacy and security policy. At a minimum, the policy should clearly define what information collected by the Business is subject to the policy and should address the following general matters:

- (i) all Personal Information that is collected, regardless of from whom it is collected, should be collected only if it is required for a legitimate business need;
- (ii) all Personal Information, particularly SSNs and credit/debit card numbers, must be stored in a secure fashion by ensuring computer files are password protected and paper records are stored in locked cabinets;
- (iii) no Personal Information should be publicly displayed, used for passwords or ID cards, or printed on any forms or mailings that could be seen by unauthorized persons;
- (iv) all records, whether paper or electronic, containing Personal Information must be adequately destroyed or otherwise made unreadable prior to being disposed of;
- (v) electronic transmission of Personal Information via the Internet should always be encrypted; and
- (vi) a contact person should be designated to oversee the implementation and enforcement of the policy, to answer questions about the policy and to receive reports about actual or suspected breaches of security or the policy.

While the above items are only the general matters that should be addressed by a privacy and security policy, each Business should ensure that its policy is detailed and addresses its specific operations and risks.

The privacy and security policy should be publicly displayed (*e.g.*, posted on the Business' website) and communicated to all employees and contractors. Employees working directly with Personal Information should receive periodic training about the policy.

## **3. Prepare an Action Plan in the Event of a Security Breach**

Each Business should develop an action plan for dealing with a breach (or potential breach) of the security of its electronic and physical systems for maintaining of Personal Information. The action plan can be part of the privacy and security policy. The Business should designate a notification coordinator and establish a team of employees to address a breach. Depending on the nature of a Business' workforce, this team should consist of technology, public relations and legal experts who can take the appropriate action to fix the security breach and notify law enforcement, if necessary, and all affected individuals. The team members should be trained on the Business' privacy and security policy and the steps to be taken in the event of a security breach.

At a minimum, the action plan should provide for the team to take the following actions: (i) evaluate the incident and determine whether a breach occurred (or was likely to have occurred) and make a determination as to whether notification is required; (ii) document the investigation and notification determination; (iii) review the notification requirements in each applicable state, including whether law enforcement must be contacted; and (iv) prepare the notices to be delivered to the affected customers and keep a record of each notification made.

#### 4. Helpful Resources

Federal Trade Commission – Fair Credit Reporting Act Information	<a href="http://www.ftc.gov/os/statutes/fcrajump.shtm">www.ftc.gov/os/statutes/fcrajump.shtm</a>
Federal Trade Commission – Gramm-Leach-Bliley Act Information	<a href="http://www.ftc.gov/bcp/menus/business/credit/reports.shtm">www.ftc.gov/bcp/menus/business/credit/reports.shtm</a> <a href="http://www.ftc.gov/privacy/privacyinitiatives/glbact.html">www.ftc.gov/privacy/privacyinitiatives/glbact.html</a> <a href="http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus67.shtm">www.ftc.gov/bcp/edu/pubs/business/idtheft/bus67.shtm</a> <a href="http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.shtm">www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.shtm</a>
Federal Trade Commission – Identity Theft Home Page	<a href="http://www.ftc.gov/bcp/edu/microsites/idtheft">www.ftc.gov/bcp/edu/microsites/idtheft</a>
Federal Trade Commission – Identity Theft Guide for Business	<a href="http://www.ftc.gov/infosecurity">www.ftc.gov/infosecurity</a>
Federal Trade Commission – Red Flag Rules How-To Guide for Business	<a href="http://www.ftc.gov/redflagsrule">www.ftc.gov/redflagsrule</a>
U.S. Department of Health & Human Services – HIPAA Privacy	<a href="http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html">www.hhs.gov/ocr/privacy/hipaa/understanding/index.html</a>
U.S. Department of Health & Human Services, Center for Medicare & Medicaid Services – HIPAA Information	<a href="http://www.cms.hhs.gov/HIPAAGenInfo">www.cms.hhs.gov/HIPAAGenInfo</a>
Connecticut Attorney General’s Office – Identity Theft Home Page	<a href="http://www.ct.gov/ag/cwp/browse.asp?A=2066&amp;BMDRN=2000&amp;BCOB=0&amp;C=19200">www.ct.gov/ag/cwp/browse.asp?A=2066&amp;BMDRN=2000&amp;BCOB=0&amp;C=19200</a>
Connecticut Department of Consumer Protection – Identity Theft Fact Sheet	<a href="http://www.ct.gov/dcp/lib/dcp/pdf/factsheets/id_theft_2009.pdf">www.ct.gov/dcp/lib/dcp/pdf/factsheets/id_theft_2009.pdf</a>
New Jersey Attorney General’s Office – Identity Theft Home Page	<a href="http://www.nj.gov/lps/dcj/idtheft.htm">www.nj.gov/lps/dcj/idtheft.htm</a>
New Jersey Division of Consumer Affairs – Identity Theft Home Page (including information on the NJ Identity Theft Prevention Act)	<a href="http://www.state.nj.us/lps/ca/idtheft.htm">www.state.nj.us/lps/ca/idtheft.htm</a>
New Jersey Division of Consumer Affairs – Identity Theft Guide for Business	<a href="http://www.state.nj.us/lps/ca/brief/idtheftbus.pdf">www.state.nj.us/lps/ca/brief/idtheftbus.pdf</a>
New York State Attorney General’s Office – Identity Theft Home Page	<a href="http://www.oag.state.ny.us/bureaus/consumer_frauds/identity_theft.html">www.oag.state.ny.us/bureaus/consumer_frauds/identity_theft.html</a>
New York State Attorney General’s Office – NY Information Security Breach and Notification Act	<a href="http://www.oag.state.ny.us/bureaus/consumer_frauds/tips/id_theft_law.html">www.oag.state.ny.us/bureaus/consumer_frauds/tips/id_theft_law.html</a>

New York State Office of Cyber Security &  
Critical Infrastructure Coordination  
– NY Information Security Breach and Notification  
Act

[www.cscic.state.ny.us/security/securitybreach/index.cfm](http://www.cscic.state.ny.us/security/securitybreach/index.cfm)

New York State Consumer Protection Board  
– Business Privacy Guide

[www.nysconsumer.gov/pdf/the\\_new\\_york\\_business\\_guide\\_to\\_privacy.pdf](http://www.nysconsumer.gov/pdf/the_new_york_business_guide_to_privacy.pdf)

## APPENDIX A: RELEVANT TRI-STATE LAWS

While the substance of the applicable laws in Connecticut, New Jersey and New York are similar, these states have taken different approaches to enacting their laws. Below is a brief description of the relevant laws in each state.

Connecticut. The Connecticut “An Act Requiring Consumer Credit Bureaus To Offer Security Freezes”,<sup>35</sup> requires Connecticut Businesses to provide notice of breaches of the security of personal information. The Connecticut “ An Act Concerning The Confidentiality Of Social Security Numbers” requires Connecticut Businesses to create a privacy protection policy to protect personal information.<sup>36</sup> The Connecticut law relating to the “Display and Use of Social Security Numbers” prohibits Connecticut Businesses from willfully displaying SSNs publicly.<sup>37</sup>

Both “An Act Requiring Consumer Credit Bureaus To Offer Security Freezes” and the Connecticut law relating to the “Display and Use of Social Security Numbers” are enforced by the Connecticut Attorney General.<sup>38</sup> For persons that hold a state license, registration or certificate, “An Act Concerning The Confidentiality Of Social Security Numbers” is generally enforced by the agency that issued such license, registration or certificate.

New Jersey. In New Jersey, the primary statute is the Identity Theft Prevention Act,<sup>39</sup> which seeks to prevent identity theft and creates certain protections and remedies related to identity theft with respect to the citizens of New Jersey. This act also creates certain duties and obligations on entities doing business in New Jersey. The New Jersey law is enforced by the New Jersey Attorney General through the New Jersey Division of Consumer Affairs.<sup>40</sup>

New York. In New York, the relevant laws relating to protection of personal information, notification of breaches of the security of such information and destruction of employee personal records are set out in various sections of the New York General Business Law.<sup>41</sup> The New York Labor Law also includes a section which specifically addresses New York employers’ use and dissemination of employee personal identifying information.<sup>42</sup>

---

<sup>35</sup> Connecticut Public Act No. 05-148, available at [www.cga.ct.gov](http://www.cga.ct.gov).

<sup>36</sup> Connecticut Public Act No. 08-167, available at [www.cga.ct.gov](http://www.cga.ct.gov).

<sup>37</sup> Connecticut General Statute 42-470., available at [www.cga.ct.gov](http://www.cga.ct.gov).

<sup>38</sup> The website for the Connecticut Attorney General is available at [www.ct.gov/ag/site/default.asp](http://www.ct.gov/ag/site/default.asp).

<sup>39</sup> New Jersey Public Law 2005, Chapter 226, N.J.S.A. 56:11-44 *et. seq.*, available at [www.njleg.state.nj.us/2004/Bills/PL05/226\\_.HTM](http://www.njleg.state.nj.us/2004/Bills/PL05/226_.HTM) or [www.state.nj.us/lps/ca/idtheft.htm](http://www.state.nj.us/lps/ca/idtheft.htm).

<sup>40</sup> The New Jersey Division of Consumer Affairs has a website relating to the New Jersey Identity Theft Protection Act at [www.state.nj.us/lps/ca/idtheft.htm](http://www.state.nj.us/lps/ca/idtheft.htm). This website includes a “Guide for Business,” at [www.state.nj.us/lps/ca/brief/idtheftbus.pdf](http://www.state.nj.us/lps/ca/brief/idtheftbus.pdf).

<sup>41</sup> New York General Business Law § 899-aa deals with notices of breaches of the security of private information. New York General Business Law §399-dd addresses the reasonable measures a business must take to protect SSNs. New York General Business Law §399-h sets out the measures a New York employer must take when disposing of employee personal records.

<sup>42</sup> New York Labor Law §203-d.

---

IRS Circular 230 Disclosure: To ensure compliance with requirements imposed by the IRS, we inform you that any tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of: (i) avoiding penalties under the Internal Revenue Code or any other U.S. federal tax law; or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein.

This document is provided as a general informational service to volunteers, clients and friends of the *Pro Bono Partnership*. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does distribution of this document create an attorney-client relationship.

Copyright 2010 Dechert LLP. All rights reserved. No further use, copying, dissemination, distribution, or publication is permitted without the express written permission of Dechert LLP.

Revised June 2010