





- Step One:** Identify and document material internal and external security risks.
- Step Two:** Design and implement reasonable safeguards to address the PII security risks.
- Step Three:** Limit access to physical data and devices.



- Step Four:** Develop a policy for discarding PII.
- Step Five:** Monitor for problems.
- Step Six:** Make your employees an active and positive part of your data security plan.
- Step Seven:** Provide for oversight by the Board of Directors or senior management.



Step Eight: Have procedures in place to address security breaches.

Step Nine: Extend your program to service providers.

Step Ten: Periodically test, evaluate and adjust the program.

Questions?

Robert M. Bryan
rbryan@rbh.com

Robert E. Harrington
rharrington@rbh.com

ROBINSON BRADSHAW & HINSON

DEVELOPING A DATA SECURITY PROGRAM

Over the last decade, identity theft has become a significant national problem. Businesses already incur material out-of-pocket costs for identity theft, and experts caution that the failure to address this problem could lead to an even more costly problem: loss of consumer confidence in electronic commerce. High profile incidents have increased public awareness of the problem and prodded public officials into acting.

Despite the seriousness of this threat, we still lack any comprehensive federal law that deals with the problem of data security in a uniform fashion. Instead, every business now faces the daunting task of complying with a patchwork of state, federal and foreign laws seeking to protect personal data. For many businesses, these requirements are supplemented by industry-specific laws and regulations and the rules of industry associations.

To date, enforcement of these laws, rules and regulations has been sporadic, leaving many businesses with a false sense of comfort that the patchwork of rules can be largely ignored until the federal government brings order to the chaos (at some unknown future time) by adopting uniform national rules. But there are signs of change. Enforcement by the FTC and the states is increasing and some recent laws have provided for more meaningful penalties and increased the risk of private consumer class action law suits challenging security lapses. The risk of noncompliance is starting to grow.

This paper seeks to bring some order to this chaos and provide some usable and commercially reasonable guidelines for an acceptable data security program. In the first part of the paper, we briefly put the problem in context by explaining how data security concerns relate to the more general concept of privacy laws, and by listing the key developments that are leading to the expansion of data security law in the United States. In the second part, we briefly discuss the complex, and often conflicting, body of law and regulation that governs this area. Finally, in the last part, we provide a step-by-step guide to developing an adequate data security program.

I. The Evolution of Data Security Law

Notions of privacy have developed differently in different parts of the world. For historical and ideological reasons, Europeans have generally been far more concerned about privacy protection than Americans. There are still tens of millions of Europeans who remember living under totalitarian regimes that kicked in doors in the middle of the night and demanded to see “papers.” Consequently, more than a decade ago, the European Union took a strong position in favor of protecting “personal data” against any intrusion, public or private, and imposed strict controls on the collection and transmission of such data. The EU regards privacy as a fundamental human right and its legal protection of personal data is much more expansive than would be required merely to deal with the commercial problems of identity theft. Many other countries have followed the EU’s lead.

Lacking a comparable historical experience, the United States has been more reluctant to view the protection of privacy as a broad fundamental right. While the U.S. Constitution

ROBINSON BRADSHAW & HINSON

provided certain limited protections against government intrusion, there was no express general protection of privacy in early U.S. law. The genesis of U.S. privacy law as we know it today was a famous law review article by Samuel Warren and Louis Brandeis in 1890 that argued for a tort-based right to prohibit public intrusion into private matters and to prevent the publication of private information. Subsequently, the Supreme Court created broader constitutional protection for privacy under the “penumbra” of other rights that are expressly stated in the Constitution.

Today there are tort-based privacy rights in the U.S., as well as a limited Constitutional right to privacy. A significant number of statutes regulate the government’s right to collect and use private information and there are broad laws protecting the privacy of certain financial and health-related information. But the general notion of privacy as a fundamental right is still far less developed in the U.S. than in Europe and much of the rest of the world.

The recent expansion of privacy law in the United States evidences a different concern. The United States has always been focused on preserving the benefits of capitalism and the free market, while appropriately protecting the rights of consumers. Not surprisingly, this concern has carried over into privacy law and, as a result, the United States has been increasingly aggressive in protecting personal data that is collected and used for commercial reasons. Privacy law can cover a wide range of concerns about the use of personal data, including limits on what data can be collected, shared and retained, and an expansion of the rights of the consumer to understand and control that process. This paper focuses specifically on one area of privacy law that has not traditionally been a central focus, but that is becoming increasingly important: the steps that must be taken to protect collected personal data from misuse by third parties.

Much of the early development of data security law in the United States grew out of privacy policies. Companies were not generally required to post a privacy policy, but, if they did, they had to live up to whatever promises they made with respect to data security. The Federal Trade Commission has long treated a failure to live up to the terms of an announced privacy policy as an unfair trade practice that violates Section 5 of the FTC Act. Since there is no private right of action under Section 5, the major risk has always been an enforcement action by the FTC itself.

More recently, the emphasis in the U.S. has shifted from merely enforcing whatever promises companies made in their privacy policies to establishing minimum standards for how companies must protect “personally identifiable information” (PII). The definition of PII will vary from statute to statute, but generally PII includes a person’s name together with the types of identifying information that would be useful in connection with identity theft, such as account numbers, passwords, personal identification numbers, social security numbers, license numbers and common security verification information such as a mother’s maiden name. There is often an exception for information that is available in public data bases. While most data security discussions focus on electronic data, some of the relevant statutes and regulations also apply to information that is manually collected and stored in paper files.

This change in emphasis has been driven by five significant developments. The first of these developments is the rapid expansion of state data security law, with California taking the lead and enacting statutes that other states have quickly imitated. In fact, California’s leadership

ROBINSON BRADSHAW & HINSON

has been so strong that until very recently, compliance with California law virtually ensured compliance nationwide. In the past year or so, Nevada, Massachusetts, and some other states have enacted specific data security requirements that go beyond California's in some respects.

The second development is the FTC's decision to apply Section 5 of the FTC Act as if it were a general national data security law. Specifically, the FTC has determined in recent years that it is an unfair practice under Section 5 for a business to fail to maintain an information security program that is reasonably designed to protect PII, whether or not the business has a privacy policy that promises that level of protection. Just within the past year, the FTC has obtained consent decrees from both retailers and data brokers whose privacy policies and practices were deemed inadequate.

The third development is the adoption and continual strengthening of sector-specific data security laws. Federal laws and regulations in the areas of banking, finance, credit, and health care now limit the collection and dissemination of PII and outline the kinds of protection policies that companies must adopt and follow. In terms of the burdens imposed on companies, there is good news and bad. First the bad: the definitions of the covered sectors are often broader than business people might expect. But the good news is that the data security requirements that are imposed are usually not onerous, and consist largely of sound business practices that companies would probably want to adopt anyway, and that may be also required by the FTC regulations and state law.

The fourth development is the increasing importance of foreign law to U.S. companies as business becomes more international. For example, European Union law specifically makes any company collecting PII responsible for the security, integrity and accuracy of the data, and restricts transfer to third parties. American companies with operations in Europe are covered directly by this law, and U.S. companies that collect substantial amounts of PII from EU citizens may be as well. U.S. companies that acquire PII from EU sources may have to either adopt EU-level protections on their own or enter into onerous form data-transfer contracts approved by the EU.

The fifth development is the promulgation (and contractual enforcement) of codes of conduct by particular industries. The most significant may be the highly technical security standards adopted by the credit card industry, which can be enforced by the card brands through fines or restrictions on noncompliant merchants.

II. THE SOURCES OF DATA SECURITY LAW

This section of the paper will present a brief overview of the laws that impose obligations with respect to data security. As discussed above, data security law is currently derived from multiple sources. This paper is organized by source: state law, general federal law, sector-specific federal law, industry standards, and foreign law.

ROBINSON BRADSHAW & HINSON

A. State Law

State privacy laws throughout the country have generally followed California's lead. When dealing with general privacy issues, companies have often thought it was safe to assume that compliance with California law would also bring them into material compliance with the privacy laws in most other states. The landscape is more complex on data security issues, with some other states recently adopting laws that are even more stringent than the laws in California.

1. *Required Level of Security.* A patchwork of state laws set forth varying requirements for the required level of security. Certain states (including California, Nevada, Arkansas and Massachusetts, as of January 1, 2010) impose a general requirement on businesses that hold PII of their residents to implement and maintain reasonable security measures to protect such information. California also requires businesses that share personal information under a contract with a third party to require the third party to implement and maintain procedures securing such information.

Many states also have more specific requirements. For example, California restricts financial institutions from sharing customer information among company units (although the law has been partially invalidated by the Ninth Circuit Court of Appeals on preemption grounds and has been accepted for further review by the U.S. Supreme Court). North Carolina and other states have laws prohibiting businesses that hold social security numbers of their residents from communicating, disclosing, or trading such numbers. California, Michigan and Florida have similar rules in the employment context. Some states now bar merchants from requesting the customer to provide additional identifying information (such as a phone number) in connection with a credit card sale.

Two new laws take a radically different approach to the physical security of PII. Nevada now requires that a company encrypt PII before transferring the data outside its own "secure boundaries." This statute has already generated extensive commentary because of its many ambiguities. It covers all "businesses within the state" of Nevada, but the meaning of this phrase is unclear. Equally unclear is whether the law covers PII collected from people outside Nevada. A similar Massachusetts law, which takes effect on January 1, 2010 (the effective date has already been postponed twice because of the deteriorating economy), may be even stricter. While the Nevada law regulates only the transmission of PII, the Massachusetts version also requires the encryption of all portable PII, including data stored on laptops or removable memory devices. As with Nevada, the scope of the Massachusetts law is unclear, particularly as it relates to businesses that are physically located outside the state but electronically collect information from state residents.

The practical impact of these two new laws is uncertain. If applied broadly, the Nevada and Massachusetts laws could impose onerous requirements on many out-of-state businesses. And some commentators believe that we will see a repeat of the California phenomenon, with multiple states imitating the encryption requirement. New Jersey already has such a bill under discussion. On the other hand, there has already been business pressure in Massachusetts to make the law more flexible, and there is some doubt as to whether the states have the Constitutional authority to impose their encryption requirement on transactions involving interstate commerce.

ROBINSON BRADSHAW & HINSON

Some plaintiffs' lawyers have attempted to expand the scope of protection beyond the statutory requirements by seeking to hold businesses liable for the claimed breach of a non-statutory common law obligation of adequate security. Late last year, for example, a court approved a settlement in a class action that charged the retailer TJX with inadequate monitoring of its computer systems that resulted in widespread disclosure of consumers' PII. Although the class members received only vouchers and other modest relief, TJX had to pay the lawyers for the class \$6.5 million in fees. This is not a well defined area, and the extent to which it will become a major issue may depend on the nature of future state and federal laws.

2. Security Breaches. Almost all state laws require that notice be given to consumers whose PII has been lost or misappropriated. (Currently, only Alabama, Kentucky, Mississippi, Missouri (which has a proposed law pending), New Mexico and South Dakota lack such laws.) State laws vary as to whether non-electronic records are covered, whether notice must be given upon any discovery of breach or only in accordance with a risk-based assessment, and whether there is any specified content for the notice. California is the leader in this area, and a majority of states now follow its model. Consequently, California law is an efficient place to start if a possible multi-state breach is suspected. The California state government has an extensive privacy website that provides detailed advice about compliance. California has recently added all health information to the category of PII whose disclosure triggers a mandatory security breach notification. Minnesota has a broad law limiting the credit card-related information that can be retained by a merchant and shifting some of the costs of notification of security breaches from the issuing bank to the non-compliant merchant.

3. Disposal of PII. This problem, too, is governed by multiple state laws. North Carolina's law follows a widespread model. In general, the state laws require a business to take reasonable steps to prevent unauthorized third party access to discarded PII. This would require that paper records be physically destroyed (usually by shredding) and that any medium containing electronic information (including the hard drive on computers to be replaced) be physically destroyed or demagnetized so that deleted electronic information could not be reconstructed.

B. General Federal Law

There are a number of federal data security laws that apply specifically to businesses in the financial and health care industries (as discussed below) and a separate, but substantively similar, body of data security law that applies generally to all other businesses.

1. Required Level of Security.

a. Posted Privacy Policies. Although Federal law still does not contain any general requirement that a company either have or post a privacy policy, the FTC views any statements about data security that a company does make in its privacy policy as a "promise," and views the failure of a business to comply with its security promises as an unfair or deceptive practice under Section 5 of the FTC Act. Even

ROBINSON BRADSHAW & HINSON

general statements that information will be held in confidence will be interpreted as a promise that there will be some reasonable level of security. One particular problem area can be marketing-driven statements to the effect that “we view your personal data as important and use state-of-the-art procedures to protect it.” In some cases, “privacy promises” may exist in other documents, such as marketing materials, employee policies and representations to third-party certification groups.

- b. *Additional Substantive Requirements.* The FTC has held in recent years that it is an unfair practice under Section 5 of the FTC Act for a business to fail to maintain an information security program that is reasonably designed to protect PII, even if it does not expressly promise to do so in a privacy policy (and probably even if it includes disclaimers about its security in its privacy policy). A security program would have to have at least the following elements to be considered adequate: (i) an employee responsible for the program; (ii) the identification of material internal and external security risks; (iii) the design and implementation of reasonable safeguards to control those risks; and (iv) the periodic evaluation and adjustment of the program. In addition, the Fair Credit Reporting Act requires every merchant to truncate credit card numbers and avoid the use of expiration dates on any electronic receipt. Finally, there are bills pending in Congress that would create federal limits on the collection and use of Social Security numbers.
2. *Security Breaches.* There is no generally applicable federal law requiring that consumers be notified of security breaches, although the FTC would require that a company comply with any promised steps in its privacy policy. During each of the last three years, Senator Dianne Feinstein has introduced legislation seeking to establish a federal security breach notice obligation, with the program to be administered by the Secret Service. Given the proliferation of partially inconsistent state laws, some experts believe that a federal law in this area is becoming more likely.
3. *Disposal of PII.* As in so many other areas, there is no generally applicable federal law governing the disposal of PII. Once again, the FTC would require that a company comply with any promised steps in its privacy policy. In addition, the Fair Credit Reporting Act Information Disposal Rule requires that any company that possesses a consumer report for any business purpose (such as deciding whether to grant credit) must use reasonable precautions in connection with the disposal of that information.
4. *Behavioral Advertising.* The FTC has been reviewing online behavioral advertising, which involves the tracking of a consumer’s website use to determine the consumer’s interests and provide advertising targeted at those interests. While this type of activity typically does not involve the collection or disclosure of traditional PII, it is still viewed as raising data security risks. At this point, the FTC has identified certain basic principles that should govern behavioral advertising (including notice, an opt-out right and adequate security for the collected data), and has encouraged industry self-regulation.

C. Finance: The Gramm-Leach-Bliley Act

1. *Scope of Coverage.* The Gramm-Leach-Bliley Act (GLB) covers the collection, protection and disclosure of personal financial information by “financial institutions.” The term “financial institutions” is not limited to traditional banks, securities firms and insurance companies, and also includes any other company that engages in a wide range of “financial activities.” However, the GLB data security rules (in particular the FTC Safeguards Rule, discussed in the next paragraph) applies only to companies that engage in such financial activities in a significant way; their coverage does not appear to extend to businesses that provide only incidental financial services such as accepting credit cards, allowing users to get cash back from debit purchases or checks, or allowing occasional layaway purchases. In a close case, the most critical factors in determining the applicability of the rule will be whether there is any formal relationship with respect to the potential financial transaction and the frequency of the activity. GLB is enforced by federal banking agencies, the SEC and the CFTC as it applies to traditional financial institutions, and by the FTC as it applies to other less traditional financial companies.

2. *Data Security Requirements.* The FTC has adopted a Safeguard Rule to carry out its GLB regulatory mandate with respect to data security. The FTC Safeguards Rule requires each covered financial institution to develop a written information security plan that describes its program to protect customer information. The security program must contain administrative, technical and physical safeguards that are appropriate to the institution’s size and complexity, the nature and scope of its activities and the sensitivity of the consumer information that it handles. As part of its information security program, each covered financial institution must (a) designate an employee or employees to coordinate its program; (b) identify the risks to the security of customer information and assess the safeguards in place to control these risks with a risk assessment program that covers each relevant area of an institution’s operations, including employee training and management, information systems, and detecting and preventing system intrusions; (c) design, implement, and monitor information safeguards; (d) oversee service providers by selecting providers that are capable of safeguarding customer information and requiring the providers by contract to maintain information safeguards; and (e) evaluate and adjust its program in light of relevant circumstances, including results of monitoring or changes in business operations. The Safeguards Rule does not require any specific safeguards beyond these listed, but allows each institution to tailor its program to its particular circumstances. However, in a guide for businesses, the FTC has suggested specific practices that financial institutions should consider implementing.

D. Credit: FACTA

1. *Scope of Coverage.* The Fair Credit Reporting Act (FCRA) was initially enacted to regulate the use and disclosure of consumer credit reports by credit reporting agencies, but was amended and expanded by FACTA in 2003. Among other things, FACTA now requires certain “financial institutions” (defined narrowly to include only banks, savings and loan associations, credit unions or any other persons who hold an account belonging to a consumer) and “creditors” (defined as anyone who regularly extends, renews, or continues credit or regularly arranges for the extension, renewal, or continuation of

ROBINSON BRADSHAW & HINSON

credit) that hold “covered accounts” to develop and implement an Identity Theft Prevention Program. The definition of “covered accounts” has two prongs. First, it covers most consumer accounts by broadly including any account used primarily for household, family or personal purposes that involves or is designed to permit multiple transactions. Second, it provides partial coverage for small businesses and sole proprietorships by including any other accounts for which there exists a reasonably foreseeable risk of identity theft. While each company will have to exercise discretion in determining which small business accounts meet the second prong of the test, factors to consider will include any history of identity theft, the nature of any existing controls and protections (including both access controls and internal security procedures), the level of risk (including the size, value and method of access to accounts), the way in which accounts are created, the number of individuals who can access the account, and the type of transactions conducted through the account. Taken together, these complex definitional terms would include under FACTA any store with an in-house credit card program, service providers who typically bill for their services (such as doctors) and any other business that provides regular periodic services that are paid for after the services are provided (such as lawns services and exterminators) but would exclude merchants that accept only third party credit cards such as Visa or MasterCard.

The federal banking agencies and the FTC have issued joint FACTA regulations. Financial institutions that are supervised by the federal banking agencies, the SEC, and the CFTC had a compliance deadline of November 1, 2008. The banking agencies have made compliance part of the bank examination process. For “creditors” and other financial institutions that fall within the FTC’s jurisdiction, the compliance deadline has been extended to August 1, 2009.

2. *Data Security Requirements.* Under FACTA, financial institutions and creditors that hold “covered accounts” must put in place an Identity Theft Prevention Program. The program centers on “Red Flag Activities” that should reasonably alert a company to a potential security risk, and the FACTA regulations discuss in detail the types of facts and circumstances that would constitute Red Flag Activities and include a nonexclusive illustrative list of 26 Red Flag Activities. The covered company must: (a) identify those Red Flag Activities that are potential risks for its covered accounts and incorporate any new Red Flag Activities into the program; (b) implement procedures to detect any Red Flag Activities that actually occur in covered accounts; (c) respond to any such Red Flag Activities that have been detected; and (d) update the program periodically to incorporate new risks. FACTA imposes detailed administrative and procedural requirements on the program, including a required level of participation by the Board of Directors and a required level of training. The regulations include Guidelines which must be followed absent a good reason for an exception. If any covered entity outsources any of the relevant activities, it must ensure that its service providers are in compliance with FACTA. As noted above, the deadline for implementing the program was November 1, 2008 in the case of traditional financial institutions supervised by the federal banking agencies, the SEC, and the FTC, and will be August 1, 2009 in the case of creditors and other financial institutions within the FTC’s enforcement jurisdiction.

E. Health Information

1. Scope of HIPAA Coverage. The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) applies to health care plans (including some employer-administered plans); health care providers, regardless of size, that transmit health care information electronically; and health care clearinghouses. The most important HIPAA privacy regulations are the Privacy Rule and the Security Rule.

2. Data Security Rules. Covered entities may use or disclose “individually identifiable health information” (in any medium) only in the specific situations permitted by the Privacy Rule or with the subject’s written authorization. The Security Rule supplements the Privacy Rule by requiring that the covered information be protected by administrative, physical and technical safeguards. Both the Privacy and Security Rules require “business associate” agreements with certain third party “business associates” that perform services on behalf of a covered entity, such as billing and transcription services.

3. 2009 Stimulus Bill. The Stimulus Bill included funds to be allocated to develop an infrastructure that would facilitate the nationwide sharing of electronic health records, and replace paper records by 2014. To address the heightened concerns about the security of electronic health data, Congress supplemented the protection of business associate agreements by also applying the administrative, physical and technical safeguard requirements of HIPAA directly to “business associates.” In addition, Congress enacted a nationwide data breach notification requirement that applies to covered entities and business associates that possess protected health information.

4. Other Statutes. Both the federal government and the states have additional laws that apply to specific conditions, such as HIV, STD, other communicable diseases and substance abuse. Some of these laws combine mandatory reporting to authorities with confidentiality protections. These laws continue to apply in the privacy area to the extent that they impose more stringent privacy protections than HIPAA.

F. Industry Standards

Some industries have voluntarily adopted or are developing best practices codes for privacy, with varying degrees of private enforcement. For example, a group called Business Forum for Consumer Privacy, which includes such technology giants as Microsoft, Google, and Hewlett Packard, has announced that it is shifting its focus from privacy legislation to creating an industry self-regulatory framework for privacy and data protection. At this point, the most influential existing industry standard may be the Payment Card Industry Data Security Standard, or PCI DSS, which was promulgated by a consortium that includes American Express, Discover, MasterCard, VISA, and JCB. The current version, PCI DSS 1.2, imposes twelve highly detailed requirements for securing cardholder data that is stored, processed, and/or transmitted by merchants and other organizations.

Each of the card brands has modified its own security policies to conform to PCI DSS. The PCI DSS consortium is trying to assure consistency in enforcement by subjecting non-compliant member banks to fines. Merchants and service providers found to be in violation are

ROBINSON BRADSHAW & HINSON

subject to restrictions up to and including denial of access. Some observers expect member banks to use contractual provisions to require merchants to reimburse them for fines they incur as a result of merchant non-compliance and, possibly, for the costs of holding card holders harmless from fraudulent use of their cards.

G. Foreign Law

Many foreign countries have laws that deal specifically with data security. These laws are often materially different from U.S. laws and, in some cases, are much more restrictive than those in this country. The potential application of these laws to U.S. companies is not always clear. However, you generally should assume that a foreign country's laws may apply to information collected from residents of that country if the U.S. company has a physical presence in that country, otherwise conducts a significant level of business in that country, or collects a significant amount of PII from users in that country.

The single most important foreign privacy law, the European Union Privacy Directive, broadly covers the activities of any company that controls the electronic collection, storage, transmittal or other use of "identifiable personal data" in the EU. In the data security area, the Directive requires the controller to maintain the accuracy and security of identifiable personal data and permits data subjects to access their data and challenge any noncompliance with the Directive. The EU concept of identifiable personal data is broader than the U.S. concept of PII. In the U.S., the focus is on information that would permit a third party to match identifying data with an individual in order to commit identity theft. In the EU, the concept is based on broader notions of privacy, and EU data security laws cover any objective or subjective data about an identifiable individual or her personal life, family life or behavior.

In addition, the Directive contains a general prohibition on transferring identifiable personal data from the EU to countries that lack EU-level protection. Since the U.S. falls into that category, such data can be transferred only if the U.S. recipient subscribes to the U.S. Department of Commerce "Safe Harbor" program, or enters into an EU-approved data transfer contract, or, in the case of intra-company transfers, adopts EU-approved Binding Corporate Rules. As a practical matter, this would impose on the U.S. company data security requirements comparable to the broader EU rules. Enforcement of the Directive is carried out by individual EU member countries. Sanctions can include fines and orders limiting the controller's activities.

Outside the European Union and the U.S., both the nature and scope of data security protection varies widely from country to country. A significant number of countries have adopted EU-type protection to minimize the problems of freely exchanging data with countries in the EU, but some of these countries enforce the rules in a more flexible and pragmatic way than the European Union. Japan follows a middle ground between the U.S. and EU approaches, with EU-type data security regulations that are enforced only by the ministries and require only that a business use best efforts to resolve complaints. Some countries, such as China, still do not have meaningful data security laws.

III. The Data Security Plan

Any data security program for PII should be comprehensive, effective and workable and should actually address the company's most significant security concerns. At the same time, it must comply with often-detailed requirements relating to PII in the applicable laws and regulations as well as in the company's contractual agreements. This section describes the elements of a basic data security plan for PII that will address the most significant general data security concerns and satisfy the laws and regulations that are generally applicable to commercial businesses operating in North Carolina. In some case, we identify additional steps that would improve any data security plan, but that are not legally required for most commercial businesses. You will need to supplement our suggestions if you are in a business that is subject to additional sector-specific regulation, such as health care and financial services, and you may need to supplement our suggestions if you collect and store data in other states.

Step One: Identify and document material internal and external security risks.

To develop an adequate data security plan, you must first understand exactly what data you need to secure and what risks you are trying to address. The first step is to survey what PII is collected, used and retained by your company. As a part of that process, you should ask why each type of PII is being retained. Companies frequently fall into the habit of collecting unnecessary personal information without fully analyzing the reason for its collection. You will simplify the job of data security if you can limit how much PII is collected and shorten the time that it is retained.

You also need to examine your internal data flow to determine which employees have access to PII. This helps to identify the locations at which such PII may be stored (including both the physical file cabinets that are used to store paper information and the computers and other devices that store electronic information).

Finally, you need to assess the level of risk from the disclosure of each type of PII. Some information would be merely embarrassing if disclosed (such as addresses and phone numbers) while other information disclosures could be costly (such as social security numbers, account numbers or passwords). Your security plan may apply differently to different types of information, depending on the level of sensitivity.

Once you understand your PII collection and storage system, you need to understand what administrative, technical and physical safeguards are already being used to protect that PII. This step will require the participation of your IT department and should result in a detailed analysis of the security of your information system, including network and software design, and information processing, storage and transmission. Most companies will use either an outside expert or free software to assist in this analysis. The analysis should include an assessment of the current level of use of common security procedures such as password-limited access, encryption (including the use of Transport Layer Security (TLS)), firewalls and the use of virus and spyware scans.

ROBINSON BRADSHAW & HINSON

As a companion to this technical assessment, you need to evaluate your systems and procedures. At a minimum, you should assess:

- the steps used in hiring, supervising and training employees to determine if the employees are actively involved in limiting the risk of internal and external security breaches;
- physical security, including both the limitations on non-employee access and the manner in which sensitive data is stored; and
- the procedures used in the disposal of information to determine whether paper and electronic data is being properly destroyed.

Finally, you should document your survey findings in a written report. The report should be as detailed as possible, since its purpose is to specifically identify those areas in which data security is adequate and those areas in which additional administrative, technical and physical safeguards are necessary.

Step Two: Design and implement reasonable safeguards to address the PII security risks.

The core of any data security plan is the development of a comprehensive set of steps to address your company's PII security risks. Some of these will be generic risks that are inherent in data collection and use, while others will be company-specific risks identified in your survey. The plan should be detailed in writing and have specifically assigned responsibilities to ensure implementation. A comprehensive plan would generally include at least the following elements:

- Limits on Data Collection and Retention. Collect only that PII required for a specifically identified business purpose and never collect PII that your Privacy Policy says you will not collect. Develop and implement a data retention policy that ensures that PII is kept no longer than necessary and destroyed when no longer needed. Avoid the unnecessary collection of particularly sensitive information like social security numbers. Destroy sensitive customer authentication data (such as the card validation number and the personal identification number) subsequent to authentication.
- Limits on Data Use. Comply with any statements in your posted Privacy Policy that limit the purposes for which PII may be used and disclosed. Understand and comply with the specific limits on the use of information that is considered to be particularly susceptible to misuse, such as social security numbers and medical information. Develop written procedures to ensure that all of these limits are followed.
- Limits on Access to Electronic Data. Limit access to particularly sensitive data to employees with a "need to know." Limit unauthorized electronic access to all PII by using unique user names and strong password protection (i.e., using passwords that avoid common words and that use a combination of letters and numbers,

ROBINSON BRADSHAW & HINSON

requiring that passwords be changed frequently and regularly and encrypting all passwords during transmission and storage). Use password-activated screen savers to limit access to unused computers. Require two-factor identification for remote system access. Never retain vendor-supplied defaults for passwords and system parameters.

- Protection of Electronic Data. Fully utilize the routine methods of protection: installing and maintaining a firewall; regularly running up-to-date virus scans, spyware scans and intrusion detection programs; and regularly installing software patches. Use industry best practices for information security for any custom-developed software and web applications.
- Use of Encryption for Transmitted Data. Protect all PII during transmission across open public lines. At a minimum, you should use Opportunistic TLS Encryption (which encrypts data to any recipient with a system designed to decrypt the data). For particularly sensitive data, you should consider using Enforced TLS Encryption (which bars the transmission of data to any recipient with a system that is not designed to decrypt the data) and using PGP or a similar encryption program to encrypt specific documents separately.
- Use of Encryption for Stored Data. Store all PII in encrypted form and permit access only through the use of authorized user passwords that decrypt the data. Store customer primary account numbers in an unreadable format, using some form of encryption or truncation, and ensure that they are partially masked when displayed. Use appropriate key management procedures to be sure encryption is fully documented and implemented and that the keys are adequately protected. If practical, extend this protection to portable storage devices such as flash drives.
- Organization of Electronic Data. To the extent practical, segregate PII into categories by sensitivity and store as much PII as possible at locations that cannot be remotely accessed over the Internet, wireless devices or electronic cash registers or by service providers. This serves two purposes. First, it allows you to selectively apply more extensive and burdensome procedures to the most sensitive information. Second, it allows you to more quickly determine if any PII has been accessed if there is a security breach, potentially saving you the time and expense of a required breach notice.
- Protection of Laptops and PDAs. Use robust protection for the data on laptops and PDAs, since these devices are particularly vulnerable and have been the source of some of the highest-profile security breaches. Encrypt all sensitive data on laptops and require that passwords be used to access the laptop and decrypt data. Require that passwords be used to access PDAs. Do not permit the use of portable devices to access networks without multiple levels of security, such as tokens. Regularly purge all unneeded PII from laptops, using wiping programs for check-out laptops or requiring users to regularly delete information from user laptops. Use “auto-destroy” programs that would limit third party access to the

ROBINSON BRADSHAW & HINSON

data if a laptop is stolen and remote wiping programs to destroy data on lost PDAs.

Step Three: Limit access to physical data and devices.

Limit access to computers and physical storage media, such as paper and storage tapes, that contain sensitive data. If practical, limit non-employee access to the building or portion of the building in which sensitive data is stored, control visitors through registration and time limited badges and monitor visitors with security cameras. Keep any physical media (such as tapes or flash drives) that contain sensitive data in a locked limited access cabinet, or in secure off-site storage, when not being used. Use physical security to protect storage media that contain PII during transit and storage.

PII is often compromised through employee carelessness. Develop and enforce policies that ensure that employees do not leave computers on and accessible while they are away from their desks or leave confidential paper documents unsecured overnight.

Step Four: Develop a policy for discarding PII.

The legal obligations relating to the destruction of PII will vary depending on your location and the type of data being destroyed. However, these rules are now pervasive enough, and the risk of data theft is significant enough, that a prudent data security program will deal with the destruction of all sensitive data. Such procedures are required for businesses in North Carolina.

Most of the required steps are straightforward. Shred sensitive paper records when they are discarded. Destroy, demagnetize or otherwise permanently erase discarded media containing sensitive electronic data (for example, in computers being replaced). Develop and enforce rules that ensure that comparable steps are taken with respect to sensitive data on home computers, personal laptops and PDAs.

Step Five: Monitor for problems.

There are two distinct aspects to data security monitoring: regular monitoring for electronic intruders and monitoring for signs of identity theft. There are several well known techniques for detecting electronic intrusion. You should use standard techniques for detecting intruders, including the monitoring of incoming data flow for signs of hacking and outgoing traffic for unusually large data flows. You should maintain a central log to monitor and respond to security breaches, including the use of secure automated audit controls for all system components, and you should regularly check websites such as www.cert.org (the Computer Emergency Response Team) for vulnerability updates.

The second aspect of data security monitoring focuses on the establishment of a program that proactively looks for signs of identity theft, both at the system level and at the customer level. The level of your identity theft risk will depend on the types of accounts that you maintain, the way in which those accounts are opened and can be accessed, and your history of

ROBINSON BRADSHAW & HINSON

identity theft. The FACTA Red Flag Rule has useful suggestions, whether or not you are technically covered.

The FACTA Red Flag Rule provides a common-sense list of Red Flags that can be a sign of identify theft:

- The receipt of alerts, notifications or other warnings from consumer reporting agencies or service providers, such as fraud detection services. This can include fraud or active duty alerts, a consumer-requested credit freeze, notices of address discrepancies or notice from a consumer reporting agency of an unusual change in activities.
- The presentation of suspicious documents, including documents that appear to be forged or altered, and documents that contain inconsistent photographs or identifying information.
- The presentation of suspicious PII, such as information that is inconsistent with public records or information that is consistent with known fraudulent activities or a suspicious address change.
- Unusual or suspicious account activity, such as the request for new cards shortly after an address change, the use of an account in a manner that is inconsistent with past patterns of use by the authorized user or consistent with known patterns of fraud, or repeatedly returned mail.
- Notices from customers, victims of identity theft or law enforcement authorities about possible identity theft.

Under the FTC program, you must have reasonable procedures in place to detect the existence of Red Flags. Your first step should be to ensure that you have a procedure that will verify the identity of customers when they set up an account by requiring adequate proof of identity. You then need to monitor transactions for Red Flags and verify address changes.

When you notice the existence of Red Flags, you must take reasonable steps to mitigate the risk. Your burden may vary widely, depending on the type of account, the nature of the information at risk and aggravating circumstances. For example, you would have a higher burden if a customer has notified you that she may have been the victim of phishing and has inadvertently provided identifying information to a fraudulent site. Depending on the circumstances of any particular Red Flag, it may be appropriate for you to more closely monitor the account in question, to require the customer to change passwords, to notify the customer or law enforcement authorities or to close the account in question and open a replacement account with a different account number.

Step Six: Make your employees an active and positive part of your data security plan.

Once you have completed the first five steps described above, you will have a basic security plan. But a security plan that looks good on paper is meaningless if it is not implemented. The remaining steps translate your written security plan into a meaningful part of your actual business.

As a first step, you should assign one or more employees the specific responsibility for implementing, enforcing and monitoring the data security plan. If more than one employee is responsible, you should either appoint a team leader or specifically allocate responsibilities. Employees must understand that they will be held accountable for carrying out these responsibilities in the same manner as other important job responsibilities.

In addition, you should minimize the likelihood that any employee will be the intentional cause of a security breach. You should screen all applicants who will have access to PII and require signed confidentiality agreements. You should then limit access to PII to those employees with a “need to know” and implement appropriate termination procedures, including the immediate termination of physical and electronic access to data. Most companies will already have these types of protections in place.

Each employee must be responsible for extending the security plan to PII retained on the employee’s home computer, and must share in the responsibility for protecting PII on laptops and PDAs. Depending on the circumstances, this may require password limited access controls, limitations on what centrally-stored PII is downloaded rather than only remotely viewed, the encryption of stored PII and the periodic destruction of unneeded copies of PII using “wiping programs.” You may also need to adopt policies extending some of the other security plan requirements to home computer users, such as the use of up-to-date virus scans, spyware scans and intrusion detection programs.

Finally, you need to ensure that all of your employees affirmatively buy into your data security plan. You should provide all new employees with training in security procedures, regularly update that training and provide periodic reminders of security issues. If you do not have trainers on staff, www.OnGuardOnline.gov can provide training resources. Properly trained and motivated employees can be your first line of defense against many types of data thefts, including third party attempts to illegally obtain PII through phishing.

Step Seven: Provide for oversight by the Board of Directors or senior management.

Senior level management should always be involved since a security plan will be taken more seriously by employees if they know compliance will be reviewed by senior management. You should have procedures that ensure that senior management and your Board of Directors is provided with regular detailed reports on the status of the data security plan. This is a legal requirement if FACTA applies.

Step Eight: Have procedures in place to address security breaches.

While data breach notification laws are not uniformly applicable in all states, they are common enough that a prudent data security program will deal with this issue. At a high level, they require individual notification to users when their personal information has been misappropriated. North Carolina has a data breach notification law.

Data security breaches present a unique problem. The nature and scope of a breach is often unclear at the time that it is discovered, making it difficult to know with certainty what PII may have been stolen. In addition, a breach can raise reputational as well as legal and financial issues. As a result, you will often have to decide how to respond to a security breach under pressure, with incomplete information and taking into account the views of multiple parties within your company. An adequate security breach notification plan takes this reality into account.

You need to take three steps to be prepared to deal with a security breach. First, you need to understand in advance the scope of your potential problem. This includes an understanding of the requirements of the particular laws that would apply to you. But it also includes an understanding of your data and information structure, so that you will know when a particular breach would be reasonably likely to result in the theft of unencrypted PII. You can make this task easier by segregating the most sensitive PPI, limiting remote access to such information and using computer logs that will help identify which computers may have been compromised.

Second, you need to have a plan in place for quickly detecting a security breach and limiting its scope. Your plan should include specific incident response procedures, business recovery and continuity procedures and data backup processes. You should test your plan at least annually.

Finally, you should develop in advance written procedures for dealing with confirmed security breaches. You should designate responsible employees on a 24/7 basis to respond to alerts and provide appropriate training. Your plan should include assigned responsibilities for sign-offs for notifications, contact numbers and a pre-approved text for notifications.

Step Nine: Extend your program to service providers.

When you permit third-party access to your PII, you will have at least some obligation to police the third party's protection of your PII. The precise extent of your legal obligation will depend on the location of your operations and the type of PII that will be disclosed. This would be an obvious issue if you outsource any of your IT operations. But it can also be an issue if you outsource other operations, including targeted marketing and order fulfillment.

It would not be practical for you to actually monitor a third party's data security program. But you can take two steps. First you should ask probing questions about data security compliance before you permit third-party access to your sensitive data, perhaps even reviewing the third party's data security plan. If you are covered by the FTC Red Flag Rule, you must ensure that any service provider that has access to covered accounts has reasonable policies and

ROBINSON BRADSHAW & HINSON

procedures to detect, prevent and mitigate the risk of identity theft. The PCI Data Security Standards impose a similar obligation.

Second, you can attempt to impose a contractual obligation on the third party to protect your PII, with meaningful liabilities for a failure to comply. The PCI Data Security Standard requires that service providers acknowledge their responsibility for cardholder data. Gramm-Leach-Bliley and HIPAA also require agreements with certain service providers (referred to as “Business Associates” under HIPAA) that process financial or health-related data. It will sometimes be difficult to negotiate complying contracts, particularly if you are outsourcing IT operations to a major company that is reluctant to accept meaningful liability.

Step Ten: Periodically test, evaluate and adjust the program.

Business and technology are dynamic, and new data security vulnerabilities are being discovered continually by hackers and researchers, so a data security plan that may be adequate today could be completely outdated next year.

You should regularly and periodically review and adjust your data security plan to be sure it reflects your current business and continues to adequately protect your PII. The PCI Data Security Standard requires quarterly internal and external vulnerability scans and a more comprehensive review (including penetration testing) after each significant system upgrade, and no less often than annually. You should document your compliance by developing a specific review schedule, assigning the review responsibility and retaining written reports on each review.

For more information on this topic, please contact Robert M. Bryan (bbryan@rbh.com; 704.377.8310) or John M. Conley (jmconley@email.unc.edu; 919.962.8502).

Robinson, Bradshaw & Hinson, P.A. offers this paper as general information. It is not intended as specific legal advice for particular situations. If you would like additional information on this topic, please contact the author(s) listed above.

© Robinson, Bradshaw & Hinson, P.A.