

Five Key Steps to Developing an Information Security Program

by Gabriel M. Helmer



Contents

Introduction	1
1. Take the Time to Comprehensively Evaluate the Company's Legal Obligations	3
2. Review What You Need to Accomplish	6
3. Choose an Information Security Coordinator/Team	7
4. Start With What You Have	8
5. Evaluate Potential Threats and Adopt Reasonable Security Measures to Combat Them	10
Appendix A - Massachusetts Identity Theft Laws & Regulations	14
Appendix B - Federal Red Flags Rules	18
FTC Guidelines to Compliance with Red Flags Rules	21
Supplement A to Appendix A	26
<i>About Foley Hoag LLP</i>	30
<i>About the Security and Privacy Practice</i>	30
<i>Gabriel M. Helmer</i>	31

“Responding to the rising tide of damaging security incidents, the federal government and the majority of states have enacted laws and regulations requiring individuals and companies to adopt comprehensive information security programs to protect sensitive information.”

Five Key Steps to Developing an Information Security Program

by Gabriel M. Helmer

Information security — the discipline of protecting information found in paper documents, electronic files and emails — has become increasingly important in business. As reports of identity theft, data breaches and cybercrime have become more common, government has begun to call on businesses, both large and small, to take on new responsibilities for protecting sensitive information.

Responding to the rising tide of damaging security incidents, the federal government and the majority of states have enacted laws and regulations requiring individuals and companies to adopt comprehensive information security programs to protect sensitive information. For instance, the Federal Trade Commission (FTC) along with federal banking regulatory authorities have adopted the Red Flags Rules. This broad set of regulations require businesses to assess their information security practices and implement an identity theft prevention program to mitigate the risk of identity theft. Financial institutions are also subject to the FTC’s Safeguards Rule, which requires the adoption of a “comprehensive information security program” to protect any nonpublic customer information.

At the state level, the majority of states have put in place regulations governing how businesses collect, handle and dispose of personal information. Aggressive new Massachusetts regulations, like those in many other states, require any individual or business that accesses personal information about a Massachusetts resident to develop a “comprehensive, written information security program.” Massachusetts has also adopted laws requiring public notification of security incidents and secure disposal of customer information.

The new federal and state identity theft regulations join dozens of other legal requirements that have emerged over time, including rules governing medical information, insider information, customer data, trade secrets, intellectual property and other kinds of sensitive information. In the past, businesses typically responded to new legislation by adopting compliance policies limited to specific categories of protected information. But new laws now demand that businesses adopt a dynamic, comprehensive approach to information security. This is an opportunity for

businesses to make sure their information assets are well protected, but it is also necessary to avoid potentially serious legal liabilities in the future.

Many businesses have trouble knowing where to begin and what to do to comply with the new federal and state regulations. What follows is a guide that explains how to begin the process of developing a compliant program in five steps.¹

First, the business should comprehensively assess what laws, regulations and rules apply. Attention is often focused on a particular regulation while other legal requirements go unnoticed. Make sure your business has identified each and every law, regulation and rule that applies.

Second, make a list of all the specific elements that will be required to fulfill the applicable legal obligations. While some of the new information security laws will require “reasonable and appropriate” protections, other have specific requirements that must be met, such as encrypting laptop computers containing personal information. Make sure you know what the objectives are before you set out to meet them.

Third, select the right person or a team to develop the information security program. The new laws require that a coordinator or team assume responsibility to developing and maintaining information security and this will require input and cooperation from a variety of different departments. Who will lead this effort is a key decision for most businesses.

Fourth, assess what the business is already doing to maintain information security. Most businesses are already taking steps to protect sensitive information and do not need to start from scratch or make drastic changes.

Finally, evaluate the potential threats and adopt the security measures necessary to combat them. Fixing any noticeable holes in existing security measures is the key to complying with information security laws.

Taking the time to follow these steps will ensure that the business remains compliant with the range of new information security laws, in particular, federal Red Flags Rules and the Massachusetts identity theft regulations. We will use these regulations as specific examples throughout this guide.

¹ Included with this eBook are Foley Hoag’s guides to the Massachusetts identity theft laws and regulations (Appendix A) and the federal Red Flags Rules (Appendix B).

1

Take the Time to Comprehensively Evaluate the Company’s Legal Obligations

The first step to establishing an information security program (and complying with recent information security rules) is to take the time to fully assess the laws that may apply to the company. This step is often overlooked. Acting on faulty assumptions about what rules apply or putting off the preliminary evaluation for fear of uncovering onerous legal obligations, are shortsighted approaches that can expand a company’s liabilities. The better course of action is to have company personnel sit down with experienced counsel and comprehensively evaluate what laws, regulations and rules apply to information collected by the company.

A reasonable evaluation of a company’s legal obligations and liabilities can be a challenge because there are hundreds of federal, state and international laws that could govern information security and experience with this area of law is still relatively scarce. Nevertheless, a comprehensive evaluation is particularly important. Not only do the new regulations require that the comprehensive information security program be consistent with all applicable legal standards, but addressing all of the company’s obligations at the same time will save the company time and money in the long term. Condensed below is a list of some key areas of law that should be considered.

- Federal Red Flags Rules, codified in 16 C.F.R. § 681, expressly apply to “financial institutions” and “creditors;” however, the FTC has stated that the term “creditor” encompasses any company that sells goods or services first and then bills its customers later. The FTC’s broad interpretation of these rules has come as a surprise to many industries. Affected businesses are required to routinely assess whether they maintain accounts that present a risk of identity theft and, if they do, develop an “identity theft prevention program” that puts in place reasonable and appropriate protections. More information on the Red Flags Rules may be found in Appendix B
- It is crucial that every business evaluate the effect of state identity theft laws and regulations. For example, any business that owns, licenses, maintains or stores “personal information,” as that term is defined under Massachusetts law, is subject to Massachusetts identity theft regulations, 201 C.M.R. §§ 17.00-

17.05. “Personal information” is defined by the statute as the name of a Massachusetts resident in combination with his or her (1) Social Security number, (2) driver’s license or state identification number, or (3) credit card, bank account or other financial account number. Under Massachusetts law, “personal information” is broad enough to include customer records, employee files, some medical records, copies of bank checks, tax filings, credit card statements and a wide range of other business records. Remember to consider this question broadly — the Massachusetts regulations apply no matter where the business is located, no matter how large or small the business, and no matter how much personal information a business accesses or how often the company accesses personal information. For more information on Massachusetts laws and regulations, review our guide at Appendix A.

- All businesses subject to the Massachusetts identity theft regulations are also subject to the Massachusetts data breach notification law, Mass. Gen. Laws ch. 93H, and the Massachusetts information disposal law, Mass. Gen. Laws ch. 93I. These laws require affected businesses to provide formal notification to customers and the Attorney General when there is a security breach and destroy, rather than merely throw away, documents and electronic records containing “personal information.” A compliant information security program should incorporate procedures for complying with these requirements.
- Any business with customers, staff, contracts or business operations in more than one state must consider the laws of multiple states. We are commonly asked whether compliance with the aggressive new Massachusetts regulations will ensure that a business is complying with similar laws and regulations in other states. For many states, the answer is no. For example, the California identity theft statute, like Massachusetts, applies to any business with access to information relating to California residents, but defines “personal information” to include medical information. Nevada’s laws, on the other hand, require specific language to be adopted in third party contracts with data collectors. When examining what the company must do to comply with the new information

“We are commonly asked whether compliance with the aggressive new Massachusetts regulations will ensure that a business is complying with similar laws and regulations in other states. For many states, the answer is no.”

security rules, remember to consider whether the rules of other states may require expanding protections to cover other categories of sensitive information or additional legal requirements.

- A comprehensive assessment should also examine a company’s potential liability for violations of federal and state laws governing “unfair or deceptive acts and practices.” For over 10 years, the FTC has sanctioned numerous companies for lapses in information security under the FTC Act which prohibits unfair or deceptive acts and practices. Because the scope of “unfair or deceptive acts and practices” is not limited to any particular categories of sensitive information (e.g., “personal information”) or any particular industry (e.g., “financial institutions” and “creditors”), all businesses should be evaluating their information security practices more broadly than they might realize. This is of particular concern because state consumer protection statutes could also be triggered. In Massachusetts, the Massachusetts Consumer Protection Act (Mass. Gen. Laws ch. 93A), like similar state statutes, carries the possibility of stiff fines, treble damages and attorneys fees.
- Businesses have also been subject to a range of industry-specific laws, regulations and rules, including the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX) and Gramm-Leach-Bliley Act (GLBA), the FTC’s Safeguards Rule (16 C.F.R. Part 314), the FTC’s Disposal Rule (16 C.F.R. Part 313), and the Federal Communications Commission (FCC) rules governing customer proprietary network information (CPNI), just to name a few. It is important to take all industry-specific requirements into account when developing a compliant information security program.
- Review the company’s existing obligations to protect and secure information under non-disclosure and confidentiality agreements, customer policies, settlement agreements or court orders. This may identify other categories of information that the company is obligated to protect or other security measures that the company has already agreed to implement.

Over the years, many businesses have adopted specific policies to comply with many of these information security rules, but this process occurred slowly to address new laws when they emerged or in response to an incident. The new regulations call on businesses to change their way of thinking and develop comprehensive, rather than piecemeal, approaches to information security. As a result, taking time to consider all of the potential legal obligations at the beginning of the compliance process can be critical.

2 Review What You Need to Accomplish

Once a business determines what laws, regulations and rules apply, it should develop a list of the general and specific goals it seeks to accomplish. All too often this task is complicated by the number of legal requirements and other tangential considerations.

Most federal and state information security regulations will require that the business develop a written program that lays out the security measures it has adopted. Taking the Massachusetts identity theft regulations as an example, affected business must develop and implement a “comprehensive, written information security program” by January 1, 2010. If a company is subject to the federal Red Flags Rules, the Safeguards Rule or other federal or state requirements, it may need to accelerate development of its information security program to meet earlier federal deadlines. A compliant information security program will be a written document built on the company’s existing policies and procedures, but developing one will require the business to perform an assessment of the way it collects, manages and disposes of information, and evaluate existing security measures against the foreseeable threats.

The primary objective for any information security program, no matter whether it is governed by the Massachusetts regulations or any other federal or state rules, is to impose reasonable and appropriate information security measures. The program should be reasonably consistent with industry standards and appropriate to the size of the business, the resources available, the amount of sensitive information at issue and the need to protect the information. The specific requirements of the Massachusetts regulations include a number of specific elements, including an annual assessment of potential risks, periodic employee training and the adoption of physical, administrative and electronic security measures. These requirements are laid out in detail in the guide to the Massachusetts regulations included in Appendix A.

Once you have developed a list of the general and specific legal requirements, the business will be able to confidently begin development of a compliant information security program. Armed with a list of its objectives, the company will be in a good position to identify the departments and individuals who should be involved in the development process.

3 Choose an Information Security Coordinator / Team

One of the key preliminary steps in the process of developing a compliant information security program is to designate the right person or people to put the program together. Both federal Red Flags Rules and the Massachusetts identity theft regulations require that the company’s information security program expressly identify a coordinator or team. Most importantly, it will streamline the compliance process to have the right personnel involved at the outset.

Keep in mind that developing an information security program is going to require the coordinator to come up to speed on the way information is collected, maintained, handled and disposed of in every department or area in the company. Having taken the time to assess what laws apply and what the company’s general legal obligations will be, a company should be in a good position to identify all the relevant areas of operation and a coordinator or team with access to those areas. Focus on identifying the individual(s) who are able to take over a host of responsibilities, including drafting policies and procedures, managing the required training program, reviewing company contractors to make sure they are taking the necessary precautions, assess potential security threats, as well as working with security officers, information technology managers, public relations, and legal counsel to identify security breaches and respond to any incidents at the company.

For small or emerging companies, the information security coordinator’s role is often merged with the CIO or IT director position. Before asking the CIO to assume the position, the company and its CIO should recognize that this usually represents an expansion of the typical responsibilities and may require additional preparation, training and input from other areas. A larger company with many different departments should make sure that the coordinator or team is in a position to navigate between all departments that will be directly involved in information security, including surveillance and physical security, IT, human resources, physical plant, general counsel’s office, and public relations.

Keep in mind when selecting the information security coordinator that the role may sometime be in tension with the goals of the CIO, who is often asked to make information available to support the company’s business projects. The selection of the information security coordinator or committee should ensure that any compromises between security and business operations are negotiated at an appropriate level in the organization.

4

Start With What You Have

After a company has selected a coordinator or team to develop an information security program, it is time to investigate the company's current practices and policies. The coordinator should identify how the company collects, handles, accesses, stores and dispose of sensitive and valuable information. This typically requires that the coordinator meet with staff responsible for collecting, handling, filing and throwing away a variety of documents and data.

The company should make sure it generally knows all the physical locations where the information resides, whether information is collected by email, fax, mail, phone, or in person, whether the information is stored in one file cabinet, ten offices or one hundred computers, and whether the information is locked in a file room, saved to a salesperson's laptop, or transferred electronically between offices. Consider both company policy and general practice. Do not forget to examine how employees access information remotely and how information is thrown away. We often forget about trash after it has been left at the curb, but identity thieves and cybercriminals commonly collect information from garbage containers and use information they find to steal money and access confidential information. Taking notice of this trend, federal regulators have penalized businesses when sensitive personal information has been found in their trash. Make sure to identify any prior security incidents or data breaches. Prior incidents often provide insights that will help the company identify potential threats and solutions.

In going through this process, it is extremely important to collect and review any prior policies and procedures that could impact information security, including any security policies, appropriate computer usage and password policies, and termination policies. Prior policies will give a business a head start in drafting its information security program, but they also help identify any threats and security measures the company has previously identified. It is important to review any public notices, policies or statements that make representations about how the company secures or manages information. In discussions with staff, be sure to identify where current business practices, policies and public statements have diverged over time. This often sheds light on potential threats, existing industry standards and will help a company work new security measures into the company's existing operations and culture.

In particular, I advise clients to assess their information practices broadly and to make sure to evaluate how the company protects its own proprietary information, intellectual property and trade secrets and any other kinds of valuable information that may not fit squarely into the statutory definition of "personal information." Not only will this help frame the different ways that the company already protects valuable information, but keeping the company's intellectual property in view is important when deciding what levels of security are appropriate. When a business is improving security around specific categories information, it may also be necessary to increase the protection in place for the company's intellectual property. A company that completes an all-inclusive review of its existing information security practices and policies will be in the best possible position to address the requirements of new laws and regulations.

"...identity thieves and cybercriminals commonly collect information from garbage containers and use information they find to steal money and access confidential information."



Evaluate Potential Threats and Adopt Reasonable Security Measures to Combat Them

The core challenge for a company developing an information security program is identifying the reasonably foreseeable threats and adopting appropriate security measures to mitigate those risks. For many companies developing information security programs, a comprehensive risk assessment may be a new undertaking or may already be part of an existing compliance program. Mindful that it is not possible to protect against all potential threats, companies will need to identify threats that are reasonably foreseeable.

In practice, a good starting point for many companies has been to compare their current practices and policies with the provisions of applicable regulations and identifying where the two do not meet. The Massachusetts regulations, like most other state regulations, do not expressly list all potential security threats that companies should consider. However, in requiring companies to adopt specific security measures, the new identity theft regulations implicitly recognize that there are a number of inherent security threats that companies must address.

“... in requiring companies to adopt specific security measures, the new identity theft regulations implicitly recognize that there are a number of inherent security threats that companies must address.”

Threat:	Required Security Measure(s):
Failure by employees to use reasonable security practices	Employee training program Disciplinary measures for violations
Unauthorized access to personal information stored at company offices	Restricting physical access by using locked facilities Restricting electronic access to authorized users Secure user name and password policies Routine monitoring of electronic access Administrative security measures
Inadvertent loss of personal information stored on lost or stolen company laptops or mobile devices	Policies for transfer of information outside of the company Encryption of all data on laptops or mobile devices Policies limiting retention of personal information
Theft of personal information by departing employees	Policies on transferring information outside of the company Policies for terminating access to departing employees
Unauthorized access to information sent to third party service providers	Verification of security practices by all third-party service providers
Security breaches caused by computer viruses, worms and Trojan horse attacks	Up to date malware software Up to date system software Training on computer security
Intrusions by hackers and other cybercriminals	Up to date network firewall system Routine monitoring of network traffic
Unauthorized access to personal information found in company trash	Procedure for destroying personal information before disposal

Companies that must comply with federal Red Flags Rules are required to review the FTC's detailed list of identity theft warning signs and determine whether any are relevant to their businesses.² Even if a company is not subject to the federal regulations, the FTC's list may be useful to review when identifying potential threats.

Adding to the difficulty of this task is the fact that new risks, exploits and security breaches are discovered every day as are new, effective solutions to those problems. It is important for information security coordinators to keep up to date on recent news, security incidents and industry standards. This can be a challenge and some businesses may need to involve counsel and security consultants to advise them directly during the risk assessment phase. The following are a handful of useful resources that can help companies identify the potential risks and find appropriate administrative, physical and electronic security measures to avoid problems:

- Staying up to date on what threats and security measures regulators have already identified can be an important way to stay ahead of any government enforcement. The FTC has taken the lead in enforcing security and privacy rules and the [FTC website](#) contains listings of prior cases that identify alleged security flaws discovered at other companies. The FTC has sanctioned companies for failing to test the security of new websites and software used to collect or manage sensitive personal information, failing to encrypt sensitive information, storing sensitive information in a number of unnecessary locations, allowing users to set easy to guess passwords, and failing to properly secure wireless internet access, among other things. Foley Hoag's Security & Privacy Practice tracks potentially relevant decisions from federal and state regulatory agencies and posts helpful reports on [SecurityPrivacyandtheLaw.com](#).
- Reviewing the security breaches experienced at similarly situated companies and organizations is one of the best ways to identify reasonably foreseeable threats and appropriate solutions. Newspapers, magazines and industry journals typically keep track of high profile incidents, but the [Identity Theft Resource Center®](#) (ITRC) maintains a website tracking data breaches nationwide. The ITRC produces a [list of high profile breaches](#) and searchable [annual reports](#) that identify how the security breaches occurred.

² The FTC's list of warning signs are included in Foley Hoag's guide to the Red Flags Rules at Appendix B.

- For detailed technical information on threats to computer systems and networks, the [SANS Institute](#) actively surveys vulnerabilities and security flaws. Federal regulators have referenced the SANS Institute repeatedly in setting information security standards.

Most importantly, when adopting security measures, it is important to maintain the right balance between the existing operations of the company and the company's legal obligations. Often there is a push to adopt strict security measures that impact a company's workflow where there is no imminent threat and companies also commonly avoid adopting low-cost security measures even where there is a pressing need. Financial limitations and other practical consideration also impact what security measures a company can put in place. Businesses should remember that federal and state regulations allow businesses a degree of flexibility to strike the right balance. Involving counsel in these delicate strategic decisions is a good way to make sure that the company remains compliant without impeding business operations.

Following these steps will make sure that a company is developing a comprehensive and compliant information security program.

“...when adopting security measures, it is important to maintain the right balance between the existing operations of the company and the company's legal obligations.”

Appendix A

Massachusetts Identity Theft Laws & Regulations

Introduction. In 2007, Massachusetts enacted broad legislation to safeguard the “personal information” of Massachusetts residents. These new laws and regulations include Mass. Gen. Laws ch. 93H and 93I and the aggressive new identity theft regulations adopted by the Massachusetts Office of Consumer Affairs and Business Regulation, 201 C.M.R. § 17.00-17.05.

Who is covered? Any individual, business or agency that stores, maintains, owns or licenses personal information about a resident of Massachusetts. The law defines “personal information” as the full name of a Massachusetts resident in combination with (1) a Social Security number, (2) driver’s license number or state identification card number, or (3) financial account number, credit card or debit card number. The Massachusetts regulations apply no matter where the business is located and no matter how large or small its operations. Importantly, the Massachusetts rules apply no matter how much personal information a business maintains or how often it uses the information.

What do I have to do? All affected entities have three primary obligations:

1. Develop, implement, maintain and monitor a “comprehensive, written information security program” on or before January 1, 2010. (17 C.M.R. §§ 17.03 + 17.05))
2. Provide a written notification when the business knows or has reason to know that there has been a security breach. (M.G.L. ch. 93H, § 3(a))
3. Dispose of personal information so that personal information cannot be read or reconstructed after documents have been thrown away. (M.G.L. ch. 93I, § 2)

What are the requirements of a “comprehensive, written information security program”? All affected entities must develop a written information security program designed to protect personal information in a manner that is reasonably consistent with industry standards and other applicable laws and regulations. The general principles for an information security program are: (a) collect only the information that is necessary, (b) retain that information only as long as you need it, and (c) provide

access to information to only those people that need it for a legitimate business purpose. In addition, the Massachusetts regulations require that affected businesses adopt a series of specific administrative, physical and electronic security measures. Below is a summary of the specific requirements.

Administrative Security Measures

1. Designation of an information security coordinator / committee
2. Regular employee training on security and information management
3. Routine review of company compliance and oversight
4. Disciplinary measures for violations of the program
5. Procedure for ensuring that terminated employees no longer have access to personal information
6. Procedures for transferring personal information outside of the company
7. Monitoring and certification of third-party service providers to ensure that they are providing appropriate levels of security
8. Procedures for limiting collection to the personal information necessary to accomplish a legitimate business purpose
9. Procedures for limiting retention of personal information to the time necessary to accomplish a legitimate business purpose
10. Procedures for limiting access to personal information to the individuals that require access to accomplish a legitimate business purpose
11. Monitoring the program to ensure effectiveness
12. Reviewing the program, at least annually, to determine whether it requires revision
13. Procedure for documenting and responding to security breaches

Physical Security Measures

14. Restrictions on physical access to personal information, including keeping personal information in locked facilities, storage areas or containers.

Electronic Security Measures

15. Policies that require the use of unique user names to access personal information
16. Policies requiring passwords of appropriate complexity and strength
17. Use of encryption to protect personal information, including the encryption of all laptops and mobile devices that contain personal information
18. Routine monitoring of computer systems for unauthorized access
19. Reasonably up to date network firewall protection
20. Reasonably up to date virus and malware protection
21. Reasonably up to date system software
22. Set up to receive regular software security updates

Under what circumstances do I have to provide notice of a security breach?

Anyone subject to the Massachusetts laws and regulations must make a formal notification when they become aware (or reasonably should have been aware) of a “security breach.” Under Massachusetts law, a “security breach” is the unauthorized acquisition or use of data “that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.” Common examples include a theft of company laptops containing personal information and the discovery that current or former employees have used company records to engage in identity theft. The statute does not require notice when there has been good faith but unauthorized access to personal information, unless this breach resulted in unauthorized use of the information or further unauthorized disclosure.

What do I have to do to satisfy the notification requirement? If you are required to make a notification, you must prepare written letters to all affected Massachusetts residents, the Massachusetts Attorney General and the director of the Office of Consumer Affairs and Business Regulation. The notice to residents should (1) let the resident know that he or she has the right to obtain a police report; and (2) provide information on how the resident requests a credit freeze. Also, the Massachusetts law prohibits you from providing certain information in your letter, including specific details of the security breach or the number of residents affected. This notification must be made “as soon as practicable and without unreasonable delay,” unless a law enforcement agency investigating the breach determines that notification must be postponed to further an ongoing criminal investigation.

How do I dispose of personal information in a way that complies with

Massachusetts law? All affected individuals, businesses and agencies must meet minimum standards for disposal of personal information. Paper documents must be redacted, buried, pulverized or shredded so that the personal information cannot practicably be read or reconstructed. Electronic files, disks, hard drives or other storage media must be securely destroyed or erased so that the personal information practicably cannot be recovered after disposal.

What is the penalty for not meeting these obligations? Failure to adopt or follow a compliant information security program or make an adequate notification may lead to civil penalties of up to \$5,000 per violation, the award of attorneys fees and the costs of investigation. Improper disposal of personal information is subject to a fine of \$100 per resident affected, up to a maximum of \$50,000 per incident. The Massachusetts Attorney General is empowered to enforce violations under the Massachusetts Consumer Protection Act, ch. 93A. Affected residents may also be able to bring private actions against violators for “unfair or deceptive trade practices” that could lead to compensatory damages awards, as well as treble damages and attorneys fees.

Appendix B

Federal Red Flags Rules

Introduction. The “Red Flag Rules” are federal identity theft regulations promulgated in 2008 by the Federal Trade Commission (FTC), the Treasury Department and a number of other federal agencies. These Rules require certain kinds of businesses to develop written programs to detect and prevent identity theft on or before August 1, 2009. Below, is a general overview of these regulations.

Who is covered? The Red Flags Rules apply to “financial institutions” and “creditors.” While this includes banks, credit card companies and institutional lenders, federal regulators have announced that the term “creditors” applies to any business that sells goods or services now and bills their customers later. Under this construction, the Red Flags Rules apply to a wide range of merchants, doctors, lawyers, consultants and other businesses.

What do I have to do? Affected entities have two primary obligations:

1. Regularly assess whether the business maintains “covered accounts.” (16 C.F.R. § 681.2(c))
2. With respect to any “covered accounts,” the business must develop and implement an “Identity Theft Prevention Program.” (16 C.F.R. § 681.2(d))

What is a “covered account?” A covered account may fall into one of two categories. The first category is personal financial accounts designed to permit multiple payments or transactions, including credit card accounts, mortgage loans, automobile loans, cell phone or utility accounts, as well traditional checking or savings accounts. The second category of covered accounts includes any account that poses a reasonably foreseeable risk of identity theft. This broad category could include virtually any kind of account.

How do I assess whether I maintain an account that poses a reasonably foreseeable risk of identity theft? Start by reviewing all of your prior incidents involving fraud or identity theft. If an account has been involved in an actual incident, it may present a sufficient risk of identity theft to make it a “covered account.” It is best to keep in mind that an “account” may cover a variety of business arrangements. It may include an identification card or a user number that could be used to obtain goods or services or to pose as the customer. It may also include an online account

that stores information such as bank account numbers, credit card numbers, passwords or other information that could be misused. The FTC suggests that businesses consider how an account is opened and accessed when making its assessment. If an account can be opened remotely, either online or by the telephone, there may be an increased risk of identity theft.

What if I do not have any “covered accounts?” Even if you do not have any covered accounts, all financial institutions and creditors are required to perform a periodic assessment to determine whether any of the accounts they offer or maintain are covered accounts. It is a good idea to perform this assessment at least once per year.

What do I have to do if my business offers or maintains “covered accounts?” Any financial institution or creditor that maintains covered accounts must (1) review the FTC’s Guidelines to Red Flags Compliance, which we include below and (2) develop and implement a written Identity Theft Prevention Program consistent with those Guidelines. The primary purpose of the Program is to put in place procedures that will enable the business to recognize the red flags of identity theft and take steps to protect consumers. A key step in developing an Identity Theft Prevention Program is to select the right team of people to take responsibility for developing the Program. Keep in mind that developing the program likely requires input from a variety of business areas including, physical plant, physical security, information technology, accounting, as well as customer and public relations.

What are the requirements of an “Identity Theft Prevention Program?” A compliant Identity Theft Prevention Program must contain: (1) the “Red Flags” that it has identified as relevant to its business; (2) procedures to detect the red flags you have identified; (3) procedures for responding to any red flags that have been detected; and (4) a number of required administrative provisions.

How do I identify “Red Flags?” A “Red Flag” is a pattern, practice or specific activity that indicates the possible existence of identity theft. The FTC’s Guidelines (reproduced below) at list a number of potential red flags including, alerts from credit monitoring agencies or service providers, receipt of suspicious documents or personal information, or suspicious activity relating to covered accounts. Businesses must consider the FTC’s list of red flags and determine which are applicable. A report of identity theft from a customer, victim or law enforcement agency should always be considered a red flag. If your business or similar businesses have had prior run-ins with identity theft, a review of these incidents can provide you with a good idea of what red flags may apply.

What procedures are necessary to detect the “Red Flags” I have identified?

The procedures needed to detect and identify red flags depend on the nature of the business and the red flags. The FTC Guidelines focus on verifying customers’ identities at the time they open accounts and on authenticating customers’ identities when they access their accounts. Most businesses already have such procedures in place, but should consider whether improvement is warranted given the increasing sophistication of identity thieves.

What procedures should I adopt to prevent identity theft once a Red Flag has been detected?

The FTC’s Guidelines suggest a number of ways to prevent identity theft once a business has detected a red flag. These include contacting the customer and monitoring an account for abuse when a red flag has been detected, changing passwords and security codes, closing the account, and reopening the account with a new account number and password. It may be appropriate to take no action or turn the matter directly over to law enforcement. The Red Flags Rules recognize that an Identity Theft Prevention Program may need to be flexible in order for the company’s response to be appropriate under the circumstances. Red flags should be reported to internal managers and the security coordinator who may select an appropriate response under the Program, perform an investigation and take any other actions to alleviate the risk of harm to consumers and the business. The Program should ensure that the response is timely and appropriate under the circumstances.

What are the administrative requirements of a compliant Identity Theft Prevention Program?

The Red Flags Rules also require a business to adopt a number of administrative procedures, including:

1. A procedure to obtain the approval of the Program from its board of directors.
2. Procedures for reviewing and revising the Program periodically to ensure that the Program reflects current practices, changes in the industry or increased risks to consumers. The board of directors or its delegate(s) also should be involved in this process.
3. Policies requiring employee training, as necessary.
4. Policies requiring appropriate supervision of service providers that may access or provide services related to covered accounts.

What do I need to do if I use a third-party service provider to manage some aspects of covered accounts?

The Red Flags Rules require a business to provide “appropriate and effective oversight” of any third-party service providers. Any

business that uses a service provider must take steps to ensure that the service providers have an adequate Identity Theft Prevention Program. Ideally, affected businesses will negotiate a written contract with the service provider requiring compliance with Red Flags Rules. At minimum, service providers should be put on notice that they are covered by federal Red Flags Rules and should provide periodic written assurances that their practices are consistent with federal and state laws and regulations.

What is the penalty for not complying the Red Flags Rules by August 1,

2009? The FTC may seek civil penalties and injunctive relief for violations of the Red Flags Rules. The trend in enforcement of similar rules over the past years has seen the FTC seek substantial civil fines when the harm has affected a large number of customers, as well as court orders requiring the adoption of a compliant Program and independent security audits that are reported to federal regulators for 20 years.

FTC Guidelines on Compliance with Red Flags Rules

Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 681.2 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 681.2(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 681.2 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

- (a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:
- (1) The types of covered accounts it offers or maintains;
 - (2) The methods it provides to open its covered accounts;
 - (3) The methods it provides to access its covered accounts; and
 - (4) Its previous experiences with identity theft.
- (b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:
- (1) Incidents of identity theft that the financial institution or creditor has experienced;
 - (2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and
 - (3) Applicable supervisory guidance.
- (c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.
- (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
 - (2) The presentation of suspicious documents;
 - (3) The presentation of suspicious personal identifying information, such as a suspicious address change;
 - (4) The unusual use of, or other suspicious activity related to, a covered account; and
 - (5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

- (a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and
- (b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

- (a) Monitoring a covered account for evidence of identity theft;
- (b) Contacting the customer;
- (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
- (d) Reopening a covered account with a new account number;
- (e) Not opening a new covered account;
- (f) Closing an existing covered account;

- (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- (h) Notifying law enforcement; or
 - (i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

- (a) The experiences of the financial institution or creditor with identity theft;
- (b) Changes in methods of identity theft;
- (c) Changes in methods to detect, prevent, and mitigate identity theft;
- (d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and
- (e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

- (a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:
 - (1) Assigning specific responsibility for the Program's implementation;
 - (2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and
 - (3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) Reports.

- (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 681.2 of this part.
- (2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.
- (c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

- (a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;
- (b) Implementing any requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

- (c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and
- (d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix A

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix A of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries;
 - b. An unusual number of recently established credit relationships;
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
 - a. The address does not match any address in the consumer report; or
 - b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
 - a. The address on an application is the same as the address provided on a fraudulent application; or
 - b. The phone number on an application is the same as the number provided on a fraudulent application.
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
 - a. The address on an application is fictitious, a mail drop, or a prison; or
 - b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
 - a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
 - b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - a. Nonpayment when there is no history of late or missed payments;
 - b. A material increase in the use of available credit;

- c. A material change in purchasing or spending patterns;
- d. A material change in electronic fund transfer patterns in connection with a deposit account; or
- e. A material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

About Foley Hoag LLP

Foley Hoag LLP is a leading national law firm in the areas of dispute resolution, intellectual property, and corporate transactions for emerging, middle-market, and large-cap companies. With a deep understanding of clients' strategic priorities, operational imperatives, and marketplace realities, the firm helps companies in the biopharma, high technology, energy technology, financial services and manufacturing sectors gain competitive advantage. The firm's 225 lawyers located in Boston, Washington, and the Emerging Enterprise Center in Waltham, Massachusetts join with a network of Lex Mundi law firms to provide global support for clients' largest challenges and opportunities. For more information visit foleyhoag.com.

About the Security and Privacy Practice

Foley Hoag's Security and Privacy practice provides clients with experienced and effective legal counsel on the security and privacy issues encountered by businesses that often require immediate and discreet solutions. We actively guide our clients through the process of complying with the ever-growing number of state, federal, and international laws governing information security, identity theft, surveillance and other privacy issues. We have decades of experience in investigating, litigating and resolving a wide variety of security incidents, including thefts of confidential information, government investigations, competitive espionage, as well as breaches and leaks involving proprietary data.

Our lawyers advise clients striving to guard company records, personnel files, customer data, intellectual property and other valuable information assets. The Security and Privacy practice is a comprehensive advisory service for clients that face an expanding universe of security and privacy issues that affect numerous industries, including technology companies, healthcare providers, investment and financial services firms, manufacturing companies, government contractors, insurance companies, and retail businesses.

Our lawyers assist clients with questions on how to legally and ethically investigate abusive email, take down infringing websites, maintain surveillance of company facilities and information systems, and fix breaches of security. We work with clients to ensure the legality and success of existing security policies and protocols and help them develop new programs when necessary. Our lawyers have managed unexpected crises ranging from surprise inspections by government investigators, to obtaining

emergency court orders needed to secure stolen company computers from rogue insiders. Above all, we successfully safeguard our clients' confidential information and manage each matter with the level of attention and discretion companies require from security and privacy professionals.

We draw together experienced counsel from all areas of legal specialty, including litigation, labor and employment, business crimes and government investigations, intellectual property, technology transactions, health care, regulatory compliance and tax. This enables us to provide efficient, cross-disciplinary solutions tailored to our clients' needs.

Gabriel M. Helmer

Click the image below for a full biography.




Gabriel M. Helmer

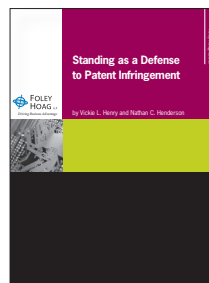
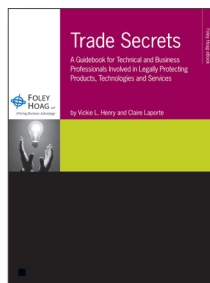
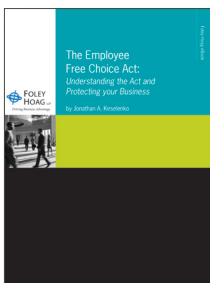
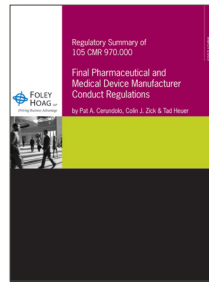
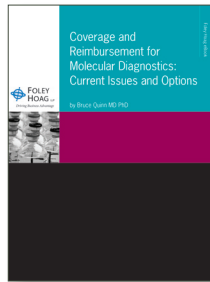
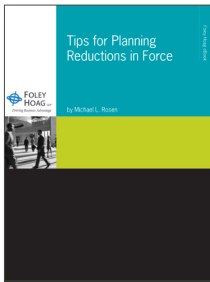
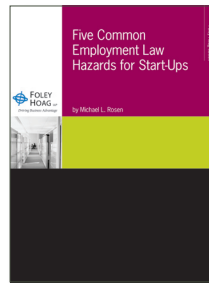
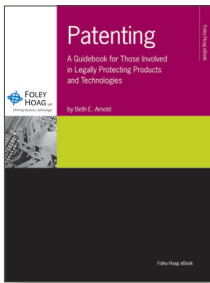
Although he has a varied litigation practice, Gabriel Helmer focuses on helping clients protect their sensitive business data and systems, as well as their intellectual property assets. He advises companies faced with electronic espionage and data theft, breaches of computer and network security, as well as electronic, audio and video surveillance, and has helped them prevail in court against the competitors and rogue employees who committed these actions. Gabriel also helps clients investigate and respond to anonymous Internet activity that involves the clients' intellectual property, including unauthorized transfers and public disclosures of proprietary information. As part of his information security work, he develops security policies and procedures that enable multinational companies to conduct internal investigations of security breaches, while complying with U.S. surveillance and privacy laws.

Foley Hoag eBook Library

Sample other free titles from the Foley Hoag eBook library, sign-up for industry-specific alerts and updates from Foley Hoag, or visit our Web site.

Visit our Web site  Sign up for industry-specific alerts and updates

You may also be interested in our eBook series. Simply click on an image to download or visit foleyhoag.com for our library.





617 832 1000 *tel* 617 382 7000 *fax*

BOSTON | WASHINGTON | EMERGING ENTERPRISE CENTER | FOLEYHOAG.COM