Gramm-Leach-Bliley Safeguard Rule Package

Insights
5.01.03

As many of you know, Gramm-Leach-Bliley requires "financial institutions" to establish and implement a Safeguard Rule Compliance Program or Safeguard Program to protect non-public customer information. This law covers the obvious financial institutions, but also generally covers any entity that obtains or uses customer financial information, including auto dealerships, retail stores, etc. The deadline for compliance is May 23. We have prepared a document that sets out compliance guidelines, a few sample forms, and a cover letter for your convenience.

COVER LETTER
May ___, 2003

Re: Gramm-Leach-Bliley Safeguard Program Compliance Guidelines

Dear _____:

The Gramm-Leach-Bliley Act ("GLB" or "the Act") was enacted in 1999. Among the provisions contained in the Act is a set of rules designed to protect the privacy interests of individuals in their interactions with various financial institutions. Because of the Act's broad definition of "financial institution," however, almost any organization that deals with or obtains "non-public personal information," is required to abide by the Act. This covers almost any organization that requires a credit application or consumer profile. If you have a question as to whether your organization is subject to the Act, you should contact your corporate or employment counsel.

As of July 2001, affected entities have been required to make disclosures to consumers that their non-public information, usually in the form of credit applications or other financial data, may be disseminated to other parties, such as credit or financing agencies. Affected entities must also provide the consumer, customer, or client a reasonable opportunity to decline to have their information disclosed.

To facilitate compliance with the Act, prudent employers conducted training regarding the Act's privacy provisions and the procedures to be used when handling private customer information. Questions about the "Privacy" elements of the Act should be directed to your corporate or employment counsel.

By May 23, 2003, affected organizations must comply with a second portion of the Act requiring them to establish, implement, and maintain a comprehensive written program to ensure the security and integrity of customer information. Pursuant to regulations promulgated by the Federal Trade Commission, this "Safeguard Program" should provide reasonable administrative, technical, and physical safeguards to protect the customer's information from unauthorized disclosure, alteration, or deletion. The regulations also require organizations to take reasonable steps to engage and utilize only those business partners and services providers that are capable of maintaining appropriate measures to safeguard the protected customer information.

Fisher Phillips has developed the enclosed guidelines to assist employers in understanding and complying with their obligations under the Act. Although each entity's Safeguard Program will be unique because of its particular facts and circumstances, there are common elements that every Safeguard Program will be required to include, and certain steps each entity should take in developing and implementing its Program. The generalized information contained here, however, is not intended to serve as particularized legal advice. Organizations that have specific questions relating to the Act, the regulations, or the development and implementation of a Safeguard Program should immediately contact their corporate or employment counsel.

If you have any questions regarding your compliance with the Safeguard or Privacy provisions of the Act or the FTC regulations, please do not hesitate to contact your Fisher Phillips attorney or other competent counsel.

Regards,

For Fisher Phillips

GUIDELINES FOR COMPLIANCE WITH GRAMM-LEACH-BLILEY SAFEGUARD RULES

These Guidelines will walk you through the development and implementation process, as well as recommend procedures for maintaining your Program and certifying your third-party service providers. Where appropriate, we have noted potential problem areas in Program development and implementation. Again, given the very general language of the Act and the FTC regulations, the information provided below is necessarily not specific, and should only be used as a template to develop your own particularized Program. Please refer any specific questions regarding compliance with the Act or the regulations to your employment or consumer counsel.

The Regulations

The Federal Trade Commission's regulations mandating a Safeguard Program do not provide much detail or guidance. Instead, the regulations set forth three broad objectives for a Program and delineate five general elements each Program must include.

The three objectives your Program must meet are:

- Insure the security and confidentiality of customer information;

- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

To help ensure that your Program meets these objectives, the FTC requires that every Program, at a minimum, contain these five elements:

- Designation of a Safeguard Program Coordinator or Coordinators;
- A thorough analysis of the potential internal and external risks to the security, confidentiality, and integrity of customer information;
- Design and implementation of safeguards to control the identified risks;
- Provisions for the selection and oversight of qualified third-party service providers; and
- Provisions for the monitoring, regular evaluation, and adjustment of the Program to accommodate changing business practices or other circumstances.

The regulations do not specify how detailed a Program must be to satisfy the mandate or how often a Program must be evaluated or adjusted. You should not, however, be careless in the development, implementation, or maintenance of your Program. The Program must be appropriate to the size and complexity of your organization, the scope of your financing and leasing activities, and the sensitivity of the customer or client information that you possess.

Neither the Act nor the regulations articulate what penalties you may face for failing to implement an effective Safeguard Program. Presumably, the FTC could initiate an Unfair Trade Practice proceeding in response to a customer complaint or otherwise suspected violation. Penalties for Unfair Trade Practice violations include monetary fines, actual and punitive damages, as well as injunctive relief.

Designation of a Safeguard Program Coordinator

The FTC regulations require that each organization appoint a Safeguard Program Coordinator or Coordinators. The regulations expressly state that this position must be held by an employee. Thus, it cannot be outsourced.

The regulations also contemplate that you may choose to appoint a committee to manage the coordination of the Safeguard Program. By engaging the experience, knowledge, and resources of several employees from various departments or offices, you may make your organization's Program more targeted, less cumbersome, and less expensive to operate.

There are several other considerations you should keep in mind:

- Appoint a corporate officer or other member of senior management to act as the Coordinator or supervise the Coordinator team;
- Establish a clear chain of command for the Coordinator;
- Appoint low-turnover or long-term employees to Coordinator positions; and
- Establish transition protocols for when a replacement Coordinator is required.

Assessing and Minimizing the Risks of the Misappropriation of Consumer Information
After designating a Coordinator, you must next undertake to "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks."

Again, the regulations provide only minimal guidance as to what is actually necessary to satisfy this requirement. Risk assessment should include all "relevant" areas of the operation. The regulations state that relevant areas will include, at a minimum: "(1) employee training and management; (2) information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) detecting preventing and responding to attacks, intrusions or other systems failures."

Employee Training and Management
All employees should be notified that your organization emphasizes customer privacy and that you have implemented a Safeguard Program. Certain personnel, e.g., your Accounting department, Information Technology staff, Management, and other employees that have access to processes, or otherwise use customer information, should receive more technical and specific instruction. Independent contractors should also receive training that comports with their access to sensitive information. Not only will these contractors likely be subject to the "service providers" provisions of your Program, to the extent that they have access to and use customer information for the benefit of your organization, their failure to comply with the Program may result in liability for your organization, irrespective of their technical relationship to the organization. You should not, therefore, distinguish between employees and independent contractors: any person with access to customer information should receive notice of your policy and training.

Current employees should be informed that the Program is official organization policy, and employees should acknowledge that policy, as well as their understanding that failure to abide by the policy will result in discipline, up to and including termination. For new hires, you should include Safeguard Program training in your normal orientation and also require acknowledgment of the policy. A sample Acknowledgment Form is attached to these Guidelines as Exhibit A.

Here are some other basic steps you can take to help maintain the security and integrity of protected consumer information:

- Only those employees and contractors who require access to consumer information should be given access;
- Rooms and file cabinets that contain sensitive information should be locked or otherwise secured;
- Documents that contain sensitive information should not be left where they can be easily compromised, such as in meeting rooms or in other open areas. Managers and other employees should be alert for documents that are left in inappropriate places;
- Computers that contain or have the ability to access sensitive information should be password-protected and either turned off when not in use or should have a password-protected screen-saver enabled; and
- Requests for information about customers from outside parties should be referred to an appropriate contact person within the organization.

You can also take several relatively simple steps to protect information from misappropriation or deletion:

- Inform applicants and new hires that your organization emphasizes customer privacy and that you have a Safeguard Program in place;
- Conduct background checks on applicants, particularly on applicants for positions that will have access to sensitive information;
- Encrypt protected customer information whenever it is transmitted electronically;
- Immediately change or delete the logins and passwords of employees or contractors no longer associated with the organization;
- Communicate changes in the Safeguard Program and have employees acknowledge the changes; and
- Enforce the Program actively by monitoring employee compliance and issuing prompt and effective discipline for violations.

Finally, you should continue to work closely with your corporate or employment counsel to address changing circumstances and new developments in the law and its application and enforcement.

Network & Information System Integrity

You must also assess and minimize the risks of customer information compromise with respect to information technology systems, including, but not limited to, paper files, your computers and servers, internet access, and back-up files**.** Obviously, each organization handles customer information differently. Therefore, in this area of the Safeguard Program, you should critically review how your organization collects, accesses, processes, stores, distributes, backs-up, transmits, and destroys the protected information, and customize your Program accordingly.

At a minimum each organization should take the following steps:

- Store records in a secure area:
- Hard copies, such as paper documents, should be stored in controlled-access areas, such as locked rooms and locked file cabinets;
- Electronic data should be stored on secure servers that also have limited access. Unless absolutely necessary, private customer information should not be stored on servers that also provide internet access or can be accessed remotely;
- Access to sensitive information should be monitored and recorded, e.g., a record should be kept of who views electronic data when, and hard copies should have to be "signed out" of a central repository; and
- Back-ups should be made regularly and stored in a separate facility, preferably in a completely separate physical location.
- Provide for secure data transmission when collecting or transmitting customer or other protected information:
- Secure connections, passwords, and encryption should be used whenever data is transmitted electronically;
- Customers submitting information to the organization should be reminded to take all necessary precautions. Secure transmissions from the customer to the organization should be automatic if possible; and
- If it is necessary to fax or mail information, appropriate precautions should also be taken, such as providing secure or private fax machines, use of private couriers, and the regular use of confirmations.
- Dispose of customer information in a secure manner:
- Hire, designate, or outsource a records retention manager/specialist to supervise the disposal of information;
- Shred or recycle sensitive documents;
- Completely erase all data when disposing of computers, diskettes, tapes, and hard drives that might contain sensitive information;
- When necessary, properly and effectively destroy all computer hardware used to store or access customer information; and
- Regularly and properly purge customer files of outdated customer information.
- Use adequate oversight and audit procedures to detect the misappropriation or loss of protected information. Each customer list or file should contain a code or identifier so that contacts, access, or changes can be monitored and controlled.

access, or changes can be monitored and controlled.

- Maintain a close physical inventory of all computer hardware.

Again, neither the Act nor the FTC regulations specify how robust your organization's security must be. You are best advised, therefore, to use currently accepted industry standard protection methods and, above all, common sense. For more sophisticated protection issues, your organization should not hesitate to engage qualified technical and security expertise**.**

Contingency Planning

The regulations also specify that you should pay particular attention to prevention, detection, and response to attacks, intrusions, or other system failures. Many of the above-described training and technical safeguards are also applicable to this element, but there are also several other steps you should take to ensure that customer information is protected.

Any Safeguard Program should include a written and readily accessible contingency plan to address any foreseeable breaches of physical, administrative, or technical safeguards. This document should not only include appropriate procedures to deal with various types disasters, but also a comprehensive list of contact information, including your Program Coordinator, management team, computer and software vendors, employment and corporate counsel, and disaster recovery services. A prompt response to an emergency or violation may reduce potential liability.

Specifically, you should also consider the following:

- Routinely check with software vendors to obtain and install patches that address software vulnerabilities;
- Install anti-virus software that updates automatically;
- Maintain and monitor up-to-date firewall protection;
- Centralize management of security tools and operations;
- Back-up data regularly and store the back-up media at an alternative and secure location. Further, back-ups should be periodically checked for viability and readability;
- Maintain a log for access to nonpublic consumer information to ensure that access is granted only to valid and authorized users. Such a log will not only aid in an investigation of a compromise, but also could assist in recouping or rebuilding the information;
- Develop methods and materials to promptly notify customers should their information ever be lost, damaged, or stolen; and
- Anticipate different types of emergencies such as internal and external theft, fraud, and vandalism.

By nature, emergencies and disasters are unexpected. The Act and the regulations, therefore, only obligate you to address "reasonably foreseeable" attacks, intrusions, or other system failures. What

constitutes "reasonably foreseeable" will depend on the nature of your operations, the location of your organization, and the amount of information that needs protection.

Design and Implementation of Your Safeguard Program

After you have completed the assessment of your existing privacy protection measures in the above areas, it is likely that certain risks will have been identified. The FTC regulations mandate that you take steps to control these risks and regularly test and monitor the effectiveness of the overall program.

Determining what risks can and should be addressed will be determined by several factors, but again, the government has provided very little guidance. Therefore, you should perform a cost-benefit analysis, and balance the size of the operation, the complexity of the customer information used, the volume of the information, and the sensitivity of the data, with the practicability of the available measures. Presumably, you will implement a plan that appropriately considers the cost of available technology and other safeguards and the relative benefits those measures provide in securing the customer information.

Selection and Oversight of Third-Party Service Providers

The FTC regulations also require you to oversee third-party service providers. A "service provider" is "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this [regulation]." Therefore, any organization that you do business with that can come in contact with protected information, such as an outsourced information technology department, a customer relations management firm or lead provider, a third-party finance or insurance platform, or an outsourced accounting department will be subject to oversight and compliance with the Act and the regulations. Note also that individual independent contractors will also be subject to oversight and compliance.

To fulfill your responsibilities under the regulations, you must (1) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the protected customer information, and (2) include the implementation and maintenance of such safeguards in your contracts with service providers. The regulations, however, do not define what "reasonable steps" are. Therefore, deciding how to select and retain service providers that are compliant with the regulations will likely be as subjective as other parts of developing your Safeguard Program. At a minimum, however, you should:

- Ask current and potential providers about their ability to comply with the FTC requirements for safeguarding;
- Note suggestions for compliance made by all service providers, even those that are not ultimately selected or retained;
- Request documentation regarding measures each provider can and will take to comply with your obligations under the Act and the regulations;

- Request and check references for potential providers;
- Discuss your requirements with the providers and obtain written guarantees respecting the measures they will implement and the cautions they will exercise;
- Obtain written guarantees in terms of contingency and security planning, as well as response and maintenance times in case of security breaches or other emergencies or failures;
- Set clear expectations for reporting mechanisms;
- Where appropriate, require a demonstration of the safeguarding policies, procedures, and protocols;
- Provide for early termination of the contract and liquidated damages should the provider not meet your clearly articulated expectations and legal obligations; and
- Require indemnification by the provider should your organization be found liable for an information misappropriation due to a failure on behalf of the provider.

After you are comfortable that a particular service provider can adequately comply with the requirements of a Safeguard Program, the regulations state that you must ensure compliance by express contract. An example of possible contract language is attached as Exhibit B. Although the contract language for each provider is likely to vary based on the services contracted for, as well as the other variables described above (such as the complexity and volume of protected information at issue), there is no requirement that a separate contract with each provider, apart from the normal contract for services, be executed. Pragmatic service providers may include compliant guarantee language in their normal contracts. Nevertheless, you should have such agreements reviewed by your corporate or employment counsel to make sure that your interests are adequately protected.

The deadlines for compliance with this provision of the regulations are express and quickly approaching. If you have contracts with service providers that were entered into on or after June 25, 2002, you are required to revise those contracts by May 23, 2003. For contracts entered into *before* June 25, 2002, the contract must be compliant by May 24, 2004.

Maintenance of Your Safeguard Program

The Safeguard Program and its corresponding obligations are ongoing. Furthermore, the regulations require regular testing, evaluation, and adjustment to ensure continuing compliance and protection to the consumer.

First, you are required to "regularly test or otherwise monitor the effectiveness of the safeguards, key controls, systems, and procedures." These "key" elements may include such things as your computer system, your data filing and storage policies and procedures, as well as employee and management training.

Given the flexibility of the FTC standard, your initial efforts to safeguard customer information may be inadequate, but the inadequacies may only be discoverable after the measures have been in place

for a certain amount of time. In such a case, only regular monitoring will reveal the deficiencies. As such, it will be critical to take such precautions as:

- Routinely test your employees on their knowledge of the Safeguard Program and its policies;
- Encourage your employees to report problems and suspected violations of the Program;
- Ensure that data is protected by regularly making sure doors, files cabinets, and computers that protect information are locked and secure, and that only authorized personnel have access;
- Use and review access records and logs;
- Visually inspect work areas for unprotected or easily accessible protected information;
- Upgrade your software and hardware as necessary and as suggested by your IT professionals and service providers;
- Quickly and thoroughly document any actual or suspected system failures, and take prompt remedial action; and
- Pay particular attention to the three main areas highlighted by the FTC regulations, i.e., employee training and management; information systems; and detecting, preventing, and responding to attacks, intrusions, and other system failures.

The regulations do not specify how often your "key controls" should be tested. Nevertheless, the less effort required to test a certain element, the more often it should be tested. For instance, visual inspection of physical controls such as locks, filing cabinets, and computer passwords should be done almost daily. More technical protective measures should be monitored regularly with scheduled testing and reporting.

In addition to this regular testing and monitoring, the regulations also require you to "[e]valuate and adjust [your] information security program in light of (1) the results of the testing and monitoring . . . ; (2) any material changes to [your] operations or business arrangement; (3) or any other circumstances that [you] know or have reason to know may have a material impact on [your] information security program." This "catch-all" provision suggests that the FTC sees your Safeguard Program as a permanent part of your continuing business, and expects that changes to your Program will accompany changes to your organization. Consequently, your Safeguard Coordinator(s) should be consulted, and the Program revised as necessary anytime:

- Computer hardware or software is upgraded or otherwise replaced;
- Sensitive information is moved;
- New procedures or products are put in place; or
- Key personnel are replaced or any other time circumstances call for a "material change" to business operations or the Safeguard Program.

Obviously, you will want to conduct a cost-benefit analysis to determine what, if any, other measures you should put in place to protect or secure sensitive customer information. In the event that customer information is inadvertently misappropriated, disclosed, or worse, used, you will want to be able to show that you took every reasonable step to prevent harm to the consumer. To that end, do not hesitate to seek competent assistance to design, implement, monitor, or revise your Safeguard Program.

EXHIBIT A

Customer Privacy Policy
[Organization Name] places a strong emphasis on its customers' and clients' privacy. As part of this emphasis, **[Organization]** has developed and implemented a Safeguard Program that makes every effort to protect non-public customer information, such as credit application information, bank account numbers, social security numbers, telephone numbers, and addresses, from unauthorized disclosure, theft, alteration, deletion, or any other type of misappropriation.

[Organization]'s Safeguard Program requires its employees, contractors, and third party service providers to take appropriate measures to protect the security and integrity of non-public customer information. These measures include, but are not limited to:

- Not leaving customer information or private documents unattended where they can be easily viewed, copied, or taken;
- Locking rooms and file cabinets where customer data is stored;
- Utilizing unique computer passwords, changing the passwords often, and not posting passwords at or near computer terminals;
- Not allowing unauthorized use of computer terminals or access of customer files;
- Referring any unusual requests for customer information to the Safeguard Program Coordinator or your supervisor;
- Promptly reporting to the Safeguard Program Coordinator or your supervisor anytime you know or suspect that customer information has been compromised or misappropriated.

If you have any questions about the Safeguard Program, or need to report a potential violation of the policy, please contact your Safeguard Program Coordinator, **[insert Coordinator's name and telephone number]**.

Employee Acknowledgment of

[Organization]'s Customer Privacy Policy
My signature below indicates that I understand that **[Organization]** has a policy to protect its customers' and clients' privacy. I have read the policy, and I understand that the policy requires me to take appropriate steps to protect information about **[Organization]**'s customers and clients from

unauthorized access, use, deletion, or other misappropriation. Further, I understand that if I have any questions regarding the **[Organization]**'s privacy policy or if I believe that the policy has been violated, I should immediately contact the Safeguard Program Coordinator or my supervisor.

I also understand that if I fail to comply with the **[Organization]**'s privacy policy, that I may face discipline, up to and including termination.

_____

Date

_____

Employee Name

_____

Employee Signature

EXHIBIT B

1. Customer Information Safeguards.

(A) As a service provider to **[Organization]**, a financial institution that is subject to the Gramm-Leach-Bliley Act and Federal Trade Commission regulations (16 C.F.R. §§ 313 - 314), that may receive, maintain, process, or otherwise access non-public customer information (as defined in the above regulations) through provision of services directly to **[Organization]**, **[Contractor or Service Provider name]** agrees to implement and maintain appropriate safeguards to: (1) insure the security and confidentiality of non-public customer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

(B) **[Contractor or Service Provider]** agrees that should it, for any reason, not be able to provide or maintain appropriate safeguards to fulfill its obligations under Paragraph 1(A), it will immediately inform **[Organization]** of such inability and such inability on **[Contractor or Service Provider**]'s part will serve as justification for **[Organization]**'s termination of this contract at anytime after the inability becomes known to **[Organization]**. **[Contractor or Service Provider**] agrees to hold **[Organization]** harmless for any and all damages it may incur from **[Organization]**'s termination of this contract pursuant to this provision.

(C) **[Contractor or Service Provider]** agrees that it will fully indemnify, reimburse, and otherwise make whole **[Organization]** should **[Organization]** be held liable to any party or entity (private or public) for any compromise or misappropriation of non-public customer information because of a

failure of **[Contractor or Service Provider**] to provide or maintain appropriate safeguards as defined in Paragraph 1(A) of this contract. Such indemnification shall include, but is not limited to, all actual and punitive damages or fines paid by **[Organization]**, any lost revenue due to a court or administrative injunction, and all attorneys' fees and costs. Further, **[Contractor or Service Provider]** agrees to reimburse **[Organization]** for all costs **[Organization]** incurs in enforcing this provision.