

Gramm-Leach Bliley Act

Complying with the Technical Requirements of the Standards Rule

People provide their personal data every day to banks, financial services and businesses with the belief that the organizations will take appropriate measures to protect their sensitive information. However, data exposure incidents continue to rise as hackers and thieves learn to exploit gaps in corporate security. Many companies fined under the Gramm-Leach Bliley Act all lacked one common protection tool—encryption. Encrypting email, media, hardware and network folders and drives is essential to meeting the requirements as outlined in the GLB act.

GRAMM-LEACH BLILEY

The Gramm-Leach Bliley (GLB) Financial Modernization Act of 1999 requires financial institutions and businesses providing financial services (such as credit) to ensure the security and confidentiality of customer's nonpublic personal information. It additionally requires institutions to give customers privacy notices and in turn, allow customers to limit the sharing of their data. Nonpublic information includes name, address, social security number, account numbers, identification of an individual as the customer of a particular financial institution, information provided on applications, information collected from internet cookies, information resulting from transactions for financial products or services, and lists that include publicly available information if the lists are created based on NPI.

The GLB Act has seven provisions (Appendix A); however, it is Title V regarding privacy to which companies are ramping up their compliance efforts. The three principle parts to the privacy rule are: the Financial Privacy Rule, the Safeguards Rule and pretexting. The pretexting rule protects consumers from individuals and companies that obtain their personal financial information under false pretenses.

THE FINANCIAL PRIVACY RULE

The Privacy Rule regulates the collection and disclosure of customers' personal information. It requires financial institutions to distribute to its customers its privacy policies and practices regarding how it shares nonpublic personal information with both affiliates and third parties. Additionally, the law requires that financial institutions offer a reasonable way for customers to "opt-out" or refuse to allow their information to be shared with third parties.

The Privacy Rule also limits what the recipients of nonpublic personal information can do with that information. For example, if a customer opts-out of a financial institution's sharing policy but the institution has an affiliated data processing company that must receive the customer data to complete the original transaction, the data processing company is entitled to receive the data, but may not then forward or sell that customer's information to another organization.

The integration of security and compliance is top of mind in 2008. In recent years, the industry witnessed the enforcement of regulations such as Gramm-Leach Bliley by agencies to combat the ever increasing risks of data exposure and identity theft. Organizations know through these regulations and customer expectations that they are accountable for the protection of sensitive data. This need to protect customer information from unauthorized access is the foundation of the Gramm-Leach Bliley Act. Companies must not only show on paper their data protection policies, but must also have technical solutions in place that in fact enforce those policies and securely protect sensitive data wherever it may reside. This paper discusses the protection of non-public personal information as outlined in Section 501b of the Gramm-Leach Bliley Act's Safeguard Rule, who must comply, and how PolicyBridgell™ from Digital Info Security Company can help organizations proactively enforce policies and protect data.



THE SAFEGUARDS RULE AND SECTION 501B

The Safeguards Rule calls for financial institutions to design, implement and maintain safeguards to protect customer information. Under the GLB Act's Privacy provision, the Safeguard Rule outlines what types of information must be protected, by whom and under what circumstances. Section 501 (b) discusses security provisions that require financial services entities to establish administrative, technical, and physical safeguards that:

1. Insure the security and confidentiality of customer records and information;
2. Protect against any anticipated threats or hazards to the security or integrity of such records; and
3. Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

There are nine agencies (Appendix B) that oversee the enforcement of the GLB Act. While each of the enforcing agencies are fairly prolific in their Final Rules for the Privacy Rule, they have collectively adopted a uniform stance with the Standards Rule:

"...each financial institution must develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of any customer information at issue."¹

Given recent headlines exposing US corporations that have leaked or lost their customers' nonpublic data, the now vague guidelines for the Safeguards Rule of Title V are ripe for greater statutory definition. With that consideration, it makes ethical and economic sense for financial institutions to implement automated, scalable data protection systems that enforce the required written policies for high-traffic areas that exchange or store customer nonpublic data. Considering the pervasive use of email to communicate and share nonpublic personal information in the financial world, it should be a top priority for companies to include a solution that can automatically secure, monitor, audit and archive the flow of email and financial information into and out of the enterprise as part of the GLB Act compliance infrastructure.

POLICYBRIDGE™ II FROM DIGITAL INFO SECURITY COMPANY (DISC)

PolicyBridge™ II is the only solution on the market today to integrate powerful digital communications monitoring technology, full-text indexed archiving and retrieval and policy-based compliance with strong encryption and digital rights management capabilities. These are powerful security and compliance tools that extend and enforce regulatory and corporate security policies to the desktop, email, removable media and recipients. The PolicyBridge™ II product family consists of three modular software offerings.

SECURSCAN™ FOR EMAIL COMPLIANCE

SecurScan is a powerful compliance tool that actively scans inbound, outbound and internal messages (email, instant messaging and Bloomberg). Using an intelligent, context-based lexicon, SecurScan identifies potential violations and securely indexes and archives digital communications. An integrated console provides comprehensive discovery tools for efficient and timely retrieval. SecurScan can be deployed post-process or pre-process. In pre-process, SecurScan provides active policy management and applies policies such as block, quarantine for review, route to administrator or automatically encrypt to triggered messages. All actions are archived for compliance.

SECURWRAP™ FOR DATA PROTECTION

SecurWrap provides easy-to-use yet powerful data encryption for email, desktops, laptops, file servers, and removable media. SecurWrap allows users to share encrypted content with other users by encapsulating information in a "wrapper." Our permission wrapper technology is a collaboration-enabling solution that provides a self-contained mechanism for encryption, digital rights management, auditing, and authentication. It flexibly supports online and offline access to all types of files in email, on removable media or to data-at-rest.

¹ Federal Register / Vol. 67, No. 100 / Thursday, May 23, 2002 / Rules and Regulations



GUIDELINES FOR COMPLIANCE WITH SAFEGUARD RULE 501B

TECHNICAL 501B GUIDELINES	POLICYBRIDGE™ II COMPLIANCE FEATURES
Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.	Policy Enforcement: To protect all digital communications, SecurScan can be deployed as a post-process message archiving and scanning engine or as a proactive, pre-processing solution with policy enforcement and message security. SecurScan actively scans inbound, outbound and internal email using a finely honed, industry-tailored lexicon. Potential compliance and security violations are identified and policies are automatically enforced to block, quarantine, re-reroute for review or encrypt. Messages and policy actions are indexed and securely archived.
Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.	Policy Education: PolicyBridge™ II can be an invaluable tool to educate appointed security employees regarding how often nonpublic personal information is being transmitted and uncover patterns of misuse or personnel who may require further training on corporate policies regarding secure customer information systems.
Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.	
Access controls on customer information systems including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.	Automatic Encryption: To protect data-in-motion, SecurScan content monitoring identifies sensitive information and can block, quarantine for review or automatically encrypt the message. SecurScan policies can be tailored by groups and individuals allowing for authorized individuals to send information in an encrypted email while blocking the same content sent from unauthorized individuals, groups or domains. Proactive Encryption: To protect data-at-rest (hardware, servers and media) – the SecurWrap module offers powerful data encryption with digital rights management. SecurWrap's revolutionary wrapper technology features a tamper-resistant audit trail. This audit trail records all access and activity with respect to the protected content, keeping a forensic trail of user actions.
Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.	Additionally, the automated policies defined by each organization control who can access information, what actions they can perform, and whether copies are archived. Ideal for the protection of media in transit as access can be audited and if lost, access can be dynamically revoked.
Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.	SecurWrap encryption is based on industry-standard encryption algorithms: AES (128, 256, 448 bit), DES, TripleDES, Blowfish, and Rijndael. These are powerful elements to prevent alteration, destruction or loss of regulated information.
Protect against destruction, loss, or damage of customer information.	
Proper disposal of all consumer information.	When customer information enters its last phase of the lifecycle, PolicyBridge™ II “wipes” all data, ensuring that sophisticated tools cannot recover nonpublic personal information from databases, document or emails.



WHO MUST COMPLY

The GLB Act applies to “financial institutions,” which includes any institution that engages in financial activities or services. This definition is quite broad and includes banks, lenders, securities and investment firms and insurance companies; plus a wide array of non-banking entities. Some examples include: companies who engage in any kind of lending or loan servicing, tax preparers, financial advisors, retailers who extend credit, accountants, payment processors, real estate service providers, debt collectors, credit bureaus and even certain lawyers.

PENALTIES

Penalties and sanctions are controlled by each of the agencies (Appendix B) according to their jurisdiction. There are no specific penalties in the GLB Act regarding lost or compromised nonpublic customer financial information due to inadequate security safeguards. However, many legislators are currently seeking tougher enforcement and penalties.

ABOUT DIGITAL INFO SECURITY COMPANY® (DISC)

A leader in secure email compliance and data protection, DISC provides comprehensive solutions of email scanning with persistent policy management, compliance archival and auditing, and powerful encryption for email and company data. DISC solutions help enterprises with email compliance and protect themselves against intellectual property or business critical data leakage. DISC is headquartered in Westminster, CO, and is a publicly traded company under the symbol DGIF.



888-841-5970
info@disecurityco.com
www.disecurityco.com



APPENDIX A: THE PROVISIONS OF THE GLB ACT

TITLE I -- Facilitating affiliation among banks, securities firms, and insurance companies
TITLE II -- Functional regulation
TITLE III -- Insurance
TITLE IV -- Unitary savings and loan holding companies
TITLE V -- Privacy
TITLE VI -- Federal home loan bank system modernization
TITLE VII -- Other provisions

EFFECTIVE DATES OF KEY PROVISIONS IN THE GLB ACT

The Gramm-Leach-Bliley Act became Public Law 106-102 with President Clinton's signature on November 12, 1991. Following are the effective dates of key provisions in the law:

Title I -- Facilitating affiliations among banks, securities firms and insurance companies: Becomes effective 120 days after date of enactment, except for Section 104, which deals with the operation of state law and contains the insurance safe harbor provisions.

Title II -- Securities and Exchange Commission provisions generally become effective 18 months after date of enactment.

Title III -- Insurance customer protections are effective immediately.

Title IV -- Prohibition against new unitary savings and loan holding companies becomes effective immediately.

Title V -- *Subtitle A*: Rules for the disclosure of institutions' privacy policies must be issued by regulators within six months of the date of enactment. The rules will become effective six months after they are required to be prescribed unless the regulators specify a later date. *Subtitle B*: Criminal penalties for pretext calling are effective immediately.

Title VI -- Federal Home Loan Bank System modernization is effective immediately unless otherwise provided in specific sections.



APPENDIX B: AGENCIES RESPONSIBLE FOR THE GOVERNING OF GLB

Title V: Section A: Privacy and the Disclosure of Non Public Information of the Gramm-Leach Bliley Act commissions the following agencies, operating under their respective provisos:

1. Under section 8 of the Federal Deposit Insurance Act, the "Banking Agencies" include:
 - a. The Office of the Comptroller of the Currency (OCC) – has jurisdiction over national banks, federal branches and federal agencies of foreign banks and their subsidiaries.
 - b. The Board of Governors of the Federal Reserve System (Board) – has jurisdiction over member banks of the Federal Reserve System branches and agencies of foreign banks, commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act, and bank holding companies and their non-bank subsidiaries or affiliates.
 - c. The Board of Directors of the Federal Deposit Insurance Corporation (FDIC) - has jurisdiction over banks insured by the Federal Deposit Insurance Corporation and insured state branches of foreign banks and their subsidiaries.
 - d. The Director of the Office of Thrift Supervision (OTS) - has jurisdiction over savings associations whose deposits are insured by the Federal Deposit Insurance Corporation, and their subsidiaries.
2. Under the Federal Credit Union Act:
 - a. The National Credit Union Administration (NCUA) - has jurisdiction over any federally insured credit union and its subsidiaries.
3. Under the Securities Exchange Act of 1934, the Investment Company Act of 1940, and the Investment Advisors Act of 1940, respectively:
 - a. The Securities and Exchange Commission (SEC) - has jurisdiction over brokers and dealers, investment companies, and registered investment advisors.
4. Under the Federal Trade Commission Act:
 - a. The Federal Trade Commission (FTC) - has jurisdiction over any other financial institution or other person engaged in "substantial financial activity" that is not subject to the jurisdiction of any other agency or authority, such as non-depository lenders, consumer reporting agencies, debt collectors, data processors, courier services, retailers that extend credit by issuing credit cards to consumers, personal property or real estate settlement services, check-cashing businesses, mortgage brokers, tax preparers and others.
5. Under the Commodity Exchange Act, amended by the Commodities Futures Modernization Act of 2000 (CFMA):
 - a. The Commodity Futures Trading Commission (CFTC) – has jurisdiction over futures commission merchants (FCMs), commodity trading advisors (CTAs), commodity pool operators (CPOs) and introducing brokers (IBs).
6. Under State insurance law:
 - a. State Insurance Authorities - have jurisdiction over of the state in which the insured lives for any person engaged in providing insurance.

Each of these agencies was required to publish a Final Rule on the two major sections of Title V Section 501: (a) the Financial Privacy Rule and the (b) Safeguards Rule.

