



GRAMM-LEACH-BLILEY ACT & FFIEC REGULATORY COMPLIANCE



PERIMETER E-SECURITY

- ▶ Providing a single, complete source for all your security needs since 1997
- ▶ Constant, around the clock monitoring with over 150 security personnel analyzing information 24/7/365
- ▶ Continuous third party assessments including an annual SAS 70 Type II and Cybertrust security audit
- ▶ Three redundant data centers and seven offices nationwide
- ▶ Profitable for past 8 calendar years (audited financials available)
- ▶ Servicing over 1,600 financial institutions in the United States

Call Us Toll Free: 800.234.2175

[C](#) [W](#) [S](#) [D](#) Sales Sheet

DEFINING THE GRAMM-LEACH-BLILEY ACT

The Gramm-Leach-Bliley Act (commonly called GLB or GLBA) is also known as the Financial Modernization Act of 1999. The GLB Act includes provisions to protect all consumers' personal financial information held by financial institutions. Member organizations of the FFIEC have contributed to the GLB Act by defining security objectives based on best security practices around the theme of confidentiality, integrity, and availability of systems and information.

The GLB Act applies to "financial institutions" - businesses that offer financial products or services. Financial institutions include banks, insurance companies, and securities firms. Also, non-traditional financial institutions are required to comply and include companies that offer financial products or services to individuals like loans, financial or investment advice, or insurance.

The GLB Act includes several rules that increase the requirements financial services companies have to keep information secure:

The Financial Privacy Rule

The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected.

Safeguards Rule

The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. This rule is intended to do what most businesses should already be doing: protecting their clients. The Safeguards Rule forces financial institutions to take a closer look at how they manage private data and to do a risk analysis on their current processes. No process is perfect, so this has meant that every financial institution has had to make some effort to comply with the GLBA.

Pretexting Protection

Pretexting (sometimes referred to as "social engineering") occurs when someone tries to gain access to personal nonpublic information without proper authority to do so. This may entail requesting private information while impersonating the account holder, by phone, by mail, by email, or even by "phishing" (i.e., using a "phony" website or email to collect data). The GLBA encourages the organizations covered by the GLBA to implement safeguards against pretexting.



GRAMM-LEACH-BLILEY ACT & FFIEC REGULATORY COMPLIANCE

GLBA/FFIEC COMPLIANT SERVICES

According to the FFIEC Handbook, Financial institutions should secure access to their computer networks through multiple layers of access controls to protect against unauthorized access to critical systems and data. Perimeter offers a number of services to help you organization remain compliant with GLBA and FFIEC regulations while providing the only online portal that unifies all of your security services on one complete, easy to use platform.

As the trusted market leader of information security services, Perimeter E-Security undergoes continuous third-party assessments including those performed by the FFIEC member agencies and annual SAS 70 Type II audits

Regulation Action Summary	Services
Financial institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls	<ul style="list-style-type: none"> Internal and External Vulnerability Scanning
Financial institutions should secure access to their computer networks through multiple layers of access controls to protect against unauthorized access	<ul style="list-style-type: none"> Managed Firewall
Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by monitoring network and host activity to identify policy violations, anomalous behavior, unauthorized configurations, and analyze the results of monitoring to respond appropriately	<ul style="list-style-type: none"> Intrusion Detection & Prevention Host Intrusion Prevention (HIPS)
Financial institutions should secure remote access to and from their systems implementing robust controls over configurations at both ends of the remote connection to prevent potential malicious use	<ul style="list-style-type: none"> VPN Remote User Access
Financial institutions should protect against attempts to gain access to personal nonpublic information without proper authority to do so	<ul style="list-style-type: none"> Social Engineering Engagement
Financial institutions should protect against the risk of malicious code by implementing appropriate controls to prevent and detect malicious code, as well as engage in appropriate user education	<ul style="list-style-type: none"> Spam Filtering Email Anti-Virus E-Security Awareness & Compliance Training
Employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit	<ul style="list-style-type: none"> MailSafe™ Email Encryption
Financial institutions should consider security needs for back-up sites and alternate communication networks	<ul style="list-style-type: none"> Email Archiving & Business Continuity
GLBA section 6801 requires that access to all customer records be carefully controlled to prevent substantial harm or inconvenience to any customer. Also any storage location that contains sensitive customer information must be protected by strong access control and secure passwords.	<ul style="list-style-type: none"> Email Compliance Manager Email Hosting
Financial institutions should control and protect access to paper, film and computer-based media to avoid loss or damage	<ul style="list-style-type: none"> Remote Data Backup

Call Us Toll Free: 800.234.2175