cpl.thalesgroup.com

THALES
Building a future we can all trust

Data Security Compliance with the Gramm-Leach-Bliley Act (GLBA)

How Thales solutions help with GLBA Compliance

What is GLBA?

The Gramm-Leach-Bliley Act (GLBA)--also known as the Financial Services Modernization Act of 1999--requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. The core aim is to prevent and mitigate cyber threats. The Federal Trade Commission (FTC) Safeguards Rule requires covered companies to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.

The GLBA is composed of three main rules regarding the privacy and protection of sensitive consumer data held by financial institutions:

- The **Financial Privacy Rule** covers collection and disclosure of most personal information (name, date of birth, SSN) and transactional data (card or bank account numbers) captured by financial institutions.
- The **Safeguards Rule** is designed to ensure the security of information gathered by financial institutions. It includes specific technical requirements for protecting sensitive data including encryption of data at rest or in transit as well as access management and authentication.
- The **Pretexting Rule** aims to prevent employees or business partners from collecting customer information under false pretenses, such as those employed in social engineering techniques.

Which companies are subject to GLBA?

The GLBA applies to a broad range of companies classified as financial institutions. The FTC explains that the GLBA applies to "all businesses, regardless of size, that are 'significantly engaged' in providing financial products or services." That includes not only companies providing financial products or services like loans, financial advice, or insurance, but also companies providing appraisals, brokerage, and loan servicing, check-cashing, payday loans, courier services, nonbank lending, and tax preparation services, among others.

When did the GLBA go into effect?

The Gramm-Leach-Bliley Act was enacted by congress in 1999 and is in full effect. Primarily, the FTC enforces the regulation, although other federal agencies, such as the Federal Reserve Board and the FDIC, and State governments are responsible for regulating insurance providers.

What are the penalties for GLBA non-compliance?

A financial institution found in violation of GLBA may face fines of $100,000 for each violation. Its officers and directors can be fined up to $10,000 for each violation and be imprisoned for five years or both.

How can Thales help with GLBA compliance?

Thales helps organizations comply with GLBA by addressing essential requirements for safeguarding customer information.

GLBA Part 314: Standards for Safeguarding Customer Information

The Safeguards Rule of the GLBA requires the development, implementation, and maintenance of an information security program with administrative, technical, and physical safeguards designed to protect customer information.

Thales helps organizations by:

- Identifying and classifying sensitive customer data for risk assessment
- Controlling and monitoring access to sensitive data
- Protecting data at rest and in motion
- Securing the development of apps
- Implementing multi-factor authentication
- Managing 3rd party risks

GLBA	Requirement	Thales Solutions
Part 314. b	**"risk assessment** that identifies... **risks to security of customer information"**	**CipherTrust Data Discovery and Classification** identifies structured and unstructured sensitive data on-premises and in the cloud. Built-in templates enable rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
Part 314. c.1.	**"Implement and periodically review access controls. Determine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it."**	**Thales OneWelcome** identity & access management products and solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensuring that the right user is granted access to the right resource at the right time; whereby minimizing the risk of unauthorized access. **SafeNet IDPrime** smart cards can be leveraged for implementing physical access to sensitive facilities. These smart cards can also augment Passwordless authentication initiatives relying on PKI and FIDO technology. **Thales OneWelcome Consent & Preference Management module** enables organizations to gather consent of end consumers such that financial institutions may have clear visibility of consented data, thereby allowing them to manage access to data that they are allowed to utilize. **CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. It provides complete separation of roles where only authorized users and processes can view unencrypted data.

GLBA	Requirement	Thales Solutions
Part 314. c. 3	**"Protect by encryption** all customer information held or transmitted by you **both in transit over external networks and at rest."**	**Protect Data at Rest:** **CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them: • **CipherTrust Transparent Encryption** delivers data-at-rest encryption with centralized key management and privileged user access control. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. • **CipherTrust Tokenization** permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data without exposing sensitive data during the analysis or in reports. • **CipherTrust Enterprise Key Management** streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases. Leveraging FIPS 140-2-compliant virtual or hardware appliances, our key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications. **Thales Luna HSMs** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Luna HSMs are available on-premises, in the cloud as-a-service, and across hybrid environments. • Generates and protects root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases • Signs application code to ensure software remains secure, unaltered, and authentic • Creates digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments **Protect Data in Motion:** **Thales High Speed Encryptors (HSE)** provide network-independent, data-in-motion encryption (layers 2, 3, and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our network encryption solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception— without performance compromise. Thales HSEs are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps. Rigorously tested and certified to exacting standards such as FIPS 140-2 L3 and Common Criteria, Thales HSE network encryption solutions have been vetted by such organizations as the USA Department of Defense Information Network (DoDIN) and NATO.
Part 314. c, 4	**"Adopt secure development practices for in-house developed applications"**	**CipherTrust Platform Community Edition** makes it easy for DevSecOps to deploy data protection controls in hybrid and multi-cloud applications. The solution includes licenses for CipherTrust Manager Community Edition, Data Protection Gateway, and CipherTrust Transparent Encryption for Kubernetes. **CipherTrust Secrets Management** is a state-of-the-art secrets management solution, which protects and automates access to secrets across DevOps tools and cloud workloads including secrets, credentials, certificates, API keys, and tokens.
Part 314. c, 5	**"Implement multi-factor authentication…"**	**SafeNet Trusted Access** provides commercial, off-the-shelf **multi-factor authentication** with the broadest range of hardware and software authentication methods and form factors. This allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally-managed policies— all managed from one authentication back end delivered in the cloud or on-premises.

GLBA	Requirement	Thales Solutions
Part 314. c, 8	**"Maintain a log of authorized users' activity and keep an eye out for unauthorized access."**	The **Thales Data Security** Solutions all maintain extensive access logs and prevent unauthorized access. In particular, **CipherTrust Transparent Encryption** security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and external SIEM systems. **SafeNet Trusted Access** allows organizations to respond and mitigate the risk of data breach by providing an immediate, up to date audit trail of all access events to all systems. Extensive automated reports document all aspects of access enforcement and authentication. In addition, the service automatically streams logs to external SIEM systems.
Part 314. f, 2	**"Oversee service providers,** by: Requiring your service providers by contract to implement and maintain such safeguards..."	**CipherTrust Cloud Key Manager** can reduce third party risks by maintaining on-premises under the full control of the financial institution the keys that protect sensitive data hosted by third party cloud providers. This increases operational efficiency through harmonization and automation. **CipherTrust Transparent Encryption** provides complete separation of administrative roles, so only authorized users and processes can view unencrypted data. Unless a valid reason to access the data is provided, sensitive data stored in a third-party cloud provider will not be accessible in cleartext to unauthorized users. These could include third party cloud provider employees, such as support engineers, DB admins, or potentially malicious processes. **Thales Data Security solutions** offer the most comprehensive range of data protection, such as **Thales Data Protection on Demand** (DPoD) that provides built in high availability and backup to its cloud-based **Luna Cloud HSM** and CipherTrust Key Management.