

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 Thales Helps with GLBA Compliance

Thales' solutions can help Financial Institutions comply with GLBA by simplifying compliance and automating security, reducing the burden on security and compliance teams. We help address essential requirements for safeguarding customer information under GLBA Part 314, which prescribes the development, implementation, and maintenance of an information security program with administrative, technical, and physical safeguards designed to protect customer information.

We provide comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, a secure Content Delivery Network (CDN), and Runtime Application Self-Protection (RASP).

Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behavior and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

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
- Securing the disposal of customer information
- Managing 3rd party risks

GLBA	Thales Capabilities	Thales Solutions
Part 314. b “risk assessment that identifies... risks to security of customer information”	<ul style="list-style-type: none"> • Discover and classify potential risk for all public, private and shadow APIs. • Identify structured and unstructured sensitive data at risk across Hybrid IT. • Identify current state of compliance and documenting gaps. 	Application Security API Security Data Security Data Discovery & Classification Data Risk Analytics Vulnerability Management
Part 314. c.1. “Implement and periodically review access controls.”	<ul style="list-style-type: none"> • Limit access to systems and data based on roles and context with policies. • Apply contextual security measures based on risk scoring. • Centralize access policies and enforcement to multiple hybrid environments in a single pane of glass. 	Identity & Access Management Workforce Access Management Customer Identity & Access Management Data Security Transparent Encryption
Part 314. c.3. “Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest.”	<ul style="list-style-type: none"> • Encrypt data at rest on-premises, across clouds, and in big data or container environments. • Protect cryptographic keys in a FIPS 140-2 Level 3 environment. • Pseudonymize sensitive information in databases. • Protect data in motion with high-speed encryption. • Protect data in use by leveraging confidential computing. • Gain full sensitive data activity visibility, track who has access, audit what they are doing and document. • Security products designed for post-quantum upgrade to maintain crypto-agility. 	Data Security Transparent Encryption Tokenization Key & Secrets Management High Speed Encryption Hardware Security Modules Confidential Computing Data Governance Data Activity Monitoring

GLBA	Thales Capabilities	Thales Solutions
Part 314. c, 4 “Adopt secure development practices for in-house developed applications”	<ul style="list-style-type: none"> • Protect apps from runtime exploitation, while integrating with tools in the CI/CD pipeline. • Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind. • Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. • Deploy data protection controls in hybrid and multi-cloud applications to protect DevSecOps. • Protect and automate access to secrets across DevOps tools. • Easily access data security solutions through online marketplaces. 	Application Security Web Application Firewall DDoS Protection Bot Protection API Security Data Security Community Edition Secrets Management DPOD Marketplace
Part 314. c, 5 “Implement multi-factor authentication...”	<ul style="list-style-type: none"> • Enable multi-factor authentication (MFA) with the broadest range of hardware and software methods. • Build and deploy adaptive authentication policies based on the sensitivity of the data/application. • Protect against phishing and man-in-the-middle attacks. 	Identity & Access Management Multi-Factor Authentication Risk-Based Authentication PKI and FIDO Authenticators
Part 314 c, 6 “Secure disposal of customer information”	<ul style="list-style-type: none"> • Locate structured and unstructured regulated data across hybrid IT and prioritize remediation. • Remove keys from CipherTrust Manager can ensure secure deletion, digitally shredding all instances of the data. 	Data Security Data Discovery & Classification Encryption & Key Management
Part 314. c, 8 “Maintain a log of authorized users’ activity and keep an eye out for unauthorized access.”	<ul style="list-style-type: none"> • Data activity monitoring for structured and unstructured data across cloud and on-prem systems. • Produce audit trail and reports of all access events to all systems, stream logs to external SIEM systems. 	Data Security Database Activity Monitoring File Activity Monitoring Identity & Access Management Workforce Access Management
Part 314. f, 2 “Oversee service providers, by: Requiring your service providers by contract to implement and maintain such safeguards...”	<ul style="list-style-type: none"> • Reduce third party risk by maintaining on-premises control over encryption keys protecting data hosted by in the cloud. • Ensure complete separation of roles between cloud provider admins and your organization, restrict access to sensitive data. • Monitor and alert anomalies to detect and prevent unwanted activities from disrupting supply chain activities. • Enable relationship management with suppliers, partners or any third-party user; with clear delegation of access rights. • Minimize privileges by using relationship-based fine-grained authorization. 	Data Security Cloud Key Management Transparent Encryption Database Activity Monitoring File Activity Monitoring Discovery and Classification Identity & Access Management Workforce Access Management Third-party Access Control Delegated User Management Externalized Authorization