Delphix

SOLUTION BRIEF

Data Compliance for the Gramm-Leach-Bliley Act

Newly toughened GLBA requires businesses to protect consumers' information in development and testing environments

The Gramm-Leach-Bliley Act (GLBA) has become significantly stricter on data privacy while broadening the definition of financial services to include retail, insurance, and even universities that provide financial aid. The newly toughened GLBA calls for secure application development practices and protection of consumer data in development environments. It imposes massive fines on organizations if nonpublic personal data is exposed in addition to possible jail time for officers.

The FTC issued a December 9, 2022 deadline to comply with new data security practices outlined in the GLBA Safeguards Rule including:

- Securing software development practices
- Identifying and managing data based on risk
- Ensuring no personally identifiable information is exposed
- Establishing secure procedures for disposing of data

Delphix Continuous Compliance: Key Features

Automated discovery of PII and other sensitive data subject to GLBA

Irreversible masking ensures data cannot be restored to its original, sensitive data

Referential integrity of masked data across sources and clouds

What Is the Cost of Non-Compliance?

GLBA imposes fines, penalties, and possible prison time for privacy violations and holds organizations responsible for protecting US consumers' personal information used in software development and testing from unauthorized disclosure. Penalties for non-compliance include:

- Up to $100,000 fine for the organization per violation
- Up to $10,000 fine for officers and directors per violation
- License revocations and/or up to 5 years in prison

What Data Require Protection?

GLBA requires protection of nonpublic personal information such as:

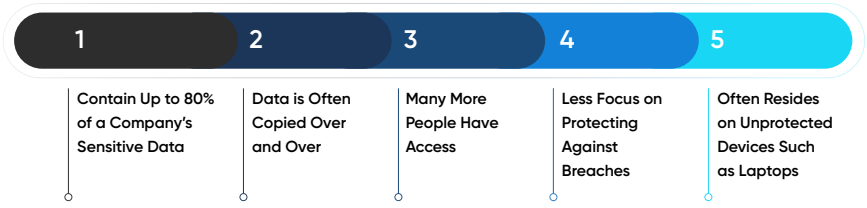
- Names, Social Security data, birthdates, addresses, biometric data
- Bank account and financial data, credit history
- Income, tax information
- Education and employment data

Information that does not identify a consumer is exempt from the GLBA Safeguards Rule. This includes aggregate information or data that does not contain personal identifiers such as account numbers, names, or addresses.

Non-Production Data Poses a High Risk

To comply with GLBA, businesses must take reasonable action to ensure that personal information will not be exposed if a systems breach occurs. Since non-production data stores used for DevOps TDM, reporting, and analytics contain up to 80% of an enterprise's personal data, these environments can represent the single largest source of GLBA risk.

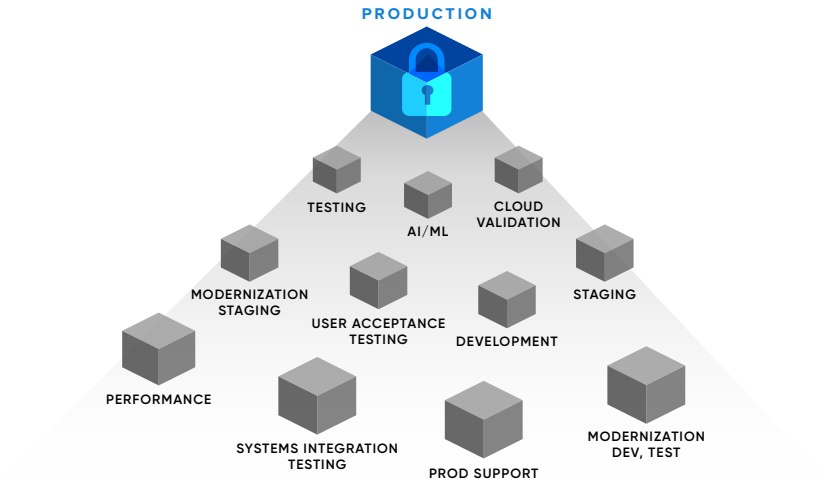
The only way to ensure this is to not have personally identifiable data contained in systems. Data that is irreversibly masked is not considered personal data.



Non-production data environments are 4-5 times larger than production and often less secure

How Delphix Enables GLBA Compliance

Delphix's Continuous Compliance solution automates compliance for application data, protecting consumers' information in the development and testing environments.



IT and security professionals are laser focused on protecting production environments, but often non-production data copies are unattended and persist in unsecure locations.

Data Discovery:

Identify and Assess GLBA Risk

Delphix scans data sources—from mainframes to cloud databases to files—automatically identifying sensitive data values and fields. Businesses can then create enterprise-level GLBA masking policies that define what sensitive data should be protected, where, when, and how. Compliance teams deploy those policies to protect environments for development and testing, and use Delphix to audit/report the data controls.

Data Masking:

Anonymize Consumer Information

Delphix masking irreversibly transforms sensitive data values into realistic, yet fictitious values to eliminate GLBA risk in development environments. Masking is applied consistently across environments to preserve referential integrity, and masked data remains fully-functional for development. Preconfigured algorithms enable teams to easily protect information covered by GLBA without requiring specialized programming expertise.

How Delphix Meets GLBA Compliance Requirements

Businesses Must…	Delphix Solution
Adopt: "Secure development practices for in-house developed applications."	Mask consumer data in development environments that contain up to 90% of GLBA risk.
Report On: "Matters related to the information security program, addressing…risk assessment, risk management and control decision."	Log, audit, and report on deployment of sensitive data controls.
Protect PII: "About a consumer resulting from any transaction involving a financial product or service."	Automatically discover consumer data including names, email addresses, payment information, and SSNs.
Enable: "Secure disposal of customer information in any format."	Masked data in development environments are exempt from disposal requests.
Implement: "Safeguards to control the risks you identify through risk assessment."	Define and centrally deploy enterprise-level masking policies in accordance with GLBA.
Protect by Encryption: "All customer information held or transmitted by you both in transit over external networks and at rest."	Tokenize or irreversibly mask data to protect data at rest or data shared inside or outside the organization.

Source: Code of Regulations, FTC, PART 314 – Standards for Safeguarding Customer Information

Delphix Masking Received a Gartner Peer Insights Distinction

Delphix received 39 customer reviews for Masking on the Gartner Peer Insights website. Because of our high ratings, we received the Gartner Peer Insights Customers' Choice 2022 distinction.

Delphix

Delphix is the industry leader for DevOps test data management.

Businesses need to transform application delivery but struggle to balance speed with data security and compliance. Our DevOps Data Platform automates data security, while rapidly deploying test data to accelerate application releases. With Delphix, customers modernize applications, adopt multicloud, achieve CI/CD, and recover from downtime events such as ransomware up to 2x faster.

Leading companies, including Choice Hotels, Banco Carrefour, and Fannie Mae, use Delphix to accelerate digital transformation and enable zero trust data management. Visit us at www.delphix.com. Follow us on LinkedIn, Twitter, and Facebook.