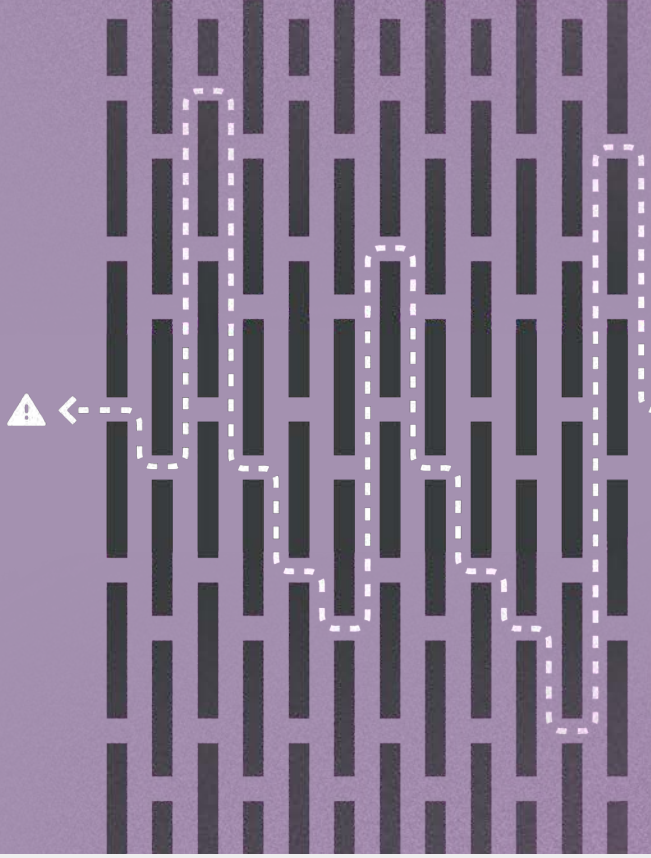
The Gramm-Leach-Bliley Act (GLBA), passed in 1999, sought to modernize and deregulate the financial industry, allowing institutions to offer a mix of banking, insurance, and investment services.

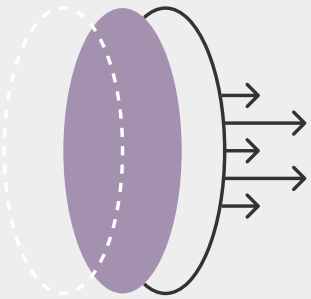


Born from a recognition of evolving financial markets and the limitations of the Glass-Steagall Act, GLBA was spearheaded by Senator Phil Gramm, Representative Jim Leach, and Representative Thomas Bliley.

The core aims of GLBA include protecting consumer financial information and giving consumers the ability to opt-out of personal data sharing between financial institutions and non-affiliated parties. While GLBA's passage enabled greater competition and service diversity in the financial sector, it has faced criticism. Some argue it played a role in the 2007-2008 financial crisis by contributing to the growth of large conglomerate banks. However, the act's privacy provisions have been generally well-received, emphasizing the importance of data security in financial transactions.

While GLBA doesn't directly mention email or specific platforms like Microsoft 365 or Google Workspace, its implications are clear: organizations must take the necessary precautions to protect, manage, and dispose of NPI wherever and however it's stored or transmitted.

GLBA Components Relevant to Email & Cloud Environments



Given the ubiquity and importance of email and cloud platforms in today's business operations, it's critical to consider them when developing and implementing GLBA-compliant strategies.

Mandate	Citation	Description	Implication	Material's Solution
Privacy Rule	15 U.S.C. § 6801 ↓ 15 U.S.C. 6809	Financial institutions must protect the privacy of consumer NPI and inform consumers about their privacy practices.	NPI must be accurately identified and any NPI stored or processed in cloud environments must be appropriately protected, both at-rest and in-transit.	Detect NPI and add an authentication layer to NPI in email to protect the data at rest.
Safeguards Rule	16 C.F.R. Part 314	Financial institutions must implement security practices to ensure the confidentiality and integrity of customer NPI.	Implement security features, including strong authentication and encryption, to protect NPI stored in cloud applications. Ensure the security of email communications and measures against phishing.	Ensure the security of email communications by securing NPI at the message-level with existing authentication workflows.
Pretexting Provisions	15 U.S.C. § 6821	Prohibits the use of false pretenses, fraudulent statements, or fraudulent means to obtain NPI.	Train staff to recognize and avoid pretexting attempts that may come via email.	Use a combination of pre-built and custom-built detections to identify pretexting attempts, instantly remediate attacks, and streamline triage workflows.
Data Retention and Disposal	General interpretation	GLBA implies NPI should be protected as long as it's retained and safely disposed of when no longer needed.	Emails containing NPI must be securely archived or deleted after they're no longer needed.	Create visibility into where NPI exists in mailboxes, the age, and trends. Securely archive it in a way that is easier than traditional methods and remove specific messages containing NPI based on rules that make sense for the risk profile.