



Could Your GLBA Compliance Be Simpler?

Digitech Systems Automation and Artificial Intelligence (AI) Technologies Make GLBA Compliance Easier.

The Gramm-Leach-Bliley Act (GLBA) of 1999 is a continuous obligation, not a one-time task. Financial institutions must safeguard personal information and enforce strict access controls. These obligations are reinforced by the 2023 Safeguards Rule, which modernizes GLBA to counter cyber threats and requires auditable, enterprise-wide practices that provide full visibility and enforceable control. Failure invites heavy fines and lasting reputational damage, but modern automation and AI technology helps.



How do Sys.tm® and the PaperVision® Product Suite Help Businesses Meet Compliance with GLBA?

- Identify and protect sensitive financial records
- Consistently apply compliant actions using automation
- Maintain audit-ready access controls and activity tracking
- Secure your data at every stage

Stay in Compliance While Minimizing Your Risk and Reducing Manual Effort:

Sys.tm and the PaperVision product suite combine AI and automation to reduce manual handling. They improve process consistency and help financial institutions maintain continuous GLBA compliance with less effort.



According to Security Scorecard research, GLBA compliance now requires “continuous monitoring, documented risk assessments, and enforceable controls across both internal systems and third-party vendors. With more than 1/3 of breaches involving third parties, reliance on manual compliance processes significantly increases regulatory and operational risk for financial institutions.”¹

— **Security Scorecard**

1: <https://securityscorecard.com/blog/what-does-the-gramm-leach-bliley-act-glba-require/>



Ensure Consistent GLBA Compliance with Less Effort

What if you could ensure that all of your critical data is always protected and managed in accordance with GLBA requirements? With Sys.tm and the PaperVision product suite, organizations can leverage AI to identify and classify sensitive information and use automation to apply security policies consistently across the enterprise.

Identify and Protect Sensitive Financial Records

Do you know where all your sensitive data is? Financial institutions risk regulatory violations if nonpublic personal information (NPI) is unclassified or unsecured. Sys.tm and PaperVision use AI to automatically identify, classify, and secure sensitive financial records, ensuring that critical information is protected.

Consistently Enforce Compliant Actions Using Automation

Are your workers following compliant processes every time? Whether intentional or accidental, manual processes increase your exposure to errors and GLBA violations. Sys.tm® Flows automates process flow from step-to-step, while the Robotic Process Automation (RPA) in Sys.tm® Automations completes rules-based tasks with machine effort. Together they eliminate any opportunity for variance from compliant processes.

Maintain Audit-ready Access Controls and Activity Tracking

Can you quickly demonstrate compliance during an audit? GLBA regulators expect full visibility into who accessed NPI and when as well as insight into what they did with the information. Both PaperVision and Sys.tm automatically capture and log user activity, generating detailed audit trails that simplify reporting and prove compliance without manual effort.

Secure Your Data at Every Stage

Is your information safe from accidental disclosure? What about hackers? GLBA requires you to safeguard NPI against data loss or unauthorized access. In addition to standard protections like password protocols and hosting redundancies, Sys.tm and PaperVision offer multi-factor authentication, multi-level access controls, and encryption both at rest and in transit. You'll rest easy knowing your data is always protected in compliance with GLBA requirements.



“The rapid growth of digital data collection and sharing has made consumer privacy and security a top priority for both state and federal lawmakers. As privacy rules continue to expand, financial institutions face increasing challenges in making sure their security policies are followed and can be demonstrated to regulators.”²

— **Tim Storey, Chief Executive Officer,**
National Conference of State Legislatures

2: <https://www.ncsl.org/resources/details/ncsl-comments-to-the-house-financial-services-committee>