GLBA AND THE SAFEGUARDS RULE
Proposed Changes

WHY THIS MATTERS

The Federal Trade Commission (FTC) is proposing changes to the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule. If your institution is subject to this rule, the following is a summary of the proposed changes:

1.	Preserve the flexibility to respond to changing landscape of security threats and provide more detail to ensure that financial institutions develop information security programs that are appropriate, reasonable and protect customer information.
2.	Require financial institutions to develop incident response plans as part of their information security program.
3.	Expand the designated employee(s) who coordinates the information security program to include an affiliate or a service provided. This position is usually the chief information security officer (CISO).
4.	Require risk assessments to describe how institution will address risks, perform reevaluations, and engage in annual penetration testing.
5.	Provide explicit language to ensure access controls are in place to protect customer information.
6.	Require documentation on data, personnel, devices, systems, and facilities related to the risk strategy of the financial institution.
7.	Restrict access to physical locations that contain customer information.
8.	Require financial institutions encrypt all customer information.
9.	Develop secure development practice for in-house applications that access or store customer information.
10.	Implement multi-factor authentication for individuals accessing customer information.
11.	Require information system to include audit trails designed to detect and respond to security events.
12.	Develop procedures for the secure disposal of customer information that is no longer necessary for their business operations.

13.	Adopt procedures for change management that govern the addition, removal or modification of elements of an information system.
14.	Require implementation of policies and procedures designed to monitor the activity of authorized users and detect unauthorized use.
15.	Require to implement various forms of training and education for information security program personnel.
16.	Require the financial institution's security coordinator or CISO to provide annual written reports to the financial institution's board of directors.
17.	Exceptions to the Safeguards Rule for financial institutions that maintain information for fewer than five thousand customers.

Source: Federal Trade Commission. *Safeguards Rule*. FTC.gov. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule

HOW WE CAN HELP

BerryDunn's higher education team understands cybersecurity and compliance challenges facing institutions today. With a thorough knowledge of common standards and frameworks – including GLBA, NIST, HIPAA, and GDPR – we deliver comprehensive and actionable plans to strengthen compliance, reduce risk, and improve security.

We have developed proven methodologies and best practices to help clients meet today's demands while planning for tomorrow's opportunities.