PROTECT:
Higher Education Services

amended FTC
Safeguards Rule &
Requirements

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

68 Main Street, Kennebunk, ME 04043 (207) 387 – 0396 www.Deer-Brook.com

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

Maine's Premier Veteran Owned & Staffed Cybersecurity Company

WHAT ARE THE NEW SAFEGUARDS RULE REQUIREMENTS?

The newly updated rule is significantly more prescriptive than the original 2002 Safeguards Rule. Under the newly revised Safeguards Rule, financial institutions must implement specific controls. Some of the more notable requirements include but are not limited to:

- Creating a ***written incident response plan*** (WISP) that includes internal processes and policy for responding to a security event.
- Developing ***data destruction procedures*** for customer information that has not been used for at least two years (unless that information is necessary for business operations).
- Adopting ***change control*** process and policy.
- ***Encrypting*** all customer information ***in transit and at rest*** and being able to verify this is in place.
- ***Continuously monitoring*** the efficacy of security safeguards or performing yearly periodic penetration testing and biannual vulnerability assessments with documented remediation plans and processes.
- Enabling ***multi-factor authentication*** for any person accessing an information system containing consumer ***financial*** information.
- Process in place to select and audit external service providers who maintain appropriate safeguards for customer information, including contractually requiring service providers to implement security safeguards
- Financial institutions must also designate ***a single qualified individual*** who is responsible for implementing and enforcing the organization's information security program. The new rule does clarify that the qualified individual who is responsible for the information security program may be an employee or a contracted service provider. The qualified individual must report in writing at least annually to the organization's board or governing body about the overall status and efficacy of the organization's information security program.
- Conduct a ***risk assessment*** to identify risks to the security, confidentiality, and integrity of customer information and assess the efficacy of safeguards.
  - Risk assessments be written, Performed periodically, Contain criteria for the evaluation of identified security threats, Requires a description of how identified risks will be mitigated or accepted (i.e., a board of compliance or other authoritative body in the organization authorized by charter to accept organizational risk.

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

Maine's Premier Veteran Owned & Staffed Cybersecurity Company

AMENDED FTC SAFEGUARDS RULE

Federal Trade Commission (FTC) announced newly updated standards for safeguarding customer information ("Safeguards Rule") under the Gramm-Leach-Bliley Act (GLBA). The new rule amends the FTC's 2002 Safeguards Rule and applies to financial institutions under the scope of the FTC's regulatory authority.

When does the new Safeguards Rule go into effect?	*The new Safeguards Rule becomes effective within 30 days after publication in the Federal Register.* • Published on December 9, 2021 (so the effective date will be January 9, 2022). • However, some requirements will be delayed one year (to December 2022). • These include the requirements to appoint a qualified individual for an organization's information security program, develop a written incident response plan, complete written risk assessments, conduct continuous monitoring (or annual penetration testing and biannual vulnerability assessments), and periodic third-party service provider assessments.
Why does the new Safeguards Rule apply to colleges and Universities?	The Rule broadly defines a "financial institution" as any entity engaging in the financial activities listed under the 1956 Bank Holding Company Act. Since colleges and universities include "making, acquiring, brokering, or servicing loans" and "collection agency services." Since specified financial activities, such as making federal student financial assistance loans or undertaking collection activities from staff and students, FTC regulations consider them financial institutions for GLBA purposes.