CAPINTECH

Revisiting GLBA: Important Updates

By Allison Davis Ward, Partner

As we've previously noted, the Gramm-Leach-Bliley Act (GLBA) is not new. The Standards for Safeguarding Customer Information Rule (Rule) component of GLBA went into effect in 2003. Since then, the Federal Student Aid Office has released several notices related to compliance, and many organizations have been evaluated on various components of compliance through their Uniform Guidance audits. So, if your higher education institution receives federal funds, you likely are very aware of GLBA and your institution's requirement under the Safeguards Rule to protect your students' personally identifiable information (PII).

However, the Federal Trade Commission (FTC) has released an update to the Safeguards Rule effective January 2022, and it's important to understand what changed and how it may affect your institution's compliance.

Where Are We Now?

The Rule requires institutions to establish an information security program and supporting controls to protect customer information obtained in conjunction with providing financial services. For higher education institutions, this information is typically the PII collected when providing financial aid.

To achieve this, organizations must assess risks, implement controls to reduce those risks, and evaluate the effectiveness of those controls on an ongoing basis. Through oversight, monitoring, and regular updates, the program should effectively mitigate threats as those threats evolve.

Although awareness of GLBA has increased over the past several years, achieving compliance has been difficult for many institutions. GLBA, as it was originally written, is relatively vague. While this supports the idea that compliance is not "one size fits all," that vagueness can make implementing the Rule very difficult. Also, the expectations related to implementation often evolve with increased scrutiny from auditors, regulatory bodies, and other agencies.

The FTC released the update to the Safeguards Rule to address these issues. **While the updated Rule still allows you to implement recommendations in relation to your institution's size and complexity, it provides focus and clarification in many areas.**

You can read the full revision here. Let's look at the key updates relevant to higher education institutions so you can evaluate your institution's compliance with these changes.

Developing and Implementing Your Information Security Program

Under the original version of the Rule, the required information security program was based on an assessment of risks to PII, with safeguards designed to mitigate those risks. The risk assessment was to consider, at a minimum, risks related to:

- Employee training and management;
- Information systems, including network and software design and information processing, storage, transmission, and disposal; and
- The ability to prevent, detect, and respond to attacks, intrusions, or system failures

These expectations did not change. However, the Rule does provide more guidance related to these areas, as highlighted below.

Risk Assessment

As outlined in § 314.4(b) of the updated Rule, your institution's risk assessment should:

- Be formalized and documented
- Define how you evaluate and categorize risks and assess how sufficiently your existing controls mitigate these risks

While the updated Rule still allows you to implement recommendations in relation to your institution's size and complexity, it provides focus and clarification in many areas.

- Identify a plan for the implementation of additional mitigations or formal risk acceptance for any risks outside of management's risk appetite

In addition, because threats constantly evolve, controls that were once sufficient may no longer be adequate. Therefore, you should review and update your assessment periodically.

Implementation of Safeguards

The update also provides further stipulations in § 314.4(c) on the types of safeguards that should be implemented. Such controls should address:

- Authentication and access to reduce the risk of unauthorized access to PII
- Identification and management of data, personnel, devices, systems, and facilities
- Encryption of PII at rest or in transmission
- Secure development of applications used to transmit, access, or store PII
- Use of multi-factor authentication (MFA) when accessing information systems
- Retention policies to minimize the unnecessary retention of PII and procedures for its secure disposal
- Change management processes
- Monitoring and logging of activity and the ability to detect unauthorized access, use, or alteration of PII

Employee Training and Management

Under the original Rule, employee training and management, or lack thereof, was an area to consider during the risk assessment process. Weaknesses in this area can jeopardize many of the safeguards you implement.

Per section § 314.4(e) of the updated Rule, your institution should have policies and procedures to support your staff in implementing your risk mitigations and controls effectively. This can include areas such as:

- Providing security awareness training that addresses relevant risks
- Relying on qualified internal or outsourced information security staff
- Ensuring information security staff receive specialized updates, awareness, and training to support their ongoing knowledge related to evolving threats and controls

Service Provider Oversight

The Rule requires institutions to ensure that any third-party service providers that host or access the institution's PII can do so securely, and institutions are to hold these vendors accountable contractually. However, the updated Rule expands upon this in § 314.4(f) and adds the requirement for periodic assessment of these providers.

Organizations can outsource the hosting and management of key systems and applications, but the responsibility for oversight remains with the institution. Establishing a strong vendor management program is a key component of demonstrating this ongoing due diligence.

Incident Response

The Rule as previously written indicated that the risk assessment should consider the detection, prevention, and response capabilities related to various incidents. However, the updated Rule establishes a written requirement for an incident response plan, and § 314.4(h) outlines the following seven areas to incorporate into the documentation:

- Goals of the plan
- Internal processes for responding to a security event
- Designation of responsibilities and decision-making authority
- Communications and information-sharing with internal and external parties
- Requirements for addressing identified weaknesses in systems and controls
- Documentation and reporting of security events and any incident response measures taken
- Post-incident evaluation and plan revision following a security event

An incident response plan supports an organization in its response to and recovery from incidents that could impact the confidentiality, integrity, or availability of PII. Such planning can help organizations minimize the impact of malware, ransomware, phishing, targeted attacks, and insider and other threats and can support an efficient and effective response.

Increasing Accountability

Accountability for the information security program is a large component of the Rule, and accountability is established in several ways.

Program Coordination

Previously, the Rule allowed for the designation of one or multiple employees to coordinate the program. However, this has been amended with the updated Rule, which states in § 314.4(a) that a *single* individual (a "Qualified Individual") should be deemed responsible for the program.

Note that if your institution chooses to outsource this function to a service provider, you will be responsible for the ultimate oversight of the service provider performing this function and this oversight should be assigned to someone on your management team.

Monitoring for Effectiveness

In § 314.4(d), the updated Rule also provides guidance on ways institutions can evaluate and monitor their information security program for effectiveness. Where there previously was little guidance related to this monitoring, the updated Rule indicates that continuous monitoring or regular vulnerability assessments and penetration testing are needed.

Approval of Exceptions

There are a few instances where certain exceptions in controls may be allowed, but these decisions should not be made in a vacuum. When certain controls cannot be met, those deviations should be documented and approved by the Qualified Individual. For example, in the event encryption is not feasible or MFA is not utilized, the Qualified Individual should review alternate compensating controls and provide written approval for the exception.

We also recommend incorporating these exceptions into your written risk assessment so they can be reevaluated periodically.

Annual Status Report

There is a new annual reporting requirement related to the effectiveness of the program, as noted in § 314.4(i). The Qualified Individual is to provide a written report at least annually to the Board of Directors or equivalent governing body. If these groups do not exist, the senior officer responsible for the program should receive the report.

The report should discuss the overall status of the information security program and its effectiveness in achieving compliance with the Rule. It should address areas such as:

- Risk assessment
- Risk management and control decisions
- Service provider arrangements
- Testing results
- Security events or violations and the response taken
- Any recommendations for changes to the program

Exceptions

Institutions that maintain customer information for fewer than 5,000 individuals are exempted from the following sections of the Safeguards Rule:

- § 314.4(b)(1) – requirement for a written risk assessment
- § 314.4(d)(2) – requirements related to continuous monitoring, vulnerability assessments, and penetration testing
- § 314.4(h) – requirement for a written incident response plan
- § 314.4(i) – requirement for an annual written status report from the Qualified Individual

During the comment period for this guidance, there were questions about how the number of individuals should be determined. Based on the FTC's response to the comments and the adoption of the final Rule, this number appears to include PII maintained for current students in addition to data on former students that is retained. Until that data is purged, your institution has a responsibility to protect it.

For more clarification, refer to Proposed § 314.6: Exceptions in the description of the updates.

Effective Date

Although the updated Rule is effective as of January 2022, there are several areas where institutions have additional time to achieve full compliance. Note that while the original due date for these areas was December 9, 2022, on November 15, 2022, the FTC extended the due date by six months, to June 9, 2023.

The June 9, 2023, due date applies to these areas of the updated Rule:

- § 314.4(a) – designation of a single Qualified Individual
- § 314.4(b)(1) – documentation of the risk assessment
- § 314.4(c)(1-8) – design and implementation of required safeguards
- § 314.4(d)(2) – establishment of continuous monitoring, vulnerability assessments, and/or penetration testing
- § 314.4(e) – implementation of policies and procedures that support training, awareness, and skills

The updated Rule indicates that continuous monitoring or regular vulnerability assessments and penetration testing are needed.

- § 314.4(f)(3) – creation of procedures to periodically assess service providers
- § 314.4(h) – documentation of a formal incident response plan
- § 314.4(i) – presentation of the annual status report on the effectiveness of the program

It is important to understand these updated requirements and ensure your institution achieves and maintains compliance. Please contact us with questions or to learn how we can assist you with GLBA compliance, including components such as vulnerability assessments and penetration testing.

This article has been updated.

Additional Resources:

CapinTech Cyber Series Webcast: Vulnerability Management

CapinTech Cyber Series Webcast: The Criticality of Vendor Management and Due Diligence

How Weak IT Controls Can Affect Your Financial Statement Audit E-book

About the Author

Allison Davis Ward, Partner
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.