THOMPSON COBURN LLP

A Guide to Understanding GLBA Requirements for Institutions of Higher Education

What is the Gramm-Leach-Bliley Act (GLBA)?

GLBA, 15 U.S.C. §§ 6801-6809, is the commonly used name for the Financial Services Modernization Act of 1999. The law overhauled many aspects of financial services regulation, including adding privacy and security requirements for nonpublic personal information (NPI).

What does GLBA require?

GLBA contains requirements relating to privacy (the collection, sharing and use of NPI) and security (how NPI must be protected). The statute provides the broad outlines of what must be done on privacy and security by a Financial Institution (FI), but much of the detail is left to rulemaking.

What entities are subject to GLBA?

GLBA applies to financial institutions (FIs), a designation essentially defined as an entity significantly engaged in activities deemed financial in nature by the Federal Reserve Board. To be a FI, the entity must engage in the financial activities in a way that is a regular part of its business or at least more than incidental.

Why are higher education institutions subject to GLBA?

Higher education institutions are subject to GLBA based on their receipt of federal financial aid under Title IV of the Higher Education Act (Title IV Institutions). In issuing its GLBA Privacy Rule in 2000, the Federal Trade Commission (FTC) stated "[t]he Commission disagrees with those commenters who suggested that colleges and universities are not financial institutions. Many, if not all, such institutions appear to be significantly engaged in lending funds to consumers." 65 Fed. Reg. 33,646, 33,648 (May 24, 2000).

What are the GLBA privacy rules for higher education?

Title IV Institutions comply with GLBA privacy rules by complying with FERPA. In 2011, the Consumer Finance Protection Bureau (CFPB) issued the agency's GLBA privacy rule (Regulation P) in which the agency stated that an "institution of higher education that complies with the Federal Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution described in §1016.3(l)(3) of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA." 12 C.F.R. § 1016.1(b)(2)(ii).

What are the GLBA security rules for higher education?

Unlike with the privacy requirements of GLBA, USED and the FTC have indicated that Title IV Institutions must comply with the security provisions of the FTC's GLBA Safeguards Rule, 16 C.F.R. Part 314. The FTC issued an original iteration of the Safeguards Rule in 2002. In 2021, the FTC released a substantially revised version of the Safeguards Rule that included several specific requirements for cybersecurity controls (See our blogpost for additional information). Most of the additional and more prescriptive cybersecurity requirements were to be effective in December 2022, but the FTC delayed effectiveness until June 9, 2023.

The revised version of the Safeguards Rule requires a FI to have an information security program (ISP) that includes the following elements:

- Designating a "Qualified Individual" to oversee and implement the ISP
- Performing a written risk assessment of security risks and threats and implementing how identified risks will be controlled or accepted
- Implementing security controls including:
    - Access controls and user limits on accessible data
    - Management of data, users and systems consistent with risk strategy
    - Encryption of customer information in transit over external networks and at rest
    - Secure development practices for in-house developed software and applications that access or transmit customer information
    - Implementation of multifactor authentication or reasonably equivalent access controls
    - Procedures for the periodic and secure disposal of customer information and review of data retention policies
    - Procedures for secure change management of systems
    - Controls to monitor and log activities of users and detect unauthorized access
- Performing annual penetration tests and twice annual vulnerability assessments of information systems
- Providing security awareness training and qualifications requirements for information security personnel
- Providing security awareness training for all personnel to address identified risks
- Performing risk assessments of service providers
- Establishing a written incident response plan to address security incidents
- Written reporting, at least annual, by the Qualified Individual to the board of directors or equivalent governing body

What is USED's role under GLBA?

USED is not given a specific regulatory or enforcement role by GLBA. However, USED has general regulatory and enforcement authority over Title IV Institutions. In particular, under the Standards of Administrative Capability regulations at 34 C.F.R. 668.16(c), an institution is required to have an adequate system of internal controls that provides reasonable assurance that the institution will achieve its objectives regarding reporting, operations, and compliance. USED has stated that an institution that does not provide for the security of the information it needs to continue its operations would not be considered administratively capable.

What has the Department of Education said about GLBA?

USED requires institutions participating in Title IV programs to enter into a Program Participation Agreement (PPA) outlining terms and conditions of participation, including compliance with the GLBA Safeguards Rule.

USED also requires, through the Student Aid Internet Gateway (SAIG) Enrollment Agreement, that all institutions and servicers protect applicant information and comply with requirements for the protection of information received from USED systems.

USED has noted the requirement to comply with the safeguarding requirements of GLBA in Dear Colleague Letters GEN-15-18 and GEN-16-12 and in Dear CPA Letter CPA-19-01.

In December 2020, USED issued an Electronic Announcement recommending the utilization of National Institute of Standards and Technology Special Publication 800-171 (NIST 800-171) as a tool for securing sensitive information and to comply with GLBA safeguarding requirements.

In February 2023, USED issued Electronic Announcement General-23-09, Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements (2023 Electronic Announcement). The 2023 Announcement summarizes past USED GLBA issuances, outlines the changes to the FTC Safeguards Rule to be effective in June 2023, and describes possible enforcement mechanisms for alleged violations of GLBA or the FTC Safeguards Rule.

How are GLBA and its rules enforced?

As stated in the 2023 Electronic Announcement, USED will be enforcing the legal requirements of GLBA through annual compliance audits. As first explained in GEN-16-12: "... the Department is beginning the process of incorporating the GLBA security controls into the Annual Audit Guide in order to assess and confirm institutions' compliance with the GLBA. The Department will require the examination of evidence of GLBA compliance as part of institutions' annual student aid compliance audit."

In addition, for most FIs, privacy requirements of GLBA are enforced by the CFPB with concurrent authority resting with the FTC. However, as noted above, the CFPB and FTC have stated that for institutions of higher education, compliance with the privacy requirements of FERPA will be deemed compliance with the GLBA privacy requirements.

Security requirements of GLBA for higher education institutions will be enforced by the FTC.

Are there benefits to being subject to GLBA?

Certain federal and state privacy and cybersecurity requirements exclude from their scope, in whole or in part, entities and/or data that is subject to GLBA. Notable exclusions include:

- The Illinois Biometric Information Privacy Act (BIPA)
- The Texas Capture or Use of Biometric Identifier Law (CUBI)
- The Washington Biometric Privacy Protection Act (WBPPA)
- The California Consumer Privacy Act/Privacy Rights Act (CCPA/CPRA)
- The Colorado Privacy Rights Act (CPA)
- Certain state security breach notice laws, if requisites are met

Thompson Coburn's Higher Education Practice

Thompson Coburn's higher education practice features a core group of attorneys with extensive experience managing regulatory, policy, transactional, and lobbying matters for postsecondary institutions. These industry attorneys work in concert with other members of the firm to regularly provide postsecondary clients insightful, creative, and efficient legal counsel across a broad range of matters. Our attorneys offer general counsel, compliance, and training services to small and mid-size colleges and universities, while providing specialized services to large institutions with in-house counsel. Our knowledge and experience informs our representation, and makes it both stronger and more efficient.

Inquiries and Disclaimer

Institutions with questions regarding the reporting requirements set out above are welcome to contact **James Shreve** at **312 580 5087** or jshreve@thompsoncoburn.com. Jim serves as a trusted advisor to clients facing complex cybersecurity and privacy issues — particularly those in the country's most highly regulated industries, such as higher education. He is the chair of Thompson Coburn's Cybersecurity group, was named a Fellow of Information Privacy and holds CIPP/US and CIPT certifications from the International Association of Privacy Professionals. Jim advises all types of companies on the myriad legal concerns surrounding confidential information and how such information is stored and transmitted. Applying the law to rapidly changing technology and software capabilities, Jim provides clients with a profile of their potential risk, then works closely with executive leadership, legal, IT and compliance information security teams to develop a comprehensive and practical plan for risk avoidance and responding to cyber and data-related issues.

CHICAGO
55 East Monroe Street
37th Floor
Chicago, IL 60603
312 346 7500

DALLAS
2100 Ross Avenue
Suite 3200
Dallas, TX 75201
972 629 7100

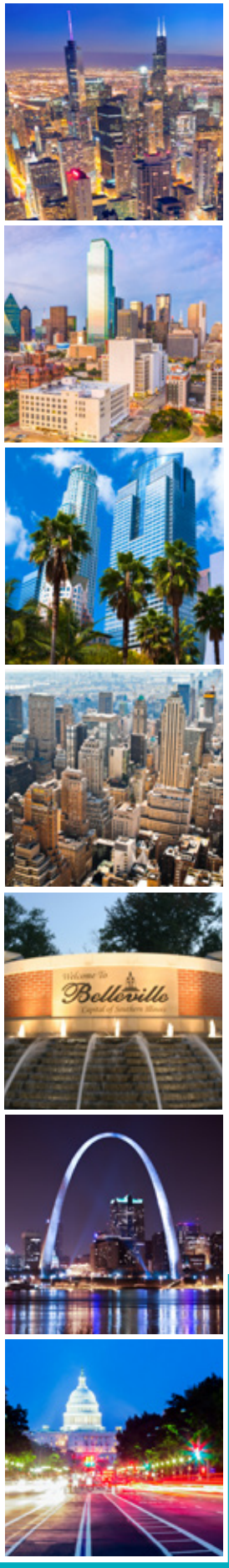
LOS ANGELES
10100 Santa Monica Boulevard
Suite 500
Los Angeles, CA 90067
310 282 2500

NEW YORK
488 Madison Avenue
New York, NY 10022
212 478 7200

SOUTHERN ILLINOIS
525 West Main Street
Suite 300
Belleville, IL 62220
618 277 4700

ST. LOUIS
One US Bank Plaza
St. Louis, MO 63101
314 552 6000

WASHINGTON, D.C.
1909 K Street, N.W.
Suite 600
Washington, D.C. 20006
202 585 6900



THOMPSON COBURN LLP

thompsoncoburn.com

March 2023