LEGAL UPDATES

PUBLISHED: FEBRUARY 27, 2023

ED Clarifies College/University Gramm-Leach-Bliley Act Compliance

Services

Data Privacy & Cybersecurity

Higher Education

Industry

Education

Professionals

SEAN TASSI
KANSAS CITY:
816.983.8330
SEAN.TASSI@HUSCHBLACKWELL.COM

ANNE D. CARTWRIGHT
KANSAS CITY:
816.983.8000
ANNE.CARTWRIGHT@HUSCHBLACKWELL.COM

In addition to new guidance on third-party servicers, the U.S. Department of Education clarified its expectations for higher education institutions' compliance with the Gramm-Leach-Bliley Act (GLBA) Cybersecurity Requirements earlier in the month.

The Department has been reminding colleges and universities of their GLBA safeguarding responsibilities through a series of Dear Colleague Letters since 2015. In early 2020, the Department issued an Electronic Announcement informing institutions that it intended to enforce the safeguarding responsibilities under the Department's Standards of Administrative Capability. Many colleges and universities have been struggling with the practical implications of their GLBA responsibilities, particularly as it relates to the categories of data subject to GLBA. The new guidance clarifies several aspects of GLBA compliance.

Most importantly, the Department clarified the terms "customer" and "customer information"— key words in defining the scope of GLBA compliance. In the college and university context, "customer information" means "information obtained as a result of providing financial services to a student (past or present)." This definition confirms what most institutions had already deduced from the previous guidance—GLBA compliance is primarily limited to student financial aid information, assuming that the institution properly restricts how such data is utilized on campus, and student business account information.

Under the GLBA Safeguarding Rules, colleges and universities (and their third-party servicers) are required to develop, implement, and maintain a written, comprehensive information security program. The Department identified nine elements that must be addressed in an institution's or servicer's information security program:

Element 1: Designates a qualified individual responsible for overseeing and implementing the institution's or servicer's information security program and enforcing the information security program (16 C.F.R. 314.4(a))

Element 2: Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (as the term customer information applies to the institution or servicer) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks (16 C.F.R. § 314.4(b))

Element 3: Provides for the design and implementation of safeguards to control the risks the institution or servicer identifies through its risk assessment (16 C.F.R. 314.4(c)). At a minimum, the written information security program must address the implementation of the minimum safeguards identified in 16 C.F.R. 314.4(c)(1) through (8)

Element 4: Provides for the institution or servicer to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 C.F.R. 314.4(d))

Element 5: Provides for the implementation of policies and procedures to ensure that personnel are able to enact the information security program (16 C.F.R. 314.4(e))

Element 6: Addresses how the institution or servicer will oversee its information system service providers (16 C.F.R. 314.4(f))

Element 7: Provides for the evaluation and adjustment of its information security program in light of the results of the required testing and monitoring; any material changes to its operations or business arrangements; the results of the required risk assessments; or any other circumstances that it knows or has reason to know may have a material impact the information security program (16 C.F.R. 314.4(g))

Element 8: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the establishment of an incident response plan (16 C.F.R. 314.4(h))

Element 9: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the requirement for its Qualified Individual to report regularly and at least annually to those with control over the institution on the institution's information security program (16 C.F.R. 314.4(i))

The Federal Trade Commission issued guidance in April of 2022 providing more detailed information on each of these elements.

The Department confirmed that the new Safeguard Rules are effective June 9, 2023, and that any findings related to non-compliance will be resolved as part of the Department's final determination of an institution's administrative capabilities. The Department also stated that it would be issuing additional guidance on NIST 800-171 Standards in a future Electronic Announcement.

What this means to you

The Department's new guidance provides an opportunity for institutions to consider reviewing their information security practices to ensure alignment with the elements above, including embedded FTC guidance. While institutions evaluate their third-party servicer relationships in the wake of evolving guidance, institutions should consider Department guidance regarding responsibility for confirming that servicers have appropriate systems in place as well.

Contact us

For assistance with GLBA compliance or other matters related to data privacy or information security, please contact Sean Tassi, Anne Cartwright, or you Husch Blackwell attorney.