Barley Snyder

New Cyber Rule Places Additional Requirements on Colleges and Universities (and Other Types of Organizations)

PUBLISHED ON
August 3, 2023

It has been a busy summer for cyber and privacy legal matters. We recently alerted you regarding SEC cyber breach reporting requirements. Earlier this summer, on June 9, 2023, the Federal Trade Commission (FTC) updated its enacting regulations to the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule. Previously, with no FTC-enacting regulations, the Safeguards Rule, a set of privacy and security requirements, only applied to banks, credit unions, and other financial organizations that are regulated by the traditional financial regulators - e.g., Federal Reserve, National Credit Union Administration, Office of the Comptroller of the Currency, the U.S. Securities and Exchange Commission and the Federal Deposit Insurance Corporation. However, the updated FTC-enacting regulations now place the requirements of the Safeguards Rule on a broader range of organizations, which now include most colleges and universities, along with automotive dealerships that facilitate consumer financing, real estate brokers, and other organizations not otherwise regulated by the traditional financial regulators but otherwise engaged in activity that is "financial in nature."

These new FTC-enacting regulations now require colleges and universities (and these other organizations) to develop, implement, and maintain an information security program to safeguard customer information. The program must include specific elements:

- Designate a qualified individual to oversee the information security program;
- Perform risk assessment regarding customer information;
- Design and implement safeguards and controls as identified by the risk assessment;
- Test and monitor the effectiveness of such safeguards and controls, including penetration attempts to access customer information;
- Provide information security training and updates for personnel;
- Oversee service providers that process customer information;
- Evaluate and adjust the information security program in response to the findings of any testing and monitoring;
- Establish a written information security incident response plan (if the organization maintains customer information on 5,000 or more consumers); and
- Report, in writing, at least annually to the board of directors (if the organization maintains customer information on 5,000 or more consumers).

The U.S. Department of Education (DOE) brought attention to the pending FTC-enacting regulations this past spring

when it indicated an intent to audit covered organizations, including colleges and universities, for compliance with the Safeguards Rule. The DOE will apply particular scrutiny (and heightened probability of sanction) on colleges and universities that have experienced a security breach.

All organizations now covered by the Safeguards Rule should commence their compliance efforts by mapping all data in the organization's control for the purpose of identifying any "customer information" and protecting it in accordance with the Safeguards Rule. Next steps should include developing and rolling out (or confirming the existence of) the specific elements required of an information security program under the Rule.

If you have any questions about the new FTC-enabled Safeguards Rule, including whether your organization must comply with the Rule, or if you need assistance developing an information security program compliant with the Rule, please reach out to Partner Donald Geiter or any member of the Barley Snyder Cybersecurity Service Team.

WRITTEN BY:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com