UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

DATE: October 30, 2019

CPA-19-01

SUBJECT: Amendment to September 2016 Audit Guide, *Guide for Audits of Proprietary Schools and For Compliance Attestation Engagements of Third-Party Servicers Administering Title IV Programs* – Student Information Security

Dear Certified Public Accountant:

This letter amends the September 2016 Audit Guide, *Guide for Audits of Proprietary Schools and For Compliance Attestation Engagements of Third-Party Servicers Administering Title IV Programs* (Audit Guide), by adding Section C.8.12 to Chapter 3 to determine whether Institutions of Higher Education have complied with the Federal Trade Commission's regulations for implementing the Gramm–Leach–Bliley Act in regards to ensuring the security and confidentiality of customer information.

The procedures described in this letter are mandatory for all proprietary school audits and third-party servicer compliance attestation engagements of fiscal years ending on or after December 31, 2019, that are conducted using the September 2016 Audit Guide.

Insert after Chapter 3, Section C.8.11

C.8.12. Student Information Security

Audit Objective:
Determine whether the institution designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 C.F.R. § 314.4(b) and documented safeguards for identified risks.

Background:
The Gramm-Leach-Bliley Act (Public Law 106-102) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data (16 C.F.R. Part 314). The Federal Trade Commission considers most institutions that participate in the Department of Education's student financial assistance programs as "financial institutions" and subject to the Gramm-Leach-Bliley Act (16 C.F.R. § 313.3(k)(2)(vi)). Under an institution's Program Participation Agreement with the Department of Education and the Gramm-Leach-Bliley Act, institutions must protect student information, with particular attention to information provided to institutions by the Department of Education or otherwise obtained in support of the administration of the Department of Education's student financial assistance programs (16 C.F.R. § 314.3; HEA 483(a)(3)(E) and HEA 485B(d)(2)). The Department of Education provides additional information about cybersecurity requirements at https://ifap.ed.gov/eannouncements/Cyber.html.

Criteria: Public Law 106-102
Sections 483(a)(3)(E) of the HEA (20 U.S.C. § 1090)
Sections 485B(d)(2) of the HEA (20 U.S.C. § 1092b)
16 C.F.R. Part 314

Guidance: FSA Handbook, Volume 2, Chapter 7, pages 2-201 through 2-203 (2018-2019 revision)
DCL GEN-15-18, Protecting Student Information, July 29, 2015 (GEN-15-18)
DCL GEN-16-12, Protecting Student Information, July 1, 2016 (GEN-16-12)
Federal Trade Commission's Financial Institutions and Customer Information: Complying with the Safeguards Rule

Required Procedures:

C.8.12.a. Verify that the institution has designated an individual to coordinate the information security program.

C.8.12.b. Verify that the institution has performed a risk assessment that addresses the three required areas noted in 16 CFR 314.4(b), which are (1) Employee training and management; (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

C.8.12.c. Verify that the institution has documented a safeguard for each risk identified from step b above.

Applicability for Third-Party Servicers

Institutions must take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information and require service providers by contract to implement and maintain such safeguards. Therefore, the Department of Education has determined that third-party servicers must also comply with the Federal Trade Commission's regulations for implementing the Gramm–Leach–Bliley Act. With the inclusion of the above procedures in Chapter 3, Section C.8.12, auditors of third-party servicers will be required to address these procedures as part of Chapter 4, Section C.10.b, which requires the servicer's auditor to perform procedures required by Chapter 3, Section C.8, as applicable.

Contact for Questions

Questions pertaining to this letter may be directed to the Office of Inspector General's Non-Federal Audit Team via email to OIGNon-FederalAudit@ed.gov.

Respectfully,

Bryon S. Gordon
Assistant Inspector General for Audit