*[Month/Day],* 2024

*[De-Identified – Name]*
President
*[De-Identified – University Name]*
*Subject: [De-Identified – Audit]*

Dear *[De-Identified - Name]*:

To better protect student data and your institution, the Federal Student Aid Enterprise Cybersecurity Group has reviewed your most-recent compliance audit of the *Title IV* programs and have identified *Gramm-Leach-Bliley Act* (GLBA) findings for *[De-Identified – University Name]*.

While the Federal Trade Commission is responsible for enforcing GLBA compliance, your auditor reported that your institution is not in compliance with the required elements of GLBA, which Federal Student Aid views as a potential risk to its systems and the students we serve. In accordance with your Program Participation Agreement with the Department of Education and the *Gramm-Leach-Bliley Act*, schools must protect student financial aid information, with particular attention to information provided to institutions by the Department or otherwise obtained in support of the administration of the federal student financial aid programs.

The *Gramm-Leach-Bliley Act* (GLBA) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. (16 CFR 314.4) The Federal Trade Commission considers *Title IV*-eligible institutions that participate in *Title IV* Educational Assistance Programs as “financial institutions” and subject to the GLBA.

The following requirements were deficient in your audit:

**Identification: 16 CFR 314.4(c)(2)**
Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy.

**Multi-factor Authentication: 16 CFR 314.4(c)(5)**
Implement multi-factor authentication for any individual accessing any information system unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls.

**Change Management: 16 CFR 314.4(c)(7)**
Adopt procedures for change management.

**Security Control Monitoring: 16 CFR 314.4(g)**
Evaluate and adjust your information security program considering the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this

section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

Please acknowledge your receipt of this correspondence within 10 days and include in your response the name of the individual responsible for your institution's information security program or point of contact.

FSA expects a written and acceptable CAP to be established within 30 days addressing the findings identified above.

If you have questions, please visit us at https://fsapartners.ed.gov.

For full GLBA requirements, please view the GLBA Safeguards Rule under 16 C.F.R. Part 314.4, visit Gramm-Leach-Bliley Act Cybersecurity Requirements, or contact us at FSA_IHECyberCompliance@ed.gov.

We look forward to working with you to address the findings and increase your institution's data security, including student information.

Sincerely,

Devin Bhatt

Devin Bhatt
Deputy, Chief Information Security Officer (CISO)
Federal Student Aid
U.S. Department of Education

Cc: Mrs Nancy Bessette, Zachary Saul