October 10, 2017

Dr. Laurel Jones, President
Cabrillo College
6500 Soquel Drive
Aptos, CA 95003-3194

UPS 2nd Day Delivery
Tracking #: 1Z A87 964 02 9259 1619

RE: Data Security Breach and Self-Report
of Data Breach Requirement– Before
Referral for Adverse Administrative Action
OPE ID Number: 00112400

Dear Dr. Jones:

CBS 5/46, KION-TV Central Coast reported that Cabrillo College (Cabrillo) suffered a breach of security caused by unauthorized access to its nonpublic personal customer information.

Requirements for Data Security

Cabrillo has significant obligations for protecting student financial aid data and Personally Identifiable Information (PII). Upon signing a Program Participation Agreement (PPA), Cabrillo agreed to comply with the Family Educational Rights and Privacy Act (FERPA), the U. S. Department of Education's (Department's) implementing regulations at 34 C.F.R. Part 99, and the Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, issued by the Federal Trade Commission (FTC), as required by the Gramm-Leach-Bliley (GLB) Act, P.L. 106-102. Thus, Cabrillo like all participating institutions, is responsible for complying with the limitations on the disclosure of PII in students' education records under FERPA and is subject to Sections 501 and 505(b)(2) of the GLB Act.

The GLB Act, also known as the Financial Services Modernization Act of 1999 (Pub. L. No. 106–102, 113 Stat. 1338), regulates the collection, disclosure, and protection of consumers' nonpublic personal information or personally identifiable information (PII) by financial institutions. Section 501 of GLB Act established the following information security standards for financial institutions:

> [E]ach agency or authority..., shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards –
>
> (1) to ensure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

The Federal Trade Commission (FTC) has defined financial institutions to include institutions of higher education (IHEs) on the basis of the financial relationships the IHEs have with students, donors, and others. For further information, please reference the FTC's guidance for Financial Institutions and Customer Information - Complying with the Safeguards Rule located at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

Consequently, IHEs are subject to the provisions of the GLB Act and must adopt an information security program, draft detailed policies for handling financial data covered by the law, and take steps to protect the data from unauthorized personnel. *See* Volume 2, Chapter 7 of the 2017-2018 Federal Student Aid Handbook, page 2-185.

The Safeguards Rule (16 CFR part 314 also referred to as the Standards for Safeguarding Customer Information) requires IHEs, as financial institutions, to develop, implement, and maintain a comprehensive information security program that includes reasonable measures to secure customer information and to regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures. The Safeguards Rule requires financial institutions to:

a. Designate an employee or employees to coordinate the institution's information security program.

b. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of the institution's operations, including:

(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. Design and implement information safeguards to control the risks the institution identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

d. Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring the institution's service providers by contract to implement and maintain such safeguards.

e. Evaluate and adjust the institution's information security program in light of the results of the testing and monitoring required by paragraph c above; any material changes to the institution's operations or business arrangements; or any other circumstances that

the institution's managers know or have reason to know that may have a material impact on the institution's information security program (16 CFR section 314.4).

The Safeguard Rule defines the following:

- An **information security program** is defined as the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
- **Customer information** is defined as any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.
- A **service provider** is defined as any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to the Safeguards Rule.

In the PPA signed by each IHE to participate in the Title IV federal student aid programs, the IHE agrees to comply with the FTC's regulations for implementing the GLB Act, 16 CFR part 314, Standards for Safeguarding Customer Information (also referred to as the Safeguards Rule). Since the GLB Act is intended to ensure the security and confidentiality of customer information, ED considers any breach of the security of student records and information as a demonstration of a potential lack of administrative capability as stated in 34 CFR section 668.16(c). ED has mandated that IHEs must notify ED of any known or suspected breaches (*see* Volume 2, Chapter 7 of the 2017-2018 Federal Student Aid Handbook, page 2-185) and strongly encouraged IHEs to inform their students, in compliance with applicable state regulation.

In addition, an institution that participates in any Title IV, Higher Education Act (HEA) program is subject to the requirements of the FTC Identity Theft Red Flags Rule (72 Fed. Reg. 63718) issued on November 9, 2007. The "Red Flags Rule" requires an institution to develop and implement a written Identify Theft Prevention Program to detect, prevent, and respond to patterns, practices, or specific activities that may indicate identity theft.

Moreover, the Student Aid Internet Gateway (SAIG) for Cabrillo requires that, as a condition of continued participation in the federal student aid programs, Cabrillo must report any suspected or actual data breaches to cpssaig@ed.gov. For the last several years, the Department has reminded all institutions of this requirement through numerous Dear Colleague letters, electronic announcements, and the annual FSA Handbook. Compliance with these reporting requirements is an important obligation for all institutions that participate in the federal student aid programs.

The Department's records indicate that Cabrillo did not self-report to the Department when it detected a suspected data breach on or about September 5, 2017. The window for submission of the self-report is now closed and Cabrillo did not report during the required period, on the day of the suspected data breach detection. The Department has the authority to fine institutions that do not comply with the requirement to self-report data breaches. Such fines may be imposed up to $54,789 per violation per 34 C.F.R. § 36.2.

Self-reporting is email enabled and there is no excuse for failing to report. The continued failure of Cabrillo to self-report breaches will be considered further evidence of a lack of administrative capability. If Cabrillo does not immediately self-report real or suspected data breaches on a timely basis, the Department will consider referring Cabrillo for appropriate administrative action, including a possible fine. Further, institutions that fail to comply with data security laws and regulations may be subject to losses, fines, and penalties (including criminal penalties) caused by the data breaches per 34 C.F.R. § 668.84.

In July 2015, the Department published a Dear Colleague Letter, GEN-15-18, which reminded institutions of their obligation to protect student information under these requirements. In addition, GEN-15-18 reminded institutions that the Student Aid Information Gateway Enrollment Agreement, entered into by each Title IV participating institution, includes a provision that the institution, "[m]ust ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel." In July 2016, the Department published another Dear Colleague Letter, GEN-16-12, as a follow up to GEN-15-18. In GEN-16-12, the Department advised institutions about the important cybersecurity protection information in the National Institute of Standards and Technology (NIST) Special Publication 800-171 (NIST SP 800-171) which identified recommended requirements for ensuring appropriate security of Controlled Unclassified Information (CUI) in the possession of institutions. *See* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf . The NIST SP 800-171 focuses on protecting the confidentiality of CUI in non-federal information systems and recommends security requirements to achieve that objective.

As a result of the reported breach by CBS 5/46, KION-TV Central Coast, please provide this office with the following information:

- Date the suspected breach occurred
- Description of the breach
- Current status of the breach incident and remediation efforts to date
- Copy of the institution's written information security program and point of contact details
- Copy of the institution's written Identity Theft Prevention Program

Please send your response within 30 days of your receipt of this letter by e-mail to Mr. Michael Holmes and Ms. Tiina K.O. Rodrigue at michael.holmes@ed.gov and tiina.rodrigue@ed.gov or by mail to:

Mr. Michael Holmes
U.S. Department of Education, Federal Student Aid
Technology Office
830 First St, NE – 10th Floor
Washington, DC 20202

If your response contains PII that information must be protected. PII is any information about a student which can be used to distinguish or trace the student's identity (some examples are name, social security number, date and place of birth).

PII being submitted electronically or on media (e.g., CD, disk, DVD) must be encrypted. The data must be submitted in a .zip file encrypted with Advanced Encryption Standard (AES) encryption (256-bit is preferred). The Department uses WinZip, however, files created with other encryption software are also acceptable, provided that they are compatible with WinZip and are encrypted with AES encryption.

The Department must receive an access password to view the encrypted information. The password must be e-mailed or otherwise communicated separately from the encrypted data. The password must be 12 characters in length and use three of the following: upper case letter, lower case letter, number, special character. A manifest must be included with the e-mail that lists the types of files being sent (a copy of the manifest must be retained by the sender).

Hard copy files and media containing PII must be:

- sent via a shipping method that can be tracked with signature required upon delivery
- double packaged in packaging that is approved by the shipping agent (FedEx, DHL, UPS, USPS)
- labeled with both the "To" and "From" addresses on both the inner and outer packages
- identified by a manifest included in the inner package that lists the types of files in the shipment (a copy of the manifest must be retained by the sender).

PII data cannot be sent via fax. If you have any questions, please contact Kevin Roberts, Institutional Review Specialist, at (415) 486-5573 or via email at Kevin.Roberts@ed.gov. Thank you for your prompt attention to this matter.

Sincerely,

Martina Fernandez-Rosario
Division Director
San Francisco/Seattle School Participation Division

cc: Ms. Tootie K. Tzimbal, Director of Financial Aid