(b)(6)

NOV 5 2009

Dear (b)(6)

The purpose of this letter is to notify you that this Office is not initiating an investigation in response to your correspondence of March 24, 2008. Your correspondence does not contain specific allegations of fact giving reasonable cause to believe that a violation of FERPA has occurred. In accordance with the FERPA regulations, this Office notifies a complainant if it does not initiate an investigation under FERPA. This Office administers the Family Educational Rights and Privacy Act (FERPA), which addresses issues that pertain to education records.

The University notified you in a January 7, 2008, letter that a computer file containing information from your education records had been "inadvertently placed on [the University's] Web server" and that it may have been possible for others to view the information. The University's letter informed you that the file had been removed from the Web server, was no longer accessible online, and that it was consulting with third party experts to improve the University's security procedures. The University's letter included an offer of free credit monitoring service from Experian for 12 months and advice on other steps you could take to minimize a risk of identity theft.

You still had concerns about the matter and contacted the University call center in January, when you spoke with a staff person and (b)(6) the call center manager. Following that conversation, on February 1 you wrote to the University president and chief information officer requesting further information about the incident, the University's response, and the University's computer and information management procedures. You had a telephone conference with the chief operating officer and the chief information officer of the University on February 21, and that was followed by a February 29 letter to you by the chief operating officer.

Your March 24 letter to this Office states that you continue to "have no trust that [your] information is secure." You feel the University employed insufficient security procedures, a "casual and incorrect notification [and] poor customer service" in its responses to you. You ask to be informed whether the FERPA regulations state "which (university/academic) personnel have the permission/need to access student's personal information;" and the location within FERPA where this information is located.

FERPA is a Federal law that gives students 18 years or older or who have attended a postsecondary institution the right to have access to their education records, the right to seek to have the records amended, and the right to have some control over the disclosure of information from the records. Education records are those records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution. Enclosed for your information is a guidance document for eligible students about FERPA.

Under FERPA, an eligible student must generally provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. Exceptions to the consent requirement are set forth at § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

FERPA specifically exempts from the prior written consent requirement those disclosures of education records that are made to other school officials, such as teachers, within the educational agency or institution whom the agency or institution has determined to have a legitimate educational interest. 34 CFR § 99.31(a)(1). Although "school official" is not defined in the statute or regulation, this Office has interpreted the term to include positions such as an institutional president, chancellor; trustee; instructor; registrar; counselor; admissions officer; attorney; information systems specialist; and support or administrative personnel. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility. Section 99.7(a)(3)(iii) of the FERPA regulations requires an educational agency or institution to include in its annual notification of rights under FERPA a statement indicating whether it has a policy of disclosing personally identifiable information under § 99.31(a)(1), and, if so, a specification of the criteria for determining which parties are school officials and what the agency or institution considers to be a legitimate educational interest.

The Final Regulations were published in the *Federal Register* on December 9, 2008 (73 FR 74806). On pages 74806 and 74843 the preamble to the FERPA Regulations explain the necessity for institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. The "Department's Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) were also published in the Final Regulations to provide institutions additional information and resources to assist them in meeting this responsibility. You can find a link to the Final Regulations on our website here: www.ed.gov/fpco.

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can guarantee to be safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. FERPA does not dictate specific requirements for safeguarding education records. An institution may use any reasonable method, combination of methods, or technologies reasonably calculated to protect such information.

The Safeguarding Recommendations specify a variety of steps to be taken when an institution that has experienced an information theft, hacking or other intrusion, equipment or program malfunction, inadvertent release of data to Internet sites, or other unauthorized release of education records. These steps include:

- Immediately retrieving the data to prevent further disclosures.
- Determine the circumstances that permitted the breach to occur
- Identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.

There is no specific requirement in FERPA to notify students that their education records may have been subject to an unauthorized release. Direct student notification may be advisable, though not required by FERPA, if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

The information you provided does not provide specific evidence that information from your education records was improperly disclosed. It appears your education records were part of the information concerned in the data breach, but there is no direct evidence that your information was improperly accessed or disclosed during the time of the breach. Additionally, you have provided evidence that the University has already completed a number of the suggested steps in the Safeguarding Recommendations. The University has also exceeded its requirements under FERPA by providing direct student notification and an offer of free credit monitoring services. Accordingly, there is no basis for this Office to initiate an investigation of your allegations.

I trust that the above information is helpful in explaining the scope and limitations of FERPA.

Sincerely,

Kathleen M. Wolan
Program Analyst
Family Policy Compliance Office