THE CHRONICLE OF
HIGHER EDUCATION

May 13, 2020

NOTICE OF DATA BREACH

Dear Account Holder:

The Chronicle of Higher Education, Inc. takes data security very seriously and we understand the importance of protecting the information we maintain. We are writing to inform you about an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

WHAT HAPPENED: On May 10, 2020, The Chronicle concluded our investigation and analysis of a data security incident that involved unauthorized access to one of our servers. The Chronicle learned about the incident after receiving an internal alert about suspicious activity on the server. Upon learning of this, The Chronicle took the server offline, a leading cyber security firm was engaged to assist with the investigation, and law enforcement was notified. Through our investigation, The Chronicle determined that unauthorized parties exploited a vulnerability in the server, through which they were able to obtain administrative account credentials for the server. The unauthorized parties then logged in to the server on February 17, 2020 and accessed a database on the server that contained credentials for online accounts to chronicle.com, philanthropy.com, and chroniclevitae.com.

WHAT INFORMATION WAS INVOLVED: Our investigation determined that the server accessed by the unauthorized parties contained a database with your username(s) and "hashed" and "salted" password(s) for your online account(s) to chronicle.com, philanthropy.com, and/or chroniclevitae.com. The password(s) for your account(s) were not in plain text, but had been altered through a cryptographic "hashing" and "salting" process, which rendered the actual password(s) indecipherable to third parties. Although access to the hashed and salted passwords would not allow access to your account(s), we are notifying you out of an abundance of caution because our investigation was unable to rule out the possibility that unauthorized parties could bypass the cryptographic "hashing" and "salting" process.

WHAT YOU CAN DO: The next time you login to your online account(s), you will be prompted to change your password(s). Also, if you use the same username(s) and password(s) for any other online account, we recommend that you change your password there as well.

WHAT WE ARE DOING: To date, we have no evidence that there has been any unauthorized access to your online account(s), however, out of an abundance of caution, we wanted to let you know this happened and assure you we take it very seriously. In addition to resetting the password(s) to your online accounts using stronger "hashing" and "salting" technology, we have taken steps to help prevent a similar incident from occurring in the future, including the replacement of the server with the unauthorized access, as well as additional procedures to further expand and strengthen security processes.

FOR MORE INFORMATION: We regret any inconvenience or concern this may cause you. If you have any questions, please contact 1-833-579-1097, Monday – Friday, 9:00 a.m. to 9:00 p.m., Eastern Daylight Time.

Sincerely,

Ken Sands

Ken Sands
General Manager, Online