

July 09, 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 information related to your online account(s) to chronicle.com, philanthropy.com, and/or chroniclevitae.com. This notice explains the incident, measures we have taken, and some steps you can take in response.

WHAT HAPPENED: On June 19, 2020, The Chronicle completed our investigation of reports we received that some of our data may have become accessible online. Through the investigation, we confirmed that unauthorized parties made data for some online accounts to chronicle.com, philanthropy.com, and chroniclevitae.com accessible online. Upon learning of this, The Chronicle launched an investigation with the assistance of a leading cybersecurity firm, and law enforcement was notified. Through the investigation, The Chronicle determined that unauthorized parties had exploited a vulnerability in one of The Chronicle's servers, through which they were able to obtain limited account information.

WHAT INFORMATION WAS INVOLVED: Our investigation determined that the account information posted online only contained your name, email address, username(s) , and password(s) for your online account(s) to chronicle.com, philanthropy.com, and/or chroniclevitae.com. Although The Chronicle "hashed" and "salted" passwords for online accounts in our database, meaning that a cryptographic process was used to render the actual passwords indecipherable to third parties and that they were not maintained in plain text, the unauthorized parties were able to bypass the cryptographic "hashing" and "salting" process, making the passwords for some online accounts accessible in plain text.

WHAT YOU CAN DO: The Chronicle reset passwords to all online accounts on June 16, 2020, so that the passwords for the accounts are no longer valid. If you have not logged in since that date, the next time you log in 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 all 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 call 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

*Prior to 2013, account holders created usernames for their online accounts that were different than their email addresses. For online accounts created after 2013, the usernames are the email addresses the account holders listed when they created their online accounts.

ADDITIONAL STEPS YOU CAN TAKE

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

New York Residents: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

The Chronicle of Higher Education
1255 23rd St. N.W., Suite 700
Washington, DC 20037
Chronicle.com