



Richard Goldberg, Esq.
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, Pennsylvania 19103
215.770.4261
rgoldberg@constangy.com

April 9, 2025

VIA ELECTRONIC SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509
Tel: 402-471-2683

Re: Notice of Data Security Incident

Dear Attorney General Mike Hilgers:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Hartwick College, located in New York, in connection with the recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Nebraska’s data breach notification statute.

1. Nature of the Security Incident

On March 13, 2025, the college learned that personal information was involved in an unauthorized access incident concerning their computer environment. The college discovered suspicious activity on October 26, 2024 when temporary disruption of their computer network occurred. The college promptly took steps to secure the environment and began an investigation to determine the nature and scope of the incident and whether personal information may have been accessed or acquired without authorization. After determining that personal information may have been involved, the college engaged a discovery vendor to perform a comprehensive review to identify what personal information was involved and to whose information may have been involved. On March 13, 2025, the college learned whose personal information may have been involved in the incident. Individuals were provided notification on April 8, 2025.

2. Number of Affected Residents & Information Involved

The incident involved personal information for approximately two (2) Nebraska resident(s). The information involved in the incident for the affected Nebraska resident(s) may have included their name as well as Social Security number.

3. Notification to Affected Individual(s)

On April 8, 2025, notification letters were sent to the affected Nebraska resident(s) by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers individuals the opportunity to enroll in twelve (12) months of complimentary identity protection services, including credit monitoring, and identity remediation services, as well as access to a call center, should any individual have questions about the incident. A sample notification letter sent to the individual(s) is included with this correspondence.

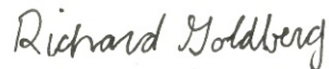
4. Steps Taken Relating to the Incident

The college is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above. The college has also established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, the college has also notified law enforcement, reviewed its cyber security, policies, and procedures.

5. Contact Information

The college has been and remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

A handwritten signature in cursive script that reads "Richard Goldberg".

Richard Goldberg

Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter



c/o IDX, P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

April 8, 2025

Re: Notice of Data <<Variable Text 1: Breach or Security Incident>>

Dear <<First Name>> <<Last Name>>:

We are writing to notify you of a data security incident which may have involved your personal information. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information, including enrolling in the complimentary identity protection services we are making available to you.

What Happened? On March 13, 2025, we learned that your personal information may have been involved in the data security incident. We discovered suspicious activity in our network on October 26, 2024 and promptly took steps to secure the environment. We also began an investigation to determine the nature and scope of the issue. We restored affected systems as quickly as possible and worked with independent experts to determine whether personal information may have been accessed or acquired without authorization during the incident. We then worked to discover whose information may have been involved in the incident. Although we have no evidence that anyone's information has been misused, we worked to notify people whose data may have been involved in the incident.

What Information was Involved? The information potentially involved in this incident includes your name as well as <<Variable Text 2: Data Elements>>.

What Are We Doing? As soon as we discovered the incident, we took the steps discussed above. In addition, we reported the matter to law enforcement and will cooperate in their efforts to investigate the matter. In order to reduce the likelihood of a similar incident occurring in the future, we also implemented additional measures to enhance the security of our network.

We are also providing you with identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. You have until July 8, 2025 to enroll in the services offered at no charge to you.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We also recommend that you review your financial account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the financial institution immediately. In addition, you can contact IDX representatives who will work on your behalf to help resolve issues you may experience as a result of this incident.

For More Information: If you have questions about this letter or need assistance, please do not hesitate to reach out to our designated call center at IDX at 1-800-939-4170, Monday through Friday from 9 am – 9 pm Eastern Time, excluding holidays and they will be happy to provide you with additional information.

We regret any concern or inconvenience this may cause you.

Sincerely,

Hartwick College

One Hartwick Drive
Oneonta, New York 13820
(607) 431-4877

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Request a Copy of Your Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <https://www.annualcreditreport.com>.

Put a Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC)

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

