



David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, New York 11201
dmcmillan@constangy.com
Direct: 718.614.8371

July 12, 2023

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents the Accreditation Commission for Education in Nursing, Inc. ("ACEN") in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On March 9, 2023, ACEN received an email from an unknown sender who claimed to have gained access to ACEN's computer network. In response, ACEN took immediate steps to secure its digital environment and engaged a leading cybersecurity firm to conduct an investigation to determine whether any sensitive information may have been accessed or acquired during the incident. Through the investigation, ACEN learned that its managed file transfer server may have been accessed without authorization. Following this confirmation, ACEN engaged a vendor to conduct a comprehensive review of the potentially affected data and on June 12, 2023, ACEN determined that personal information belonging to certain individuals may have been impacted in connection with this incident. ACEN then worked diligently to obtain contact information to effectuate notification to potentially affected individuals.

ACEN is notifying all potentially impacted individuals of this incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services. ACEN has no evidence of any misuse or attempted misuse of any personal information in conjunction with this incident.

2. Number of Maine residents affected.

ACEN notified two (2) Maine residents of this incident via first class U.S. mail on July 12, 2023. The information potentially impacted in connection with this incident includes name, and Social Security number. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as ACEN discovered this incident, ACEN took steps to secure its network environment and

July 12, 2023

Page 2

launched an investigation to determine what happened and the scope of personal information potentially impacted. In addition, ACEN implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future.

ACEN has 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. The call center is available at 1-888-220-5764 from 9:00 A.M. to 9:00 P.M. CEST on Monday through Friday (excluding holidays). In addition, while ACEN is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, ACEN is also providing complimentary credit and identity protection services to notified individuals.

4. Contact information.

ACEN 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 Constangy.

Best regards,

/s/ David McMillan

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter



Return to IDX:
4145 SW Watson Ave
Suite 400
Portland, OR 97005

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

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

July 12, 2023

Subject: Notice of Data <<Variable1 – Breach or Security Incident>>:

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

The Accreditation Commission for Education in Nursing, Inc. (“ACEN”) is writing to inform you of a data security incident that may have affected your personal information. ACEN is a non-profit organization that accredits nursing education programs throughout the United States. Please read this letter carefully as it contains important information about the incident and resources you can utilize to protect your information.

What Happened? On March 9, 2023, ACEN received an email from an unknown sender who claimed to have gained unauthorized access to ACEN’s computer network. After working with IT staff to ensure our network was secure, we engaged outside cybersecurity experts to conduct a forensic investigation into the legitimacy of these claims. That investigation concluded that an unknown actor gained unauthorized access to ACEN’s managed file transfer server and potentially acquired certain files between February 6 and February 27, 2023. ACEN reviewed the files in detail to determine whether any personal or other sensitive data was involved. That review concluded on June 12, 2023 and confirmed that your personal information may have been impacted, which is the reason for this notification.

What Information Was Involved? The information that may have been accessed or acquired during the incident includes your name, as well as your <<Variable2 – Data Elements>>. Please note that ACEN has no evidence of any actual or attempted misuse of this information.

What Are We Doing? As soon as we learned of the claims of unauthorized access, we worked with IT staff to ensure our environment was secure and implemented security measures to further protect our network going forward. We also enlisted external cybersecurity experts to conduct a forensic investigation. We have reported the incident to federal law enforcement and are cooperating in their investigation to hold the perpetrators accountable.

In addition, to alleviate any concerns you may have, we are offering you <<12/24>> of credit monitoring and identity theft protection at no cost through IDX – an expert in data breach and recovery services. These services include credit¹ and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With these services, IDX will help you resolve issues if your identity is compromised. To enroll, please visit <https://app.idx.us/account-creation/protect> or call 1-888-220-5764 and provide the enrollment code above. The enrollment deadline is October 12, 2023.

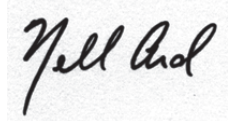
¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What Can You Do? ACEN encourages you to enroll in the IDX credit monitoring and identity protection services being offered to you. You may also review the guidance following this letter for additional steps you can take to protect your information.

For More Information: If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, please call IDX at 1-888-220-5764 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays).

We sincerely regret this incident and apologize for any worry or inconvenience that this may cause. ACEN takes this matter extremely seriously and has taken steps to ensure a similar incident does not happen again.

Sincerely,

A handwritten signature in black ink that reads "Nell Ard". The signature is written in a cursive style and is positioned above a light gray rectangular background.

Nell Ard, Interim CEO
Accreditation Commission for Education in Nursing, Inc.
3390 Peachtree Road NE, Suite 1400
Atlanta, GA 30326

Steps You Can Take to Protect Your Personal 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>.

