



Matthew Toldero, Partner
Cybersecurity & Data Privacy Team
One West 4th Street, Suite 850
Winston-Salem, NC 27101
mtoldero@constangy.com
Mobile: 336.448.8552

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

July 11, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Telephone: 410-576-6491
Email: Idtheft@oag.state.md.us

Re: Burrell College of Osteopathic Medicine - Notice of Data Event

Attorney General Anthony G. Brown:

We represent Burrell College of Osteopathic Medicine (“BCOM”), located at 3501 Arrowhead Dr, Las Cruces, New Mexico 88001, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately nine (9) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, BCOM does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

On January 26, 2024, BCOM became aware of suspicious activity involving its digital environment disrupting access to certain of its systems. In response, BCOM took immediate steps to secure its systems and promptly launched an investigation. In so doing, BCOM engaged digital forensics and incident response specialists to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On May 31, 2024, BCOM learned that personal information may have been impacted in connection with the incident and worked diligently to confirm contact information to begin mailing notice letters. BCOM then needed to complete an extensive review to confirm identities and collect addresses to begin notification efforts. That effort was completed on June 17, 2024.

The information that could have been subject to unauthorized access includes first and last name, as well as enrollment related medical information, and Social Security number/Individual Taxpayer Identification number.

2. Notice to Maryland Residents

On or about July 11, 2024, BCOM provided written notice of this incident to approximately nine (9) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

3. Other Steps Taken and To Be Taken

Upon discovering the event, BCOM moved quickly to investigate and respond to the incident, assess the security of BCOM systems, and identify potentially affected individuals. Further, BCOM notified law enforcement regarding the event. BCOM is also working to implement additional safeguards and training to its employees. BCOM is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, BCOM is providing impacted individuals with guidance on how to better protect against identity theft and fraud. BCOM is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

BCOM is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 336.448.8552.

Very truly yours,

A handwritten signature in black ink that reads "Matthew Toldero". The signature is written in a cursive, flowing style.

Matthew Toldero of
Constangy, Brooks, Smith & Prophete LLP

Exhibit A

BURRELL COLLEGE
of
OSTEOPATHIC MEDICINE

P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

July 11, 2024

Subject: Notice of Data <<Variable Text 1: Breach/Security Incident>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident experienced by Burrell College of Osteopathic Medicine (“BCOM”) that may have affected your personal information. BCOM takes the privacy and security of all personal information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On January 26, 2024, BCOM became aware of suspicious activity involving its digital environment disrupting access to certain of its systems. In response, BCOM took immediate steps to secure its systems and promptly launched an investigation. In so doing, BCOM engaged digital forensics and incident response specialists to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On May 31, 2024, BCOM determined that personal information may have been impacted in connection with the incident; BCOM then needed to complete an extensive review to confirm identities and collect addresses to begin notification obligations. That effort was completed on June 17, 2024. Please note that BCOM has no evidence of the misuse or attempted misuse of any potentially impacted information.

What Information Was Involved? The information potentially impacted in connection with this incident included your first and last name as well as your <<Variable Text 2: Potentially Impacted Data Sets>>.

What Are We Doing? As soon as BCOM discovered this incident, BCOM took the steps described above. In addition, BCOM implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. BCOM also notified the Federal Bureau of Investigation of this incident and is cooperating where necessary to hold the perpetrator(s) of the incident accountable.

Although BCOM has no evidence of the misuse of any potentially impacted information, BCOM is providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<Membership Length>> 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. The deadline to enroll in these services is October 11, 2024.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. BCOM also encourages you to enroll in the complementary services being offered to you through IDX by using the enrollment code provided.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call the toll-free number at 1-800-939-4170 from 7:00 A.M. to 7:00 P.M. Mountain Time, Monday through Friday (excluding holidays). The call center representatives will ensure that your questions are answered.

Please accept our sincere apologies and know that BCOM takes this matter very seriously and deeply regrets any problems that this may cause you.

Sincerely,

Burrell College of Osteopathic Medicine

STEPS YOU CAN TAKE TO HELP 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).

Copy of 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 <http://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

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 <http://www.annualcreditreport.com>.

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

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
Please note that there were 2 affected
individuals residing in Rhode Island.

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>.