



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)

September 19, 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
Tel: 410-576-6491
Email: Idtheft@oag.state.md.us

Re: Johnson & Wales University - Notice of Data Event

To Whom It May Concern:

We represent Johnson & Wales University ("JWU"), located at 8 Abbot Park Place, Providence, Rhode Island 02903, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately 318 Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, JWU 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 July 11, 2024, JWU learned of activity in its network that happened without its permission. In response, JWU took immediate steps to secure its systems and promptly launched an investigation. In so doing, JWU engaged digital forensics and incident response specialists to determine the nature and scope of the incident and to identify any information that may have been accessed or acquired without authorization. On August 21, 2024, JWU learned that personal information related to certain individuals may have been accessed in connection with the incident. JWU worked diligently to identify and gather contact information for potentially affected individuals and to engage a vendor to assist with notification. This process was completed on September 6, 2024.

The information that could have been subject to unauthorized access includes first and last name, as well as Social Security number.

2. Notice to Maryland Residents

On or about September 19, 2024, JWU provided written notice of this incident to approximately 318 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, JWU moved quickly to investigate and respond to the incident, assess the security of JWU systems, and identify potentially affected individuals. Further, JWU notified federal law enforcement regarding the event. JWU also implemented additional safeguards and training. JWU is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals, and is providing impacted individuals with guidance on how to better protect against identity theft and fraud. JWU 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.

JWU 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 "Matt Toldero". The signature is written in a cursive, flowing style.

Matt Toldero of
Constangy, Brooks, Smith & Prophete LLP

Exhibit A



JOHNSON & WALES
UNIVERSITY

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Subject: Notice of Security Incident/Subject: Notice of Data Breach)>>

Dear <<first_name>> <<last_name>>,

We are writing to inform you of the recent data security incident experienced by Johnson & Wales University (“JWU”) that may have affected your personal information. JWU takes the privacy and security of all personal information within its possession 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 July 11, 2024, JWU learned of activity in its network that happened without its permission. In response, JWU took immediate steps to secure its systems and promptly launched an investigation.

In so doing, JWU engaged digital forensics and incident response specialists to determine the nature and scope of the incident and to identify any information that may have been accessed or acquired without authorization as a result. On August 21, 2024, JWU learned that personal information of yours may have been accessed in connection with the incident. Please note that JWU has no evidence of the misuse or attempted misuse of any potentially accessed information.

What Information Was Involved? The information potentially accessed in connection with this incident included your name as well as your <<b2b_text_2(data elements)>>.

What Are We Doing? JWU is working to implement measures to enhance the security of its digital environment. JWU also notified the Federal Bureau of Investigation of this incident and will provide whatever cooperation is necessary to assist in law enforcement’s investigation.

Although JWU has no evidence of the misuse of any information as a result of this incident, JWU is providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity monitoring services through Kroll.

What You Can Do: JWU encourages you to take steps to avoid identity theft. Review your account statements, credit reports, and other data. Look for errors or suspicious items and report them right away. You can follow the recommendations on the enclosed “Steps You Can Take to Help Protect Your Information” for more specific guidelines. JWU also encourages you to activate the complimentary services being offered to you through Kroll by using the enrollment information provided.

For More Information: If you have questions or need assistance, please call [TFN](#) from 9:00 am to 6:30 pm, Eastern Time, Monday through Friday (excluding holidays).

Please know that JWU takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Johnson & Wales University

Steps You Can Take to Help Protect Your Information

Enroll in Monitoring: To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<Monitoring Term Length (Months)>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit 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.

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 may 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 2000
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

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; and 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>.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, 1-800-952-5225.

District of Columbia Residents: For more information you can contact the Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW Washington, DC 20001, 202-442-9828, consumer.protection@dc.gov. You can also visit the Office of Consumer Protection's website at <https://oag.dc.gov/consumer-protection> for more information.

Iowa Residents: You may wish to report suspected incidents of identity theft to local law enforcement or the Attorney General, Consumer Protection Division, at Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, by phone at 515-281-5926 or 888-777-4590, or by email at consumer@ag.iowa.gov. You can also visit the Consumer Protection Division website at <https://www.iowaattorneygeneral.gov/forconsumers> for more information.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: You may wish to contact the Attorney General, Consumer Protection Division, for more information at 200 St. Paul Place, Baltimore, MD 21202, by telephone at 410-528-8662 or 888-743-0023, or by email at Consumer@oag.state.md.us. You can also visit the Consumer Protection Division website at <https://www.marylandattorneygeneral.gov/Pages/CPD/default.aspx> for more information. JWU is located at 8 Abbott Park Place, Providence, RI 02903.

New Mexico Residents: Please note your rights under the Fair Credit Reporting Act, which can be viewed here https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

New York Residents: You may wish to contact the Attorney General's Office at The Capitol, Albany, NY 12224-0341, or by telephone at 800-771-7755 or 800-788-9898. You may also contact Bureau of Internet and Technology Resources at 1-212-416-8433 or visit <https://www.dos.ny.gov/consumerprotection/> for more information.

North Carolina Residents: You may wish to contact the Attorney General's Office at 9001 Mail Service Center Raleigh, NC 27699-9001, or by telephone at 1-877-566-7226. You can also find more information from the Consumer Protection Division by visiting <https://ncdoj.gov/protectingconsumers/>.

Oregon Residents: You may wish to contact the Attorney General's Consumer Protection Division by email at help@oregonconsumer.gov or by telephone at 877-877-9392. You may also visit <https://www.doj.state.or.us/consumer-protection/> for more information.

Rhode Island Residents: You may wish to contact the Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400. Please note you have the ability to file or obtain a police report related to this incident. [Please note that there were \[#\] 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