Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, Pennsylvania 19103
aweaver@constangy.com
Direct: 941.875.5335

October 24, 2023

VIA ELECTRONIC MAIL
Attorney General Anthony G. Brown
Maryland Attorney General's Office
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents North River Co. ("North River") in connection with a recent data security incident described in greater detail below. North River takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent because personal information for Maryland residents may have been involved in the incident.

1. Nature of the Security Incident

On September 4, 2023, North River became aware of unusual network activity and immediately took steps to secure our systems. North River engaged cybersecurity experts to assist with the process. The investigation determined that certain North River data may have been acquired without authorization in early September. After undertaking a review of the potentially affected files, North River identified certain personal information was involved. This review concluded on October 9, 2023 and revealed the individuals whose personal information could have been involved. North River thereafter worked to gather outstanding information needed to provide individual notification.

2. Number of Maryland Residents Involved

On October 24, 2023, North River notified three (3) Maryland residents of this data security incident via U.S. First-Class Mail pursuant to the A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

The personal information involved in this incident includes individuals' names, Social Security numbers, and financial account information such as would appear on K-1 forms or other tax-related documents.

3. Steps Taken to Address the Incident

As soon as North River discovered this unusual network activity, it took steps to secure the affected systems and launched an investigation to determine whether, and to what extent, individual information had been accessed or acquired without authorization. North River has also implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, North River has offered individuals 24 months of complimentary services through Kroll, which include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

North River has established a toll-free call center through Kroll to answer questions about the incident and address related concerns.

4. Contact Information

North River remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at aweaver@constangy.com.

Sincerely,

Aubrey Weaver
Partner
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter

NORTH RIVER
COMPANY

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

I am writing to inform you of an unfortunate data security incident at our business that may have affected your personal information. We take the privacy and security of personal information very seriously at North River Company ("North River"). Based on this occurrence we are providing you with steps you can take to help protect your personal information, and offering you complimentary identity monitoring services.

What Happened. On September 4, 2023, North River became aware of unusual network activity and immediately took steps to secure our systems. We engaged cybersecurity experts to assist with the process. The investigation determined that certain North River data may have been acquired without authorization in early September. After undertaking a review of the potentially affected files, we identified certain information that we believe was involved. Our review concluded on October 9, 2023, and identified that some of your information may have been involved.

What Information Was Involved. The potentially affected information may have included your name, Social Security number, and/or financial account information that may be on subscription agreements, K-1 forms or other tax documents.

What We Are Doing. As soon as North River discovered the incident we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. We also notified law enforcement and will provide whatever cooperation may be necessary to hold the perpetrators accountable

In addition, we have secured the services of Kroll to provide identity monitoring services at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.[1]

> 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>>**

What You Can Do: Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to help protect your information. You can also enroll in the Kroll identity monitoring services, which are offered to you at no cost, using the instructions above. Please note the deadline to enroll in these complimentary services is <<b2b_text_6(activation deadline)>>. Please do not discard this letter, as you will need the Membership Number provided above to access services.

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

For More Information. If you have questions about this letter or need assistance, please call TFN. Representatives are available Monday through Friday from 9:00 am – 6:30 pm Eastern Time. Representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. You can also call me at 212-695-8090.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause. We regret this incident occurred and are working to implement safeguards to further secure our network environment.

Sincerely,

Christopher S. Flagg, President
North River Company
610 West 26th Street, Suite 910
New York, NY 10001

STEPS YOU CAN TAKE TO 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).

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 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

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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

KROLL

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.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.