



Lindsay B. Nickle, Partner & Vice Chair
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, Texas 75270
LNickle@constangy.com
Direct: 806.535.0274
Emergency:
BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

February 26, 2024

VIA EMAIL

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

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents McKinley Architecture & Engineering ("McKinley") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you, in accordance with Maryland's statute, that this incident may have affected the personal information of one (1) resident of Maryland.

1. Nature of the Security Incident

On November 23, 2023, McKinley discovered it was the victim of a sophisticated cybersecurity attack that impacted their network environment. Upon discovery the activity, McKinley took immediate steps to secure the environment and engaged a leading cybersecurity firm to assist with a forensic investigation to determine what happened and evaluate the extent of unauthorized activity. The investigation revealed that an unauthorized actor gained access to some of the data in the McKinley computer network. McKinley took steps to review affected files and determined that the data may have included personal information of some of their employees. It is also possible that personal information for spouses and dependents of employees could have been impacted.

2. Number of Maryland Residents Involved

On February 26, 2024, McKinley notified one (1) resident of Maryland of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter is included with this correspondence.

The personal information involved in this incident includes names and Social Security numbers.

3. Steps Taken to Address the Incident

As soon as McKinley discovered this unauthorized activity, it took steps to secure the affected system and launched an investigation to determine whether, and to what extent, personal information had been accessed or acquired without authorization. McKinley has implemented additional measures to enhance its network security and minimize the risk of a similar incident occurring in the future. Further, as referenced in the sample consumer notification letter, McKinley is providing individuals with complimentary credit and identity protection services.

4. Contact Information

Pond 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 (806)-535-0274 or by e-mail at lnickle@constangy.com. Please let me know if you have any questions.

Sincerely,



Lindsay B. Nickle
Vice Chair
Constangy, Brooks, Smith & Prophete,
LLP

Enclosure: Sample Notification Letter



ARCHITECTURE + ENGINEERING

Return to IDX:

4145 SW Watson Avenue, Suite 400

Beaverton, OR 97005

<<first name>> <<last name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

February 26, 2024

Subject: Notice of Data Security Incident

Dear <<first name>> <<last name>>:

I am writing to inform you of a potential data security incident that may have affected personal information. At McKinley Architecture & Engineering ("McKinley") we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps to take to protect personal information, and offering complimentary credit monitoring and identity protection services.

What Happened? On November 23, 2023, McKinley discovered it was the victim of a sophisticated cybersecurity attack that affected our network environment. Upon discovering this activity, we took immediate steps to secure the environment and engaged a leading cybersecurity firm to assist with a forensic investigation to determine what happened and evaluate the extent of unauthorized activity. The investigation revealed that an unauthorized actor gained access to some of the data in our computer network. We reviewed the affected files and we determined that the data impacted may have included some of your personal information. In addition, if you have provided McKinley with personal information belonging to a spouse or any dependents as part of our benefits process, their personal information may also have been impacted.

What Information Was Involved? The information potentially impacted included names and Social Security numbers.

What Are We Doing? As soon as McKinley discovered the incident we took the steps described above. We also implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. In addition, we are offering complimentary credit monitoring and identity protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help protected individuals resolve issues if there is an identity compromise.

What Can You Do? We recommend that you review and implement the guidance included with this letter about how to protect your information. We also encourage you to enroll in the services offered to you through IDX by scanning the QR code above, calling 1-800-939-4170, or going to <https://app.idx.us/account-creation/protect> and using the individual enrollment code provided above. If you provided McKinley with personal information belonging to your spouse or dependents, use the following code for your enrollment and to enroll each of them for the services we are offering: <<family code>>. Please note that credit monitoring is not available to minors. The deadline to enroll is May 26, 2024.

McKinley Architecture & Engineering
1324 Chapline Street, Suite 400
Wheeling, West Virginia 26003

For More Information: Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call 1-800-939-4170 Monday through Friday from 9 am – 9 pm Eastern Time or go to <https://app.idx.us/account-creation/protect>. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Sean Doyle". The signature is fluid and cursive, with the first name "Sean" and last name "Doyle" clearly distinguishable.

Sean Doyle
Director of Operations
McKinley Architecture & Engineering

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).

Change Your Passwords on Your Online Accounts: It is good practice to regularly update your passwords on any online account, but it is even more important to do so in the event of a security incident. Consider using different passwords for each account and ensure that the password includes at least one uppercase letter, lowercase letter, number, and symbol where possible.

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

New York Attorney General

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

New Jersey Attorney General

Department of Law and Public Safety
25 Market St,
Trenton, NJ 08611
1-609-292-4925

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://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf.