



Matthew Toldero, Esq.
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
One West 4th Street, Suite 850
Winston-Salem, NC 27101
mtoldero@constangy.com
336.448.8552

August 12, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Department of Professional and Financial Regulation
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident

Dear Attorney General Anthony G. Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Haumiller Engineering Company (“Haumiller”), located at 370 Joseph Drive in South Elgin, Illinois. We are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately two (2) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Haumiller 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.

Nature of the Data Event

On April 30, 2024, Haumiller identified suspicious activity within its environment temporarily disrupted the operability of its computer network. Haumiller promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. In addition, Haumiller began working to restore impacted systems as quickly as possible. Haumiller also engaged a digital forensics firm to conduct a privileged investigation to determine the nature scope of the incident and whether any personal information was accessed. On June 21, 2024, Haumiller determined that the incident may have affected personal information belonging to Maryland residents. Following this determination, Haumiller worked to identify the necessary contact information for the impacted population and prepare the necessary notification materials.

The affected information may have included individuals’ names, Social Security number, health insurance information, and treatment or diagnosis information.

Notice to Maryland Residents

On or about August 9, 2024, Haumiller provided notice of this incident to approximately two (2) Maryland residents via U.S. Mail. A sample copy of the notification letter is included with this correspondence as ***Exhibit A***.

Other Steps Taken and To Be Taken

Alabama Arkansas California Colorado District of Columbia Florida Georgia Illinois
Indiana Maryland Massachusetts Minnesota Missouri New Jersey New York
North Carolina Oregon Pennsylvania South Carolina Tennessee Texas Virginia Washington

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

Additionally, Haumiller is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Haumiller 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.

Contact Information

Should you have any questions or require additional information, please do not hesitate to contact me at mtoldero@constangy.com.

Sincerely,

A handwritten signature in cursive script that reads "Matthew Toldero".

Matthew Toldero, Esq.

Haumiller Engineering, Co
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB-09175



<<First Name>> <<Last Name>>

<Address>>

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



August 8, 2024

Re: Notice of Data Breach

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

Haumiller Engineering Company (“Haumiller”) is writing to notify you of a data security incident which may have included your personal information. Haumiller takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information.

What Happened? On April 30, 2024, Haumiller discovered suspicious activity temporarily disrupted the operability of its computer network. Haumiller promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. In addition, Haumiller began working to restore impacted systems as quickly as possible. Haumiller also engaged a nationally-recognized digital forensics firm to conduct an investigation into what happened and determine whether personal information was accessed or acquired without authorization. On June 21, 2024, Haumiller learned that your personal information was impacted in connection with the incident which is the reason for this notification.

What Information was Involved? The information that may have been affected in connection with this incident includes your name as well as your <<elements>>.

What Are We Doing? As soon as Haumiller discovered the incident, Haumiller took the steps discussed above. In addition, Haumiller reported the matter to law enforcement and will cooperate with efforts to hold the perpetrator(s) accountable. In order to reduce the likelihood of a similar incident occurring in the future, Haumiller also implemented additional measures to enhance the security of its network environment.

In addition, Haumiller is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This

notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. Haumiller recommends that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

In addition, you can contact TransUnion representatives who will work on your behalf to help resolve issues you may experience as a result of this incident.

For More Information: If you have questions about this letter or need assistance, please do not hesitate to reach out to our designated call center at Cyberscout at 1-800-405-6108, Monday through Friday from 8 AM to 8 PM Eastern Time, excluding holidays and they will be happy to provide you with additional information.

We take your trust in Haumiller and this matter very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Haumiller Company
370 Joseph Drive
South Elgin, IL 60177



STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services: To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Code>>.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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>.