



Maria Efaplatidis
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
175 Pearl Street
Suite C 402
Brooklyn, NY 11201
mefaplatidis@constangy.com
718.719.6475

December 16, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
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 Beltway Companies (“Beltway”), an international truck dealer headquartered in Baltimore, Maryland. Beltway 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 on behalf of Beltway because personal information for 456 Maryland residents could have been involved in the data security incident.

1. Nature of the Security Incident

On November 12, 2024, Beltway was alerted to unusual activity within our network. In response, Beltway immediately took measures to secure our network and to commence an investigation to determine the full nature and scope of the event. Beltway engaged cybersecurity experts to assist with the process. On or around November 25, 2024, Beltway’s investigation determined that some data may have been acquired without authorization. Beltway then conducted a comprehensive review of all potentially affected information. During a thorough review of the information, Beltway determined that some of your personal information was contained in the potentially affected data. Beltway then took steps to locate contact information needed to effectuate notification to such individuals. At the conclusion of this process on November 27, 2024, Beltway arranged for notification to potentially affected individuals.

The potentially affected information varies for each individual, but may have included individuals’ names, Social Security number, and driver’s license or state identification number.

2. Number of Maryland Residents Affected

Beltway notified 471 Maryland residents within the potentially affected population on December 16, 2024, via USPS First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as Beltway discovered the unusual network activity, it took steps to secure its systems and launched an investigation to determine learn more about what happened and what information could have been affected. Beltway has implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

Quality Enclosures has established a toll-free call center through IDX to answer questions about the incident and address related concerns. Additionally, Beltway is providing those whose Social Security number was involved with identity protection services through IDX. The IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 718.719.6475 or mefaplatidis@constangy.com.

Sincerely,



Maria Efaplatidis
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter



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

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

December 16, 2024

Subject: **Notice of Data Security Incident**

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

I am writing to inform you of a recent incident that may have affected some of your personal information. Beltway Companies (“Beltway”) is committed to maintaining the privacy and security of all information in our possession. This letter includes information about the incident and provides you with steps you can take to protect your personal information, along with a complimentary offer of credit and identity monitoring services.

What happened? On November 12, 2024, Beltway was alerted to unusual activity within our network. In response, we immediately took measures to secure our network and to commence an investigation to determine the full nature and scope of the event. Beltway engaged cybersecurity experts to assist with the process. On or around November 25, 2024, our investigation determined that some data may have been acquired without authorization. Beltway then conducted a comprehensive review of all potentially affected information. During a thorough review of the information, we determined that some of your personal information was contained in the potentially affected data. Beltway then took steps to locate contact information needed to effectuate notification to such individuals. At the conclusion of this process on November 27, 2024, Beltway arranged for notification to potentially affected individuals.

What Information Was Involved? The potentially affected information included your name, <<Variable Text 1—Impacted Data Elements>>.

What We Are Doing: As soon as we discovered the incident, we took the steps described above. We also performed a thorough review of our systems to investigate the incident and ensure that our systems remain secure. Beltway implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents.

In addition, we are offering identity protection services through IDX, 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 id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-903-3648, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is March 16, 2025.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information: You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-903-3648 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'JS' or 'Saum', written in a cursive style.

Jack Saum

Beltway Companies
1800 Sulphur Spring Road,
Baltimore, MD 21227

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER 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 (the “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 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 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
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

NC Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.