



Lauren Godfrey
Partner
1650 Market Street, 36th Floor
Philadelphia, Pennsylvania 19103
lgodfrey@constangy.com
Direct: 973.462.9521

March 31, 2023

Via Email

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

Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Pegasus Logistics Group (“Pegasus”) in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

In late April 2022, Pegasus discovered suspicious activity within its computer network. Pegasus immediately took steps to secure its network and launched an investigation with the assistance of a leading independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation revealed that an unknown actor gained access to and may have obtained some data from the Pegasus network. Pegasus then conducted a comprehensive review of the potentially affected data and determined that some personal information may have been involved in the incident. Pegasus then worked to gather current mailing addresses so that it could notify all potentially affected individuals.

The impacted information may have included the following: name, date of birth, Social Security number, driver’s license number, passport number, financial account number, medical information, and/or health insurance information.

2. Number of Maryland residents affected.

Pegasus notified thirteen (13) Maryland residents of this incident via first class U.S. mail on March 31, 2023. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Pegasus discovered this incident, Pegasus took the steps described above and launched an investigation to determine what happened and the scope of personal information potentially impacted. In addition, Pegasus implemented additional safeguards to help ensure the security of its network and

March 31, 2023

Page 2

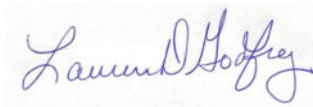
to reduce the risk of a similar incident occurring in the future.

Pegasus established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-833-903-3648 from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays). In addition, while Pegasus is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Pegasus is also providing complimentary credit monitoring and identity protection services to notified individuals.

4. Contact information.

Pegasus remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

A handwritten signature in blue ink, reading "Lauren Godfrey". The signature is written in a cursive, flowing style.

Lauren Godfrey
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

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

March 30, 2023

Re: Notice of Data <<Variable 1>>

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

We are writing to inform you of a data security incident that may have affected your personal information. At Pegasus Logistics Group (“Pegasus”), we take the privacy and security of personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including enrolling in the complimentary credit and identity protection services we are making available to you.

What Happened: In late April 2022, Pegasus discovered suspicious activity within its computer network. We immediately took steps to secure our network and launched an investigation with the assistance of a leading independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation revealed that an unknown actor gained access to and may have obtained some data from the Pegasus network. We then conducted a comprehensive review of the potentially affected data and determined that some of your personal information may have been involved in this incident. We then worked to gather current mailing addresses so that we could notify all potentially affected individuals. We have no evidence that your information has been misused.

What Information Was Involved: The information may have included your name, <<Variable data 2>> <<Variable data 3>>.

What We Are Doing: As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our network and to reduce the risk of a similar incident occurring in the future.

To help relieve concerns and to help protect your identity following this incident, we are providing you with information on steps you can take to help protect your personal information, and offering you credit and identity monitoring and protection services through IDX, a data security and recovery services expert. Your complimentary IDX identity monitoring and protection services include: <<12 months/ 24 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 you resolve issues if your identity is compromised. Additional information about these services is included with this letter. To take advantage of these services, you must follow the instructions in this letter to enroll. Please note the deadline to enroll is June 30, 2023.

What You Can Do: Please read the recommendations included with this letter which you can follow to help protect your personal information. **You can also enroll in the complimentary services being offered to you, at no cost.** Activation instructions and a description of the services being provided are included with this letter.

For More Information: If you have questions or need assistance, please contact 1-833-903-3648, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays or go to <https://app.idx.us/account-creation/protect> and use the Enrollment Code provided above. Our representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information. 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,

Marc Sherman

Marc Sherman
Chief Information Officer
Pegasus Logistics Group
306 Airline Drive, Suite 100
Coppell, TX 75019

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).

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/articles/pdf-0096-fair-credit-reporting-act.pdf>.