



Sean Hoar, Partner
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, Oregon 97035
shoar@constangy.com
503.459.7707

May 31, 2023

VIA EMAIL

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

Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Walker SCM. We are writing to notify you of data security incident experienced by Walker SCM which is described in greater detail below.

1. Nature of the Security Incident

On January 30, 2023, Walker SCM experienced a network disruption and immediately initiated an investigation of the matter. It engaged cybersecurity experts to assist with the process. The investigation determined that certain administrative and internal files may have been accessed without authorization. After a thorough review of those files, personal information was identified as being contained within the potentially affected data. Notification of affected persons was initiated as soon as their names and addressing information was obtained.

2. Number of Maryland Residents Involved

On April 27, 2023, Walker SCM notified eight (8) Maryland residents of this incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken to Address the Incident

Walker SCM has implemented additional security measures in its environment to reduce the risk of a similar incident occurring in the future. In addition, Walker SCM has provided the Maryland residents with complimentary credit monitoring and identity protection services – for a period of 12 months – along with additional resources to assist them. Walker SCM has also established a toll-free call center to address any questions and to help individuals resolve issues if their identity is compromised due to this incident.

4. Contact Information

Walker SCM 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 me at 503.459.7707 or by email at SHoar@constangy.com or David Rice at 718.614.2656 or by email at DRice@constangy.com.

Sincerely,



Sean B. Hoar
Partner & Chair, Cybersecurity & Data Privacy Team

Encl.: Sample Consumer Notification Letter

Walker International Transportation LLC
Return to IDX:
4145 SW Watson Ave. Suite 400
Beaverton, OR 97005



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

To Enroll, Please Call:

1-800-939-4170

Or Visit:

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

Enrollment Code: <<XXXXXXXX>>

April 27, 2023

Subject: Notice of Data Security Incident

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

I am writing to inform you of a data security incident that may have affected your personal information. At Walker International Transportation LLC ("Walker") 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 you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services.

What Happened. On January 30, 2023, Walker experienced a network disruption and immediately initiated an investigation of the matter. We engaged cybersecurity experts to assist with the process. The investigation determined that certain administrative and internal files may have been accessed without authorization. After a thorough review of those files, on April 6, 2023, some of your personal information was identified as being contained within the potentially affected data due to your relationship as a dependent of a Walker employee.

What Information Was Involved. The information may have included your name and Social Security number.

What We are Doing. As soon as Walker 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. We also notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable. In addition, we are offering you complimentary credit monitoring and identity protection services through IDX, a leader in consumer identity protection. These services include 12 months of credit monitoring, identity protection through CyberScan monitoring, a \$1,000,000 identity theft insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is affected. Please note that the deadline for enrollment is July 27, 2023.

What You Can 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 contacting 1-800-939-4170 or visiting <https://app.idx.us/account-creation/protect> and providing the enrollment code above.

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 9:00 am – 9:00 pm Eastern Time. 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 "Giorgio Laccona". The signature is fluid and cursive, with the first name "Giorgio" written in a larger, more prominent script than the last name "Laccona".

Giorgio Laccona

COO

Walker International Transportation LLC

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