



Laura K. Funk, Partner
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, Texas 75270
LFunk@constangy.com
Mobile: 248.709.9385

October 2, 2024

VIA EMAIL

Attorney General Anthony Brown
Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy Brooks Smith & Prophete LLP represents Ward Transport & Logistics Corporation ("Ward Transport"), located in Altoona, Pennsylvania, with respect to a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident.

Nature of the Security Incident

On March 3, 2024, Ward Transport experienced an encryption incident that disrupted access to certain parts of its digital environment. In response, Ward Transport took immediate steps to secure its environment and promptly launched an investigation. It also engaged independent cybersecurity experts to conduct an investigation. As a result of this investigation, Ward Transport learned that an unauthorized actor may have acquired certain data stored in Ward Transport's systems.

Ward Transport then undertook a comprehensive review of the potentially affected data. On September 23, 2024, it identified that certain individuals' personal information was contained in the affected data. The affected information varies by individual, but may have included individuals' names, driver's license or state ID numbers, username and information needed to access the accounts, financial account numbers, DNA profiles, medical information, parent's birth names, health insurance information, and Social Security numbers.

Number of Maryland Residents Affected

On October 2, 2024, Ward Transport notified 219 Maryland residents of this incident via First-Class U.S. Mail. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

Steps Taken Relating to the Incident

To help prevent something like this from happening again, Ward Transport is implementing additional security protocols. It is also offering complimentary credit and identity protection monitoring services to all individuals whose Social Security numbers were potentially affected by the incident.

Contact Information

Ward Transport remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please do not hesitate to contact me by phone at 248.709.9385 or by email at lfunk@constangy.com.

Regards,

A handwritten signature in black ink, appearing to read 'L. Funk', with a long, sweeping horizontal line extending to the right.

Laura K. Funk
Partner

Enc.: Sample Consumer Notification Letter



0007244

Ward Transport & Logistics
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB-09469

27_0007244



Dennis A Wescott
818 Scrubgrass Rd
Mercer PA 16137-5544



October 2, 2024

Subject: Notice of Data Security Incident

Dear Dennis A Wescott:

We are writing to inform you of a data security incident experienced by Ward Transport & Logistics Corporation ("Ward Transport"), located in Altoona, Pennsylvania, that may have involved some of your information. This letter is to notify you of the incident, offer you complimentary identity protection services, and inform you about steps you can take to help protect your personal information.

What Happened. On March 3, 2024, Ward Transport experienced an encryption incident that disrupted access to certain parts of its digital environment. In response, we took immediate steps to secure our environment and promptly launched an investigation. We also engaged independent cybersecurity experts to conduct an investigation. As a result of this investigation, we learned that an unauthorized actor may have acquired certain data stored in our systems. After a thorough review of the data, on September 23, 2024, Ward Transport determined that your personal information may have been impacted by this incident.

There is no evidence that your personal information has been misused as a result of this incident. However, out of an abundance of caution, we are notifying you about the incident, providing you with resources to help you protect your personal information, and offering you complimentary identity protection services.

What Information Was Involved. The data that could have potentially been acquired by the unauthorized party included your name and Social Security number, driver license number, username and access information for a non-financial account and individual health insurance policy number.

What We Are Doing. To help prevent something like this from happening again, we have reported this incident to the Federal Bureau of Investigation and are implementing additional technical security measures. We are also providing you with information about steps that you can take to help protect your personal information. As a further precaution, we are offering you 12 of complimentary identity protection services through TransUnion. This product helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do. You can follow the recommendations included with this letter to help protect your information. In addition, you can also enroll in TransUnion's complimentary identity protection services by logging on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: **A3364F3426D1**. 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.

For More Information. If you have any questions regarding the incident, please call 1-833-531-1370, Monday through Friday, between 8am to 8pm Eastern, excluding holidays.

The security of the information in our possession is a top priority for Ward Transport. We take your trust in us and this matter very seriously, and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Ward Transport & Logistics Corporation
1436 Ward Trucking Drive
Altoona, PA 16602

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 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 <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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.

