Alyssa Watzman
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
1901 Broadway, Suite 529
Denver, CO 80202
awatzman@constangy.com
720.536.3234

March 19, 2024

VIA ELECTRONIC MAIL
Attorney General Brenna Bird
Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
Email: consumer@ag.iowa.gov

Re: Notice of Data Security Incident

Dear Attorney General Bird:

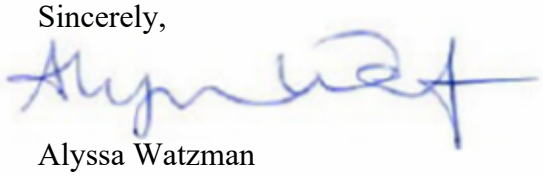
Constangy, Brooks, Smith & Prophete, LLP represents Schuster Company ("Schuster"), a transportation services company located in Iowa, in connection with the recent data security incident described below. I am writing to notify you of this incident because personal information belonging to residents of your state was involved. The affected information included individuals' names, Social Security numbers, and driver license or state identification numbers.

On January 30, 2024, Schuster discovered that it had experienced a temporary network outage that disrupted business operations. In response, Schuster took immediate steps to secure its network and initiated an investigation with the assistance of a nationally recognized digital forensics firm. Schuster determined on February 27, 2024, that the incident affected personal information belonging to Iowa residents. On March 19, 2024, Schuster provided notice of this incident to 807 Iowa residents whose information was involved. A sample copy of the notice letter is included with this correspondence.

In providing notice , Schuster offered notified individuals complimentary identity protection services through IDX. The services include credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity recovery services. Schuster has also reported this incident to law enforcement and will cooperate with investigate efforts.

Schuster 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 720.536.3234 or awatzman@constagy.com.

Sincerely,



Alyssa Watzman

Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter

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

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

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

March 19, 2024

Re: Notice of Data <<Variable Text 1: Breach or Security Incident>>

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

Schuster Company ("Schuster") is writing to notify you of a data security incident which affected your personal information. Schuster 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 January 30, 2024, Schuster discovered that it had experienced an incident that temporarily disrupted the operability of its computer network. Upon discovery, Schuster promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. In addition, Schuster began working to restore impacted systems as quickly as possible. Schuster also engaged a nationally-recognized digital forensics firm to conduct an independent investigation into what happened and determine whether personal information was accessed or acquired without authorization. On February 27, 2024, Schuster 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 <<Variable Text 2: Data Elements>>.

What Are We Doing? As soon as Schuster discovered the incident, Schuster took the steps discussed above. In addition, Schuster 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, Schuster also implemented additional measures to enhance the security of its network environment.

Additionally, Schuster is providing you with information about steps that you can take to help protect your information and is offering you complimentary identity protection services through IDX, a data breach and recovery services expert. These services include: <<12/24>> months of credit[1] and dark web monitoring, a $1,000,000 identity fraud loss insurance reimbursement policy, and fully managed identity recovery services. Please note that your deadline to enroll is June 19, 2024.

[1]To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. Schuster 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 IDX representatives at 1-888-683-5018 who will work on your behalf to help resolve issues you may experience as a result of this incident. IDX representatives are available Monday through Friday from 8 am – 8 pm Central Time.

For More Information: If you have any questions or need assistance, we encourage you to contact our dedicated call center at 1-888-683-5018 between 8 am and 8 pm Central Time.

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

Sincerely,

Steve Schuster
President, Schuster Company

STEPS YOU CAN TAKE TO HELP 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 (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.