



Matthew Toldero, Partner
Cybersecurity & Data Privacy Team
One West 4th Street, Suite 850
Winston-Salem, NC 27101
mtoldero@constangy.com
Mobile: 336.448.8552
Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

June 25, 2024

VIA E-MAIL

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 Event

To Whom It May Concern:

We represent General Sullivan Group Inc (“GSGI”), located at 85 Route 31 N, Pennington, NJ 08534, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately one (1) Maryland resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, GSGI does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about May 31, 2021, GSGI detected suspicious activity that temporarily disrupted the operability of its computer network. GSGI promptly took steps to secure the environment, restore affected systems, and begin an investigation to determine the nature and scope of the issue. The investigation determined that between May 30 – 31, 2024, an unauthorized actor gained access to certain portions of GSGI’s network and copied files without authorization. GSGI completed a diligent review of the files potentially impacted to determine the information that may have been affected and to identify to whom it belonged. On June 7, 2024, GSGI completed the review and first determined personal information was potentially accessible

The information that could have been subject to unauthorized access includes name, Social Security number, bank routing number and account number

Notice to Maryland Resident

On or about June 25, 2024, GSGI provided written notice of this incident to approximately one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, GSGI moved quickly to investigate and respond to the incident, assess the security of GSGI systems, and identify potentially affected individuals. Further, GSGI notified federal law enforcement regarding the event. GSGI is also working to implement additional safeguards and training to

Alabama Arkansas California Colorado District of Columbia Florida Georgia Illinois
Indiana Maryland Massachusetts Minnesota Missouri New Jersey New York
North Carolina Oregon Pennsylvania South Carolina Tennessee Texas Virginia Washington

its employees. GSGI is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, GSGI is providing impacted individuals with guidance on how to better protect against identity theft and fraud. GSGI is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

GSGI is providing written notice of this incident to relevant state federal regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (336) 448-8552.

Very truly yours,

A handwritten signature in black ink that reads "Matt Toldero". The signature is written in a cursive, flowing style.

Matt Toldero

Partner, Cybersecurity & Data Privacy Team

General Sullivan Group, Inc.

P.O. Box 989728

West Sacramento, CA 95798-9728

<< First Name>> << Last Name>>

<<Address1>>, <<Address2>>

<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

June 25, 2024

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

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

General Sullivan Group Inc (“GSGI”) is writing to notify you of a data security event that may involve your personal information. GSGI 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 May 31, 2024, GSGI detected suspicious activity that temporarily disrupted the operability of its computer network. GSGI promptly took steps to secure the environment, restore affected systems, and begin an investigation to determine the nature and scope of the issue. The investigation determined that between May 30 – 31, 2024, an unauthorized actor gained access to certain portions of GSGI’s network and copied files without authorization.

What Information was Involved? GSGI completed a diligent and comprehensive review of relevant systems to determine the information that may have been affected and to identify to whom it belonged. On June 7, 2024, we determined that information related to you was stored on the affected systems. The information that may have been affected by this incident includes your name, Social Security number, documentation needed to meet i9 verification, bank routing number and account number. At this time, we have no indication that your information was subject to actual or attempted misuse in connection with this incident.

What Are We Doing? GSGI takes this incident and the security of information within our care very seriously. Upon discovery of this incident, GSGI launched an in-depth investigation to determine the full nature and scope of this incident. As part of our ongoing commitment to the privacy of information in our care, we reviewed the efficacy of our security policies and procedures to protect against similar incidents in the future. We are also notifying state regulators, as required.

Additionally, GSGI 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 ZeroFox Company, a data breach and recovery services expert. These services include <<12/24 months>> of identity protection. Please note that your deadline to enroll is September 25, 2024.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports to detect errors or suspicious activity. You can find more information about resources available to you to help protect your information from possible misuse in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find information on how to enroll in the complimentary credit monitoring services.

For More Information: If you have any questions or need assistance, we encourage you to contact our dedicated call center at 1-800-939-4170, Monday through Friday from 9 am - 9 pm Eastern Standard Time.

Sincerely,

General Sullivan Group, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. The deadline to enroll is September 25, 2024.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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
<https://www.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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.