STG International, Inc. Provides Notice of Data Privacy Incident

STG International, Inc. ("STGi") is providing notice of a recent event that may impact the privacy of certain individuals' information. We are unaware of any actual or attempted misuse of individuals' information as a result of this event but are providing details about the event, steps we have taken in response, and resources available to help individuals better protect their information, should they feel it is appropriate to do so.

What Happened? We became aware of suspicious activity related to an employee's email account and promptly commenced an investigation to determine the nature and scope of the activity. The investigation determined that an email phishing campaign targeted certain employees' email accounts and resulted in unauthorized person(s) intermittently logging into the accounts between October 22, 2020 and January 12, 2021. However, the investigation was unable to determine which, if any, emails and attachments in the account were viewed by the unauthorized person(s). Out of an abundance of caution, we undertook a thorough review of the accounts' contents to determine whether they contained any sensitive information. We recently completed this review and determined, on May 3, 2021, that information related to certain individuals was present in the email account during the relevant time period. We took additional steps to identify address information for individuals and worked to provide notice of this event as quickly as possible.

What Information Was Involved? We cannot confirm if the unauthorized person(s) accessed or viewed any specific information relating to individuals. However, we determined that the information present in the relevant accounts included certain individuals' names, dates of birth, driver's license numbers / state identification numbers, financial account information, Social Security numbers, U.S. alien registration numbers, passport numbers, taxpayer identification numbers, employer-assigned identification numbers, payment card information, medical information, health insurance information, and/or online account credentials (i.e. usernames and passwords) Please note that the information varies by individual and for many individuals, a limited number of data types were determined to be accessible.

What We Are Doing. We have taken steps to enhance the security of our systems, including resetting the affected employees' credentials, increasing conditional access protocols for email access outside of the United States, and requiring multifactor authentication for access to email. As part of our ongoing commitment to the privacy and security of information in our care, we are providing enhanced training to our broader employee base on the how to detect suspicious emails. We are also in the process of reviewing our existing policies and procedures to better prevent future events.

As an added precaution, we are providing access to 12 months of complimentary credit monitoring and identity restoration services through Kroll, along with guidance on how to better protect against the possibility of information misuse. The complimentary credit monitoring services will be available to individuals whose Social Security numbers or the equivalent were accessible as a result of this event. If you did not receive written notice of this incident but believe you may be affected, please contact our dedicated assistance line, which can be reached at (855) 731-2989, 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. holidays. The call center will verify whether you are eligible for services.

What You Can Do. Individuals can find out more about how to protect themselves generally against the potential misuse of information in the enclosed *Steps You Can Take to Protect Information.*

For More Information. If you have questions or concerns that are not addressed in this notice, please do not hesitate to contact (855) 731-2989, 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. holidays.

Steps You Can Take to Protect Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. There are 4 Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.