MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 16, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent STG International, Inc. ("STGi") located at 2900 S. Quincy Street, Suite 888, Arlington, Virginia 22206, and are writing to notify your office of an incident that may affect the privacy of some personal information relating to twelve (12) New Hampshire residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned after its submission. By providing this notice, STGi does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

STGi 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, STGi undertook a thorough review of the accounts' contents to determine whether they contained any sensitive information. STGi 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. STGi took additional steps to identify address information for individuals and worked to provide notice of this event as quickly as possible.

STGi cannot confirm if the unauthorized person(s) accessed or viewed any specific information relating to individuals. However, STGi determined that the information present in the relevant accounts included the following data related to New Hampshire residents: name and Social Security number.

Notice to New Hampshire Residents

STGi began providing notice to individuals regarding this incident on June 2, 2021. On June 16, 2021, STGi is providing written notice of this incident to additional individuals whose information was accessible within the email accounts, which includes twelve (12) New Hampshire residents. 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

STGi has taken steps to enhance the security of its 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 its ongoing commitment to the privacy and security of information in its care, STGi is providing enhanced training to its broader employee base on the how to detect suspicious emails. STGi is also in the process of reviewing its existing policies and procedures to better prevent future events. As an added precaution, STGi is providing potentially affected individuals with access to complimentary credit monitoring and identity restoration services for one (1) year through Kroll.

Additionally, STGi is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. STGi 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/eyl

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

NOTICE OF <<b2b_text_1(SubjectLine)>>

Dear <<first_name>> <<last_name>>:

STG International, Inc. is writing to inform you of a recent event that may impact the privacy of some of your information. Although we are unaware of any actual or attempted misuse of your information, we are providing you with details about the event, steps we have taken in response, and resources available to help you better protect your information, should you 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 such as yourself 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 you. However, we determined that the information present in the relevant accounts included your <<b2b_text_2(DataElements)>>.

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 also providing you with 12 months of complimentary access to identity monitoring services through Kroll, along with guidance on how to better protect against the possibility of information misuse. We are covering the cost of these services, but due to privacy restrictions, you will need to complete the activation process yourself using the activation instructions below.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to detect errors. You can find out more about how to better protect against the potential misuse of information in the enclosed *Steps You Can Take to Help Protect Information.* There, you will also find more information about the identity monitoring services we are offering and how to activate.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call 1-???-???-????, 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. holidays. You may also write to us at: STG International, Inc., ATTN: Marcia Euwema, VP Human Resources, 2900 South Quincy Street, Suite 888, Arlington, VA 22206.

We apologize for any inconvenience this event may cause you and remain committed to the privacy of information in our possession.

Sincerely,

Jeff Bell

Chief Operating Officer
STG International, Inc.

Steps You Can Take to Help Protect Information

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit 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.

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 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 in regard to this incident. There are [#] 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/.