

BAKER BOTTS LLP

101 CALIFORNIA ST.
SUITE 3200
SAN FRANCISCO, CALIFORNIA
94111

TEL +1 415 291 6200
FAX +1 415 291 6300
BakerBotts.com

AUSTIN
BRUSSELS
DALLAS
DUBAI
HONG KONG
HOUSTON
LONDON

RECEIVED
MOSCOW
NEW YORK
PAKISTAN
RIYADH
SAN FRANCISCO
WASHINGTON
CONSUMER PROTECTION
RECEIVED

NOV 12 2021

November 4, 2021

SI GROUP, INC.

Matthew R. Baker
TEL: 4152916213
FAX: 4152916313
matthew.baker@bakerbotts.com
CONSUMER PROTECTION

Via Certified Mail

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

Re: Supplemental Data Breach Notification

To whom it may concern,

I write on behalf of SI Group, Inc. (“SI Group” or “Company”), which previously reported a ransomware attack on or about October 4, 2021, to provide supplemental information identified through the Company’s ongoing incident assessment.

Per N.H. Rev. Stat. Section 359-C:20, I write to provide the following information:

1. Background

On August 14, 2021, SI Group, Inc. became the victim of a ransomware attack, which infected the Company’s systems and resulted in the unauthorized access or theft of files containing personal information. Upon discovery, the Company took immediate steps to contain the threat and engaged leading third-party forensic experts to investigate the incident and assist with its remediation efforts. The Company also notified federal law enforcement authorities of the incident and are cooperating with their investigatory efforts.

The Company’s internal investigation has found that, between August 9, 2021, and August 14, 2021, the threat actor infiltrated SI Group’s system and was able access and remove data from file servers on our corporate networks.

2. Impacted Personal Information

The exact personal information accessed varies by individual, but the Company has determined that the types of personal information impacted may include name, address, date of birth, and other sensitive data elements, such as a social security number, driver’s license number, or passport number. Not all of this information was disclosed in each instance, and the impacted personal information may be a subset of these categories for each person.

BAKER BOTTS LLP

Office of the New Hampshire Attorney
General

- 2 -

November 4, 2021

3. Affected Residents

The Company's ongoing assessment has revealed three additional New Hampshire residents who may have been impacted by the incident. The Company has issued individual notices to these individuals on October 26, 2021, a copy of which is enclosed.

Please contact me directly if you have questions or require additional information.

Respectfully,



Matthew R. Baker

MB
Enclosure



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>,

We are writing to inform you of an incident that may have affected your personal information.

What Happened?

On August 14, 2021, SI Group, Inc. became the victim of a ransomware attack, which infected the Company's systems and may have resulted in the unauthorized access or theft of files containing personal information. Upon discovery, we took immediate steps to contain the threat and engaged leading third-party forensic experts to investigate the incident and assist with our remediation efforts. We also notified federal law enforcement authorities of the incident, and are cooperating with their investigatory efforts.

Our internal investigation has found that, between August 9, 2021, and August 14, 2021, the threat actor infiltrated our system and was able to access and remove data from file servers on our corporate networks, which principally contained personal information relating to certain Company employees (both current and former), but may have also contained personal information of contractors, beneficiaries, and other third parties.

We regret the impacts that this incident may have on you, and we are sending this letter to inform you of what we know and provide some options to minimize risk to yourself.

What Information Was Involved?

The exact personal information accessed varies by individual, but we have determined that the types of personal information impacted include name, address, date of birth, and other sensitive data elements, such as a social security number, driver's license number, passport number, or health or insurance information. Please know that not all of this information was disclosed in each instance, and your impacted personal information may be a subset of these categories.

What We Are Doing.

We take the security of your personal information very seriously. As soon as we discovered the incident, we isolated our networks and launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. In response to this attack, we have enhanced our security and monitoring processes and taken other measures to minimize the risk of similar incidents in the future.

In addition, we have arranged to offer you credit monitoring, identity theft protection, and Dark Web monitoring services for a period of two years, at no cost to you, through Equifax. It is possible that this incident impacted both adults and minors, which may have been identified as beneficiaries, for example. As a result, instructions on how to activate these services for both adults and minors are included in the attached Equifax Enrollment Instructions. If your minor does not receive an individual notice, though, we have no reason to believe that their information has been impacted by this event. **Please note that if you have already enrolled in this service pursuant to a previous notice from the Company, then you are already covered by the plan and no further action is required.**

What You Can Do.

In addition to enrolling in the complimentary credit monitoring, we have established a dedicated call center to assist you with answering any questions you may have. You may contact the call center toll-free at 800-983-8781 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday, except holidays.

Finally, we encourage you to carefully review your accounts and your credit reports to ensure that all of your account activity is valid. You should promptly report any questionable charges to the organization with which the account is maintained.

For More Information.

If you have any questions about this incident or would like additional information, please refer to the enclosures for general steps you can take to monitor and protect your personal information or contact the call center at 800-983-8781 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday, except holidays.

We regret that this incident occurred and apologize for any inconvenience this incident may have caused you.

Sincerely,

David Bradley

President & CEO – SI Group



Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourage potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate.

Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **Register:** Complete the form with your contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

¹ The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

² Credit monitoring from Experian and TransUnion will take several days to begin.

³ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

⁴ The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁶ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Child Monitoring Package

Key Features

- Child Monitoring for up to four children under the age of 18
- Emailed notifications to the primary adult member of activity on the child's Equifax credit report

Enrollment Instructions

Parent/guardian Go to www.equifax.com/activate.

Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **Register:**
Complete the form with parent/guardian contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:**
Enter parent/guardian email address, create a password, and accept the terms of use.
3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
Upon successful verification of parent/guardian identity, you will see the Checkout Page.
Click 'Sign Me Up' to finish enrolling.
The confirmation page shows parent/guardian completed enrollment.
Click "View My Product" to access the product features and enroll minor children.

How to Add Minors to Your Equifax Child Monitoring Package

You will be able to add minors to your Equifax Child Monitoring Package through your product dashboard.

1. Sign in to your account to access the "Your People" module on your dashboard.
2. Click the link to "Add a Child."
3. From there, enter your child's first name, last name, date of birth and social security number.
Repeat steps for each minor child (up to four).

Equifax will then create an Equifax credit file for your child, lock it and then alert you if there is any activity on that child's Equifax credit file. You can add up to 4 children under the age of 18 with your Equifax Child Monitoring Package.

STEPS YOU CAN TAKE TO FURTHER 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.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

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 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 can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
535 Anton Blvd., Suite 100
Costa Mesa, CA 92626

TransUnion
(800) 916-8800
www.transunion.com
P.O. Box 6790
Fullerton, CA 92834

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 12 months. 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. For more information on fraud alerts, you may contact the three national credit reporting agencies, the FTC (as described below), or visit <http://www.annualcreditreport.com>.

Security Freeze

In some US states, you have the right to put a security freeze on your credit file at no cost to you. 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. For more information on security freezes, you may contact the three national credit reporting agencies or the FTC (as described below). As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

Additional Free Resources on Identity Theft

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit <http://www.ftc.gov/idtheft>, call 1-877-ID-THEFT (877-438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

North Carolina Residents

You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You may review the information provided by the North Carolina Attorney General at <http://www.ncdoj.gov>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

District of Columbia Residents

You can obtain information from the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can review the information provided by the D.C. Attorney General at <https://oag.dc.gov/> or by calling 202-727-3400.

Maryland Residents

Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

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 violators. 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.

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/>.

Oregon Residents

State laws advise you to report any suspected identity theft to law enforcement, as well as the Attorney General and the Federal Trade Commission.

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 two Rhode Island residents impacted by this incident.