SIMPSON
Strong-Tie

March 19, 2024

VIA U.S. MAIL

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

On behalf of Simpson Strong-Tie Co. Inc. ("SST"), an engineering and building materials manufacturing company, I am writing to inform you about an incident in which personal information relating to New Hampshire residents was accessed by an unauthorized third party.

On October 10, 2023, we discovered that an unknown third party had gained access to our information technology infrastructure. After becoming aware of this issue, we immediately took steps to secure our environment and launched an investigation with the support of external cybersecurity experts to determine the actions the unknown third party had taken. Although our investigation was in its early stages, we disclosed the incident publicly in an 8-K on October 11, 2023, and alerted federal law enforcement the same day.

Through our investigation, we have determined that, from October 9, 2023 to October 11, 2023, the unknown third party had access to certain data that included personal information, largely relating to current and former SST employees. Because of the complexity of the data at issue, including significant unstructured data, SST had to undergo a lengthy data review process to determine whether the third party accessed any personal information and, identify the individuals to whom that personal information related – and this process took time. Through our review, we have determined that the third party accessed the following types of personal information:

In addition to conducting a thorough review of the relevant SST systems, we have taken various steps to harden our environment, including, among others, blocking all known indicators of compromise, conducting an enterprise-wide password reset, enhancing our security monitoring and logging capabilities, reviewing the account permissions for both administrative and standard user accounts and further restricting access rights where appropriate.

On March 19, 2024, we will begin notifying 8 New Hampshire residents about this incident. We are offering these individuals complimentary credit and identity monitoring services, which are provided by Experian. These services include credit monitoring and certain fraud support services. Each individual's letter contains instructions on how to enroll in these services. Attached is a sample of the letter that we are providing to New Hampshire residents.

If you have any questions, please do not hesitate to contact me at . I can also be reached at 5956 W. Las Positas Blvd. Pleasanton, CA 94588 and cpayton@strongtie.com.

Sincerely,

Cassandra Payton
Executive Vice President, General Counsel
Simpson Strong-Tie Co. Inc.

SIMPSON
Strong-Tie

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

L0285-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 NON-MA
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Notice of Data Breach

March 19, 2024

On behalf of Simpson Strong-Tie Co. Inc., I am writing to notify you about an incident that involved certain personal information about you. Please know that we take the security of personal information seriously and we regret that this incident occurred.

What Happened

On October 10, 2023, we discovered that an unknown third party had gained access to our information technology infrastructure. After becoming aware of this issue, we immediately took steps to secure our environment and launched an investigation with the support of external cybersecurity experts to determine the actions the unknown third party had taken. We also disclosed the incident publicly in an 8-K on October 11, 2023, and notified federal law enforcement the same day.

What Information Was Involved

Through our investigation, we determined that the unknown third party's period of access lasted from October 9, 2023 to October 11, 2023, and that during this time they had access to data that included personal information about certain individuals, including you. Please note that due to the complexity of the data at issue, this incident required a lengthy data review process, which we conducted with the goals of identifying all of the data that was accessed and, to the extent that the data included personal information, identifying the individuals to whom that personal information related – and this process has taken time. Through this review, we determined that the personal information involved in this incident included the following: [Variable text].

What We Are Doing

In addition to conducting a thorough review of the affected systems, we have taken several steps to harden our environment, including blocking all known indicators of compromise, conducting an enterprise-wide password reset, enhancing our security monitoring and logging capabilities, reviewing the account permissions for both administrative and standard user accounts and further restricting access rights where appropriate. We are also currently in the process of evaluating whether additional security enhancements are warranted.

What You Can Do

As a precaution, we have arranged for you, at your option, to enroll in complimentary credit and identity monitoring services. We have engaged Experian to provide you with its IdentityWorks℠ service, which includes credit monitoring and enhanced fraud support services. You have until June 30, 2024 to activate these services by using the following activation code: This code is unique for your use and should not be shared. To enroll, please visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit. If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at by . Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian. Additionally, and consistent with certain laws, we are providing you with the information below about steps that you can take to protect against potential misuse of personal information.

For More Information

Please know that we regret any inconvenience or concern this incident may cause you. If you have any questions or concerns, please do not hesitate to contact us at

Sincerely,

Cassandra Payton
Executive Vice President, General Counsel

Steps you can take to protect against potential misuse of personal information:

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.ftc.gov/idtheft, or call the FTC at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from the nationwide credit reporting agencies. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Department
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.Equifax.com	www.Experian.com	Chester, PA 19022-2000
		www.TransUnion.com

You also have other rights under the Fair Credit Reporting Act ("FCRA"). For information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

You can obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to verify your identity. You may place a fraud alert in your file by calling any of the nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to provide the credit reporting agency with certain information, such as your name, address, date of birth and Social Security number. After receiving your request, the credit reporting agency will send you a confirmation containing a unique PIN or password that you will need in order to remove or temporarily lift the freeze. You should keep the PIN or password in a safe place.

State-specific Information

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.