STRATEGIC TECHNOLOGY INSTITUTE INC

Notice of Data Breach

August 23, 2021

Important Notice Regarding Potential Disclosure of Personal Information

Dear Current or Former Employee:

Strategic Technology Institute, Inc. (STi) is contacting you about a security incident involving potential disclosure of your personal information. As described below, we experienced a breach to certain human resources information that resulted in the potential acquisition of personal information associated with you. As a result, STi is notifying you of this incident so that you can take steps to protect your identity, as further described below.

What Happened?

On June 25, 2021, STi discovered an email account used by human resources personnel had been compromised by an unauthorized user. After an internal investigation into the contents of that email account, STi determined that email account contained personal, including personal information associated with you. STi implemented corrective actions to ensure the security of our storage and transmission of personal information, including by implementing additional security measures on employee email accounts and restricting access to employee personal information. STi's investigation did not conclude that any personal information was targeted by an unauthorized person, and to date, we have received no indication that any personal information has been misused.

What Information Was Involved?

Personal information that was potentially accessed or acquired may have included your name, home address, birthday, phone number, employee identification number, social security number, and email address. A small number of individuals who submitted Family Medical Leave Act and Short-Term Disability forms to STi's Human Resources department may have had their doctor's information and diagnoses accessed or acquired.

What We Are Doing?

STi took immediate steps upon the discovery of the compromised account to terminate the compromised account and prevent any further unauthorized access to personal information. STi has secured our account logins and updated policy to require 2-Factor Authentication (2FA) when employee's login to their accounts. STi also has implemented restricted access to files containing employee information when sent to external organizations. We have been in contact with legal counsel about our legal obligations.

What You Can Do?

STi recommends you remain vigilant by reviewing your account statements and monitoring free credit reports that you can obtain from the three consumer reporting agencies. You may also have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. Finally, you may want to consider placing a fraud alert on your credit report. Please review the "Additional Resources" page enclosed with this letter for more information.

We encourage you to report suspected incidents of identity theft to local law enforcement, the state attorney general, or the Federal Trade Commission ("FTC"). Please see the "Additional Resources" page for the relevant contact information for these agencies. We also encourage you to review the FTC's comprehensive guide called "Take Charge: Fighting Back Against Identity Theft" to help you guard against and deal with identity theft. This guide is available at www.ftc.gov/IDtheft.

For More Information

STi sincerely apologizes for any inconvenience or concern that this situation may cause. We take the security of your personal information seriously. If you have any further questions regarding this matter, please do not hesitate to call us at 301-770-7077 or email us at employeesupport@sti-inc.com.

Sincerely,

Strategic Technology Institute, Inc.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax	Experian	TransUnion
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorney General's Office. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the State Attorney General's office. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

You may contact the **Montana Attorney General's Office, Office of Consumer Protection** at 215 North Sanders, P.O. Box 201401, Helena, MT 59620, https://www.dojmt.gov, 1-406-444-4500

Other Information. We have not delayed this notification due to any law enforcement investigation.