



Richard W. Goldberg
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Richard.Goldberg@lewisbrisbois.com
Direct: 215.977.4060

File No. 30841.1706

January 21, 2022

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

Re: **Notice of Data Security Incident**

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Startek, Inc. ("Startek"), a customer solutions and digital experiences business located in Greenwood Village, Colorado in connection with a recent data security incident that may have affected the information of certain Maryland residents.

1. NATURE OF THE SECURITY INCIDENT

Startek experienced a network disruption on June 26, 2021. Startek immediately took steps to secure their environment and engaged cybersecurity experts to assist with an investigation. The investigation determined that an unknown actor gained access to and obtained data from the Startek network without authorization.

Startek undertook a review of the information that could have potentially been accessed as a result of the incident. On December 23, 2021, Startek determined that information related to its customers and employees, including the personal information of seventeen (17) Maryland residents, was potentially impacted. The information potentially accessed without authorization may have included the first and last name, Social Security Number and Date of Birth. To date, Startek has no evidence that any potentially impacted information has been misused in conjunction with this incident.

2. NUMBER OF MARYLAND RESIDENTS AFFECTED

Startek notified the seventeen (17) Maryland residents of this data security incident via first class U.S. mail on January 21, 2022. A sample copy of the notification letter sent to the affected individuals is attached.

3. STEPS TAKEN RELATING TO THE INCIDENT

Startek implemented additional security features to reduce the risk of a similar incident occurring in the future. Startek also reported this incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to attempt to hold the perpetrators of this incident accountable, if possible.

While Startek has no indication that the information has been misused, it nonetheless is providing individuals with information about steps that they can take to help protect their personal information. As a further precaution, Startek is also offering Maryland consumers one (1) year of complimentary credit and identity monitoring services through IDX. This product helps detect possible misuse of personal information and provides consumers whose information may have been accessed without authorization with identity protection support.

4. CONTACT INFORMATION

Startek is committed to protecting the security of the personal information in their possession. Please feel free to contact me at Richard.Goldberg@lewisbrisbois.com or by phone at 215-977-4060 if you have any further questions.

Sincerely,



Richard W. Goldberg of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

RWG

Enclosure: Sample Consumer Notification Letter



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

To Enroll, Please Call:
(833) 704-9387
Or Visit:
<https://www.experianidworks.com/credit>
And Provide:
Engagement Number: ENGAGE#
Activation Code: ABCDEFGHI



H3644-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 GENERAL (12 MONTHS)
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



January 21, 2022

Subject: Notice of Data Security Incident

Dear Sample A. Sample:

I am writing to inform you of a data security incident that may have affected your personal information. At StarTek, we take the privacy and security of personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including enrolling in the complimentary identity protection services we are making available to you.

What Happened? On June 26, 2021, StarTek learned of unusual activity occurring on its network. Upon discovering this activity, StarTek immediately took steps to secure its technological environment and began an internal investigation with the help of cybersecurity experts. Our investigation identified that an unauthorized individual gained access to and acquired some documents from StarTek's environment. At this point, StarTek did not know if these documents contained any personal information. StarTek undertook a thorough review of this subset of files and determined that some of your personal information was found in these documents. We are not aware of the misuse of any personal information that may have been involved in this incident. Out of an abundance of caution, we are offering free credit monitoring services.

What Information Was Involved? The potentially affected information may have included your [Extra1].

What Are We Doing? As soon as we discovered this incident, we took the steps described above. In addition, we are providing you with information about steps you can take to help protect your personal information and, out of an abundance of caution, we are offering you credit monitoring and identity theft restoration services at no cost to you through Experian. With this protection, Experian will help you resolve issues if your identity is compromised.

What Can You Do? We recommend that you review the guidance included with this letter about how to help protect your information. We encourage you to contact Experian with any questions and to enroll in free identity protection services.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

0000001



H3644-L01

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll** by April 30, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **ABCDEFGHI**

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 (833) 704-9387 by April 30, 2022. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH 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.

We encourage you to take full advantage of this service offering if you have not done so already. Experian representatives are fully versed on the incident and can answer questions or respond to concerns you may have regarding the protection of your personal information.

For More Information: Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call our dedicated call center (833) 704-9387 toll-free Monday through Friday from 9:00 am – 11:00pm Eastern, or Saturday and Sunday from 11:00am – 8:00pm Eastern (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,



Dixie Pepper
General Counsel & Chief Legal Officer
StarTek

* 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.

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 (FTC).

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

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 one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

0000001



