



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

August 24, 2021

VIA EMAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent SmartStart Employment Screening, Inc. ("SmartStart") in connection with a data security incident which is described in greater detail below. SmartStart takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On December 18, 2020, we identified suspicious activity on our server. Upon identifying this activity, we immediately launched an investigation into the incident. We also consulted with cyber experts to determine what information, if any, may have been accessed. After an extensive forensic investigation and data mining that ended on August 4, 2021, we learned both that personal information may have been involved in the incident, whose information it was, and where those people were located. Based on the results of the forensic investigation, SmartStart offered credit monitoring services to the impacted individuals.

2. Number of New Hampshire residents affected.

SmartStart mailed notification letters on approximately August 24, 2021 to the 181 New Hampshire residents regarding this data security incident. A sample copy of the notification letter sent to the affected individuals is enclosed with this letter.

3. Steps taken relating to the incident.

SmartStart has taken steps outlined above in response to this incident and has made alterations to its cyber environment to help prevent similar incidents from occurring in the future. Additionally, we are providing impacted individuals with information about steps they can take to help protect their personal information. SmartStart is also offering identity protection services at no cost through IDX, which will help individuals resolve issues if their identity is compromised due to this incident.

4. Contact information.

SmartStart remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (215) 977-4060 or via email at Richard.Goldberg@lewisbrisbois.com.

Regards,



Richard W. Goldberg of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosures: Sample Consumer Notification Letter

To Enroll, Please Call:
1-833-325-1769
Or Visit:
<https://response.idx.us/smartstart>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>> <<Suffix>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

August 24, 2021

Re: Notice of Data <<Variable Data 1>>

Dear <<FIRST NAME>> <<LAST NAME>> <<Suffix>>,

I am writing to inform you of a data security incident that involved your personal information. You may not have heard of SmartStart Employment Screening, Inc. (“SmartStart”) but we are a company which provides background screening services to other companies. Your data may have been with us because you applied for a position with one of these companies.

SmartStart takes the privacy and security of data very seriously. This is why I am notifying you of the incident, offering you credit and identity monitoring services, and informing you about steps you can take to help protect your personal information.

What Happened? On December 18, 2020, we identified suspicious activity on our server. Upon identifying this activity, we immediately launched an investigation into the incident. We also consulted with cyber experts to determine what information, if any, may have been accessed. After an extensive data mining investigation, on August 4, 2021, we learned that your information may have been involved.

What Information Was Involved? The information which may have been exposed included names <<Variable Data 2>>.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. In addition, we are offering you information about steps you can take to help protect your personal information, including complimentary identity monitoring and recovery services for <<Membership Offering Length>> through a leading identity protection company called IDX, as described below.

What You Can Do: You can follow the recommendations included with this letter to protect your personal information. We strongly encourage you to enroll in the credit and identity monitoring services we are offering through IDX to protect your personal information. To enroll, please visit <https://response.idx.us/smartstart> or call 1-833-325-1769 and provide the enrollment code at the top of this letter. Your <<Membership Offering Length>> of services will include credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

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. Additional information describing your services is included with this letter.

Please note you must enroll by November 24, 2021. If you have questions or need assistance, please call IDX at 1-833-325-1769.

For More Information: Information about additional steps you can take is on the accompanying pages. You should also report suspected identity theft to law enforcement, including the Attorney General of your state and the Federal Trade Commission. If you have any questions about this letter, please contact IDX at 1-833-325-1769. Please know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in cursive script, appearing to read "Elaine Rosenberg".

Elaine Rosenberg
Chief Executive Officer
SmartStart Employment Screening, Inc.

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL 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 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:

TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Experian P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 740241 Atlanta, GA 30374 1-866-349-5191 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 annualcreditreport.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 90 days. 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: Under U.S. law, 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	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 401-274-4400
---	---	---	--

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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

