



David B. Sherman, CIPP/US
550 E. Swedesford Road, Suite 270
Wayne, PA 19087
David.Sherman@lewisbrisbois.com
Direct: 215.977.4070

May 15, 2019

File No. 24725.740

VIA E-MAIL

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

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

I represent Vista Autism Services (“Vista”), located in Hershey, Pennsylvania, with respect to a recent data security incident. This letter is submitted on behalf of Vista pursuant to N.H. Rev. Stat. §§ 359-C:19-21, because the personal information of one (1) New Hampshire resident may have been affected by the incident. The information potentially impacted may include names, addresses, Social Security numbers, tax and wage information, and financial account information.

On March 1, 2019, Vista discovered suspicious activity within its third-party employee payroll system. Vista immediately launched an investigation with the assistance of a leading independent digital forensics firm. Vista also reported the incident to the Federal Bureau of Investigation, Cyber Division. The collective investigation served to determine what happened, whether any personal information had been accessed without authorization, and to identify the scope of individuals affected. On April 30, 2019, the investigation revealed that one (1) New Hampshire resident may have been affected. In response to the incident, Vista promptly implemented additional security features to safeguard personal information in its possession and minimize the likelihood that an event like this could occur again in the future.

Vista notified the affected New Hampshire resident via the attached letter on May 15, 2019. Vista is offering complimentary credit monitoring and identity restoration services for twelve (12) months to the affected resident through TransUnion. Please contact me should you have any questions.

Office of the Attorney General
May 15, 2019
Page 2

Very truly yours,

A handwritten signature in black ink, appearing to read "David Sherman".

David B. Sherman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter



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>>

Subject: Notice of Data Security Incident

Dear <<Name 1>>,

I am writing to inform you of a data security incident that may have affected your personal information. We take the privacy and security of your information very seriously and regret any concern that this incident may cause you. We are providing this notice to inform you of the incident and to call your attention to some steps that can be taken to protect your information.

What Happened? On March 1, 2019, we discovered suspicious activity within our third-party payroll system when certain employees did not receive their pay in a timely fashion. Upon learning of this, we immediately commenced an investigation and reported the incident to law enforcement. We also engaged a leading digital forensics firm to perform an independent investigation to determine what happened, whether any personal information had been accessed without authorization and to identify the scope of individuals affected. Our investigation recently revealed that some of your personal information may have been accessed without authorization. This letter serves to inform you of the incident, and to share steps that you can take to help protect your information.

Additionally, this letter includes instructions to enroll in credit monitoring and identity restoration services that **we arranged to provide for a period of twelve (12) months at no cost** in order to help further safeguard your personal information.

What Information Was Involved? The information involved may include names, addresses, Social Security numbers, tax and wage information, and financial account information.

What Actions Are We Taking? As soon as we discovered the incident, we took the steps described above. In addition, we notified the Federal Bureau of Investigation, Cyber Unit, engaged cybersecurity professionals, and implemented a number of additional network security features to safeguard personal information in our possession and minimize the likelihood of a similar event from occurring in the future. **We are also providing you with a twelve (12) month membership of TransUnion Interactive's myTrueIdentity credit monitoring and identity restoration service at no cost to you.** This product provides you with premier credit monitoring and identity theft resolution, including up to \$1 million of identity theft insurance coverage. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: <<Enrollment Deadline>> (Your code will not work after this date)
- Visit the myTrueIdentity website to enroll: www.MyTrueIdentity.com
- Provide your activation code: <<Insert Unique 12-letter Activation Code>>
- Additional information describing your services and how to enroll offline is included with this letter.

What Can You Do? You can follow the recommendations on the following pages of this letter to protect your personal information. You can also enroll in the myTrueIdentity credit monitoring and identity restoration service that we are providing through TransUnion Interactive. In addition, if you have not already done so, we encourage you to complete IRS Form 14039, Identity Theft Affidavit, which you can obtain at <http://www.irs.gov/pub/irs-pdf/fl4039.pdf>. We also recommend that you review your credit report and consider placing a security freeze on your credit file. If you have other identity theft / tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. You should be especially aware of any requests, calls, emails, letters, or other questions about your financial accounts or from individuals purporting to be from the IRS or other entities you would not be expecting contact from. If you receive any type of unexpected request for personal information, you should not provide that information and instead contact the organization to verify the request is legitimate.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please do not hesitate to call 877-330-3487, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Kirsten Yurich". The signature is fluid and cursive, with the first name "Kirsten" and last name "Yurich" clearly distinguishable.

Kirsten K. L. Yurich
Chief Executive Officer
Vista Autism Services

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 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 this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 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: You have the right to put a security freeze on your credit file. 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. There is no charge to place, lift or remove the security freeze. 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, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

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), including: 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 others. 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.

IRS Notice: Please note that the IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels. For additional information from the IRS, please visit <https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft>.

Complimentary One-Year *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. Mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)