NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com



February 6, 2017

**By Certified Mail**
**Return Receipt Requested**

**Office of the New Hampshire Attorney General**
**Consumer Protection & Antitrust Bureau**
**33 Capitol Street**
**Concord, NH 03301**

**Re: Legal Notice of Information Security Incident**

Dear Sirs or Madams:

I write on behalf of my client, Astadia, Inc., to inform you of a potential security incident involving personal information that may have affected approximately 23 New Hampshire residents. Astadia is notifying affected individuals and outlining some steps they may take to help protect themselves.

On February 2, 2017, an unauthorized individual, impersonating a Astadia executive, contacted an Astadia employee requesting certain information for Astadia employees. Before it was determined that the request was fraudulent, the Astadia employee provided files that contained limited information about some of its employees, including first and last name, address, Social Security number, and 2016 compensation information. The files did not include employees' dates of birth information. Astadia has investigated this incident and has found no evidence that the unauthorized individual was able to gain access to any Astadia systems as a result of this incident or that any customer information or other employee information was affected.

Astadia takes the privacy of personal information very seriously, and deeply regrets that this incident occurred. Astadia took steps to address this incident promptly after it was discovered, including working to investigate and remediate the situation. In addition to the annual cyber-security training that Astadia employees currently undergo, Astadia will proactively begin providing periodic updates to employees throughout the year as new phishing schemes or email scams come to its attention. Astadia will also implement additional training concerning how to handle any requests for sensitive information and how to potentially recognize a phishing scheme for employees in departments with access to sensitive employee information including conducting training sessions with mock phishing scenarios. In addition, Astadia has contacted law enforcement and will continue to cooperate in their investigation of this incident.

Affected individuals are being notified via written letter, which will begin mailing on or about February 6, 2016. A form copy of the notice being sent to the affected New Hampshire residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,

Kristopher Kleiner

KCK
Enclosure

Astadia

February 6, 2016

**[ADDRESS]**

**Dear [NAME],**

Astadia recently experienced a potential security incident involving the personal information of some of its current and former employees. We are providing this notice as a precaution to inform potentially affected individuals of the incident and to call your attention some steps you can take to help protect yourselves. We sincerely regret any concern this may cause you.

***What Happened***

On February 2, 2017, an unauthorized individual, impersonating an Astadia executive, contacted an Astadia employee requesting W-2 information for Astadia employees. Later that day, before it was determined that the request was fraudulent, the employee provided these files that contained limited information about some of our employees. It's important to note that Astadia's network including client data was never compromised; unfortunately this incident was the result of human error.

***What Information Wos Involved***

The files contained employee information including first and last name, Social Security number and 2016 compensation and deduction information as well as mailing/home address. Dates of Birth were not included in the files. Based on our investigation, we have not found any evidence that this incident involves any unauthorized access to or use of any Astadia computer system or network and no further information about any employee or customer was provided to any unauthorized individual. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

***What We Are Doing***

Astadia takes the privacy and protection of personal information very seriously, and deeply regrets that this incident occurred. We took steps to address this incident promptly after it was discovered, including working to investigate and remediate the situation. In addition to the annual cyber-security training that our employees currently undergo, Astadia will proactively begin providing periodic updates to employees throughout the year as new phishing schemes or email scams come to our attention. Astadia will also implement additional training concerning how to handle any requests for sensitive information and how to potentially recognize a phishing scheme for employees in departments with access to sensitive employee information including conducting training sessions with mock phishing scenarios. In addition, we have contacted the FBI's Cyber Division and will continue to cooperate in their investigation of this incident.

In addition, to help protect your identity, we are offering two years of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the information in the "Information about Identity Theft Protection" reference guide included here.

***What You Can Do***

We want to make you aware of steps you can take to guard against fraud or identity theft. We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. Also, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade

Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

As an additional precautionary measure, we also recommend that you file a Form 14039 "Identity Theft Affidavit" with the IRS to help prevent someone from filing a fraudulent tax return in your name. For additional information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft or call 800-908-4490. There may also be similar resources and forms to file for individual states, so we recommend that you contact your state department of revenue directly for more information.

***For More Information***

For more information about this incident, or if you have additional questions or concerns about this incident, you may contact us directly at 1-877-458-2650 between 8 am – 5 pm Eastern time, Monday through Friday or via email at IncidentFAQS@astadia.com. Again, we sincerely regret any concern this event may cause you.

Very truly yours,

Michelle Simpson
CFO

Astadia

## Information about Identity Theft Protection

As a precautionary measure to safeguard your information from potential misuse, we have partnered with Equifax® to provide its ID Patrol identity theft protection product for two years at no charge to you. If you choose to take advantage of this product, it will provide you with a notification of any changes to your credit information, $1 million Identity Fraud Expense Coverage and access to your credit report. ID Patrol will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies. Note: You must be over age 18 with a credit file in order to take advantage of the product.

ID Patrol provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports
- Wireless alerts and customizable alerts available (available online only)
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites (available online only)
- Ability to lock and unlock your Equifax Credit Report™ (available online only)
- Up to $1 million in identity theft insurance with $0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality* (available online only)

To enroll, go to www.myservices.equifax.com/patrol and follow the following steps:

- **Welcome Page**: Enter the following Activation Code **[ACTIVATION CODE]** in the "Activation Code" box and click the "Submit" button.
- **Register**: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
- **Create Account**: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
- **Verify ID**: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
- **Order Confirmation**: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

Please note that you must complete the enrollment process by [DATE].

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

**Review Accounts and Credit Reports:** You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For additional information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft or call 800-908-4490. There may be similar resources available at the state level, so we recommend that you contact your state department of revenue directly for more information.

**For residents of Maryland**: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

**For residents of North Carolina**: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

**For residents of Rhode Island** You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

**Fraud Alerts:** There are also two types of fraud alerts that 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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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 at the addresses or toll-free numbers listed at the bottom of this page.

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

## National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
**General Contact:**
P.O. Box 740241
Atlanta, GA 30374
800-685-1111
**Fraud Alerts:**
P.O. Box 740256, Atlanta, GA 30374
**Credit Freezes:**
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
**General Contact:**
P.O. Box 2002
Allen, TX 75013
888-397-3742
**Fraud Alerts and Security Freezes:**
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
**General Contact:**
P.O. Box 105281
Atlanta, GA 30348
877-322-8228
**Fraud Alerts and Security Freezes:**
P.O. Box 2000, Chester, PA 19022
888-909-8872