

April 5, 2022

**Anjali C. Das**  
312.821.6164 (direct)  
Anjali.Das@wilsonelser.com

**Via Email:**

**Attorney General Brian Frosh**  
Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
[IDTheft@oag.state.md.us](mailto:IDTheft@oag.state.md.us)

**Re: Notice of Cybersecurity Incident Involving River City Insurance Group d/b/a  
Lavinder Group & Associates**

Dear Attorney General Frosh:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents River City Insurance Group d/b/a Lavinder Group & Associates (“Lavinder Group”), an insurance brokerage company vendor that provides services to certain insurance carriers on behalf of their employer located at 525 Main Street, Danville, Virginia 24541, with respect to a recent cybersecurity incident that was first discovered by Lavinder Group in November 2020 (hereinafter, the “Incident”). Lavinder Group takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that Lavinder Group has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

**1. Nature of the Incident**

Sometime in November 2020, Lavinder Group became aware of a potential business email compromise. Lavinder Group quickly engaged a third-party professional cybersecurity forensics team on November 4, 2020 to conduct a thorough investigation into the entire email tenant. On December 23, 2020, the investigation determined that an unknown party did gain unauthorized access to one Lavinder Group employee’s email account. Lavinder Group engaged a data mining vendor on February 2, 2021 to determine if the email account contained sensitive information. On May 10, 2021, the data mining activity concluded that sensitive information was stored in the impacted email account. On or around December 3, 2021, Lavinder Group received information

---

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston  
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans  
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

**wilsonelser.com**

identifying individuals whose information may have been exposed. Lavinder Group reviewed this information internally to verify the names and addresses of potentially impacted parties.

Although Lavinder Group is unaware of any fraudulent misuse of information, it is possible that individuals' Name, Social Security Number, Driver's License or State ID Number, Financial Account Information, limited medical information, and/or health insurance information, may have been exposed as a result of this unauthorized activity.

As of this writing, Lavinder Group has not received any reports of related identity theft since the date of the incident (November 2020 to present).

## **2. Number of Maryland residents affected.**

A total of two (2) Maryland residents have been potentially affected by this incident. Notification letters to individuals were mailed on April 5, 2022, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

## **3. Steps taken in response to the Incident.**

Lavinder Group is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Lavinder Group moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, Lavinder Group engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, LSC is continuing to enhance security measures and providing cyber security training for the staff; implementing Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) software throughout the environment; encrypting local machines and emails; migrating data to Azure; implementing email spam filter and DNS filtering; implementing Dark Web monitoring; implementing firewall management; and implementing Multi Factor Authentication on email and Office 365. Lastly, Lavinder Group informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although Lavinder Group is not aware of any actual or attempted misuse of the affected personal information, Lavinder Group offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through Kroll to all individuals to help protect their identity. Additionally, Lavinder Group provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

## **4. Contact information**



Lavinder Group remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at [Anjali.Das@WilsonElser.com](mailto:Anjali.Das@WilsonElser.com) or 312-821-6164.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**

A handwritten signature in blue ink, appearing to read 'Anjali C. Das'.

Anjali C. Das

**EXHIBIT A**

<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

***Notice of Data Security Incident***

River City Insurance Group d/b/a Lavinder Group & Associates (“Lavinder Group”) is an insurance brokerage company vendor that provides services to certain insurance carriers on behalf of their employer. Lavinder Group is writing to notify you of a data security incident at Lavinder Group that may have resulted in the unauthorized access to some of your personal information. Lavinder Group takes the security of personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to help protect your information.

***What Happened:***

Sometime in November 2020, Lavinder Group became aware of a potential business email compromise when we received numerous emails from individuals informing that they received suspicious emails from a Lavinder Group employee. Lavinder Group quickly engaged a third-party professional cybersecurity forensics team on November 4, 2020 to conduct a thorough investigation into our entire email tenant. On December 23, 2020, the investigation determined that an unknown party did gain unauthorized access to one Lavinder Group employee’s email account. Lavinder Group engaged a data mining vendor on February 2, 2021 to determine if the email account contained sensitive information. On May 10, 2021, the data mining activity concluded that sensitive information was stored in the impacted email account. On or around December 3, 2021, Lavinder Group received information identifying individuals whose information may have been exposed. Lavinder Group reviewed this information internally to verify the names and addresses of potentially impacted parties. In addition, Lavinder Group obtained the services of a vendor to mail the notice, provide identity monitoring services, and set up a call center. Lavinder Group has also implemented a number of new security measures discussed below to prevent a similar incident from occurring.

***What Information Was Involved:***

Based on the investigation, it appears that some of your information may have been contained in the email account, including your name, Social Security number, Driver’s License or State ID Number, Financial Account Information, limited medical information, and/or health insurance information was included in the email account. While we do not have any evidence of the misuse of your information, we are nonetheless notifying you out of an abundance of caution and encourage you to take full advantage of the services offered.

***What We Are Doing and What You Can Do:***

Data privacy and security are among Lavinder Group’s highest priorities, and there are extensive measures in place to help protect information in Lavinder Group’s care. We are taking steps to prevent a similar event from occurring in the future, including but not limited to: continuing to enhance security measures and providing cyber security training for our staff; implementing Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) software throughout the environment; encrypting local machines and emails; migrating data to Azure; implementing email spam filter and DNS filtering; implementing Dark Web monitoring; implementing firewall management; and implementing Multi Factor Authentication on email and Office 365. This investigation and response included confirming the security of Lavinder Group’s systems, reviewing the contents of the relevant files for sensitive information, and notifying business partners associated with that sensitive information.

In light of this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you for one year. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefit forms, and to monitor your free credit reports for suspicious activity and to detect errors.

***How Do I Activate The Free Services:***

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b\_text\_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s\_n>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Additional information describing your services is included with this letter.

***For More Information:***

We sincerely regret any inconvenience that this matter may cause you and remain dedicated to maintaining the security and protection of your information. We encourage you to remain vigilant and review the enclosed addendum outlining additional steps you can take to help protect your personal information. If you have questions, please do not hesitate to call 1-???-???-????, Monday – Friday, 9:00 a.m. to 6:30 p.m., excluding major U.S. holidays.

Sincerely,

Lavinder Group & Associates



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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 Important Information**

**For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:** It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

**For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:** It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

**For residents of Oregon:** State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

**For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:** You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**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](http://www.oag.state.md.us)

**Rhode Island Office of the Attorney General** Consumer Protection 150 South Main Street, Providence RI 02903  
1-401-274-4400 [www.riag.ri.gov](http://www.riag.ri.gov)

**North Carolina Office of the Attorney General** Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 [www.ncdoj.com](http://www.ncdoj.com)

**Federal Trade Commission** Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580  
1-877-IDTHEFT (438-4338) [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**New York Office of Attorney General** Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755  
<https://ag.ny.gov/consumer-frauds/identity-theft>

**Colorado Office of the Attorney General** Consumer Protection 1300 Broadway, 9<sup>th</sup> Floor, Denver, CO 80203  
1-720-508-6000 [www.coag.gov](http://www.coag.gov)

**Arizona Office of the Attorney General** Consumer Protection & Advocacy Section, 2005 North Central Avenue,  
Phoenix, AZ 85004 1-602-542-5025

**Illinois Office of the Attorney General** Consumer Protection Division 100 W Randolph St., Chicago, IL 60601  
1-800-243-0618 [www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

**For residents of all states:**

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**Security Freeze:** You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

**Equifax Security Freeze**

P.O. Box 105788  
Atlanta, GA 30348  
800-525-6285

**Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
888-397-3742

**TransUnion (FVAD)**

P.O. Box 2000  
Chester, PA 19022  
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.