WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

November 10, 2021

Jennifer S. Stegmaier
312.821.6167 (direct)
Jennifer.Stegmaier@wilsonelser.com

Via Certified Mail; Return Receipt Requested:

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Cybersecurity Incident Involving Christensen O'Connor Johnson Kindness PLLC

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Christensen O'Connor Johnson Kindness PLLC ("COJK"), an intellectual property law firm located at 1201 Third Avenue, Suite 3600, Seattle, WA 98101, with respect to a ransomware attack that was first discovered by COJK on December 24, 2020 (hereinafter, the "Incident"). COJK 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 Washington residents being notified, and the steps that COJK 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

COJK has been serving the Seattle, Washington area since its founding in 1929. Unfortunately, on December 24, 2020, COJK's systems became infected with malware, which resulted in the encryption of some of our firm's servers and information stored on those systems. In response, COJK engaged a specialized digital forensics firm to investigate the incident on January 15, 2021. The firm discovered that an unauthorized individual was able to access COJK servers and potentially viewed COJK data using a vulnerability against COJK's VPN service provider.

COJK immediately enhanced its security by patching any known vulnerabilities, implementing organization-wide multifactor authentication, forcing password resets, and deploying a next-generation security suite to prevent this incident from occurring in the future. This system-hardening process concluded on or about February 15, 2021. Thus, the maximum window of compromise was from December 24, 2020, until February 15, 2021.

On March 11, 2021, the specialized forensic firm completed its investigation, confirming the Incident resulted in the unauthorized access of personally identifiable information. Upon learning

which systems were impacted, COJK worked to determine which individuals were likely to have been impacted. Regarding personal information, COJK determined, on March 15, 2021, that the unauthorized individual only accessed information belonging to past and present employees of COJK. Between April and August, COJK compiled a complete list of individuals that required notification. This process included fielding proposals from mailing, call center, and credit monitoring services firms to send notice letters to the affected population. On September 8, 2021, COJK engaged the mailing firm. Wilson Elser drafted notice letters for the affected individuals and appropriate regulatory bodies for COJK's review on October 5, 2021, subsequently approved on October 13, 2021. Lastly, the mailing vendor finalized the notice letters and proceeded to mail notice on November 10, 2021.

With any such event, it takes time to gather the relevant information, identify the affected individuals, hold the necessary internal discussions, and make the appropriate decisions to line-up the assistance services being offered. COJK was diligent with the investigation to ensure the appropriate protection services would be provided. In addition, COJK notified the Federal Bureau of Investigation (FBI) of the Incident and provides regular updates regarding any recent developments.

Although COJK is unaware of any fraudulent misuse of information, it is possible that individuals' full name, address, date of birth, Social Security number, and financial account number may have been exposed as a result of this unauthorized activity.

As of this writing, COJK has not received any reports of related identity theft since the date of the incident (December 24, 2020 to present).

2. Number of New Hampshire residents affected.

A total of three (3) New Hampshire residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on November 10, 2021, 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.

COJK 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, COJK moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, COJK engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. COJK then informed our law firm and began identifying the potentially affected individuals in preparation for notice. Moreover, to minimize the risk of a similar incident occurring in the future, COJK took steps including, but are not limited to: patching any known vulnerabilities; implementing organization-wide multifactor authentication; forcing password resets; and deploying a next-generation security suite.

Although COJK is not aware of any actual or attempted misuse of the affected personal information, COJK offered twelve (12) months of complimentary credit monitoring and identity

theft restoration services through Kroll to all individuals to help protect their identity. Additionally, COJK 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

COJK 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 Jennifer.Stegmaier@wilsonelser.com or 312-821-6167.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Jennifer S. Stegmaier

EXHIBIT A

CHRISTENSEN | O'CONNOR
JOHNSON | KINDNESS

COJK

<<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>>,

Out of an abundance of caution, we are writing to inform you of a recent cybersecurity incident which affected Christensen O'Connor Johnson Kindness PLLC ("COJK"). The cybersecurity incident may have resulted in the potential compromise of some of your data. This letter contains information about the incident and information about how to help protect your personal information going forward. COJK considers the protection of sensitive information a top priority, and sincerely apologizes for any inconvenience as a result of the incident.

What Happened

COJK has been serving the Seattle, Washington area since its founding in 1929. Unfortunately, on December 24, 2020, COJK's systems became infected with malware, which resulted in the encryption of some of our firm's servers and information stored on those systems. In response, Christensen O'Connor engaged a specialized cybersecurity firm to conduct an investigation of the incident. The firm found that an unauthorized individual was able to access some COJK servers and may have been able to view COJK data using a vulnerability against our VPN service provider.

What Information Was Involved

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the unauthorized individual may have had access to your name, contact information, date of birth, Social Security number, and financial account number. While we appreciate that the incident may be concerning, please note that COJK is not aware of any instances of misuse of sensitive data.

What We Are Doing

COJK takes the protection and proper use of your information very seriously. Ensuring the safety of your data is of the utmost importance to us, and we sincerely regret any inconvenience or concern that this may cause. In light of this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you, for twelve (12) months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the identity monitoring services we are making available to you.

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>>**

Additional information describing your services is included with this letter.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

Other Important Information

Again, COJK takes the protection and proper use of your information very seriously and we sincerely apologize for any concern or inconvenience this letter causes. Should you have any questions or concerns about this matter, please do not hesitate to call 1-???-???-???? Monday through Friday, 9:00 a.m. to 6:30 p.m., Eastern Time, excluding some U.S. holidays.

Sincerely,

Stacey Thompson, Chief Operating Officer
Christensen O'Connor Johnson Kindness PLLC
1201 3rd Avenue Suite 3600
Seattle, WA 98101

Steps You Can Take to Help Protect Your Information

Credit Reports: 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, 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.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You 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:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

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 *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island*: 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.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

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

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

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

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov

KROLL

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.