RECEIVED
AUG 01 2022
CONSUMER PROTECTION

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

July 25, 2022

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

Via Certified Mail; Return Receipt Requested:

Attorney General John Formella
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Cybersecurity Incident Involving Wilson Tool International

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Wilson Tool International, Doering Company, aspectLED, and Wilson Golf Group (collectively "Wilson Tool") a business that provides a comprehensive line of tooling systems and accessories for punching, bending, stamping, tableting, fluid motion, and Lighting industries, with respect to a recent data privacy incident that was first discovered by Wilson Tool on March 13, 2022 (hereinafter, the "Incident"). Wilson Tool 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 New Hampshire residents being notified, and the steps that Wilson Tool 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

On March 13, 2022, Wilson Tool discovered that an unauthorized party had accessed and encrypted information stored on their systems. Wilson Tool terminated the unauthorized access, and promptly commenced an internal investigation to determine the nature and scope of the Incident. Upon discovery of the incident, Wilson Tool promptly engaged a team of cyber security professionals to assist with the recovery of its data, and to conduct a forensic investigation to fully determine the scope and the overall impact of the Incident. After a thorough investigation, Wilson Tool concluded some personal information from our systems may have been accessed by an unauthorized actor.

Although Wilson Tool is unaware of any fraudulent misuse of information, it is possible that individuals' names, addresses, dates of birth, and Social Security numbers may have been exposed as a result of this unauthorized activity.

As of this writing, Wilson Tool has not received any reports of related identity theft since the date of the incident (March 13, 2022 to present).

2. Number of New Hampshire residents affected.

A total of two (2) New Hampshire residents have been potentially affected by this incident. Notification letters to individuals were mailed on July 25, 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.

Wilson Tool 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, Wilson Tool moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. In response to the Incident, Wilson Tool engaged a specialized third-party cybersecurity firm, changed administrative credentials, implemented a data back-up system, installed new security firewalls, enhanced already-existing monthly vulnerability scanning and system patching capabilities, began strictly enforcing multi-factor authentication, improved anti-virus active monitoring, conducted additional cybersecurity awareness training, and took steps and will continue to take steps to mitigate the risk of future harm.

Although Wilson Tool is not aware of any actual or attempted misuse of the affected personal information, Wilson Tool offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through Kroll to all individuals to help protect their identity. Additionally, Wilson Tool 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

Wilson Tool 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 or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

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>>

Re: NOTICE OF DATA SECURITY INCIDENT

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Out of an abundance of caution, Wilson Tool International. ("Wilson Tool"), is writing to inform you of a data security incident that may have resulted in an unauthorized access of your personal information. Wilson Tool sincerely apologizes for this incident and any inconvenience it may cause you. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the events, steps that Wilson Tool is taking in response, and resources available to help you protect against the potential misuse of your information.

Why Do We Have Your Information?

Wilson Tool has your information because you are currently or were previously employed by Wilson Tool or one of Wilson Tool's affiliated companies.

What Happened?

On March 13, 2022, Wilson Tool discovered that an unauthorized party had accessed and encrypted information stored on our systems (the "Incident"). Wilson Tool terminated the unauthorized access, and promptly commenced an internal investigation to determine the nature and scope of the Incident. While the Incident is still being investigated, it was determined that the unauthorized party accessed servers which contain some of your sensitive personal information. While Wilson Tool has no reason to believe that any individual information has been misused, upon this discovery, Wilson Tool has decided to make notification to you, and to provide identity monitoring services to help protect you from the potential misuse of personal data.

What Information Was Involved?

The personal information that may have been accessed by an unauthorized includes your full name, as well as your: <<b2b_text_1(data elements)>>.

Please note that Wilson Tool has received no indication that your information has been used by the unauthorized actor or by any unauthorized party to commit fraud. Wilson Tool is providing notice to you out of an abundance of caution.

What We Are Doing

Wilson Tool values the privacy of your information and will continue to do everything it can to help protect it. Since the discovery of the incident, Wilson Tool moved quickly to investigate, respond, and confirm the security of our systems. Specifically, Wilson Tool engaged a specialized third-party cybersecurity firm, changed administrative credentials, implemented a data back-up system, installed new security firewalls, enhanced already-existing monthly vulnerability scanning and system patching capabilities, began strictly enforcing multi-factor authentication, improved anti-virus active monitoring, conducted additional cybersecurity awareness training, and took steps and will continue to take steps to mitigate the risk of future harm.

Out of an abundance of caution, and to help relieve concerns and restore confidence following this incident, Wilson Tool has secured the services of Kroll to provide identity monitoring at no cost to you for 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, Web Watcher, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

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

What You Can Do

You may activate the identity monitoring services we are making available to you. Once again, Wilson Tool is making these services available to you at no cost; however, you will need to activate yourself in these services. **The deadline to activate is** <<b2b_text_6(activation deadline)>>. Wilson Tool would like to reiterate that, at this time, there is no evidence that your information was misused. However, Wilson Tool encourages you to take full advantage of the services offered.

Enclosed with this letter you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information. Wilson Tool encourages you to activate the services offered and to remain vigilant against incidents of identity theft and fraud. Such vigilance includes reviewing account statements and credit reports for suspicious activity. Individuals are encouraged to report any suspicious activity to the affiliated institutions immediately.

For More Information:

The protection of your information is a top priority, and Wilson Tool International sincerely regrets any concern or inconvenience that this matter may cause. If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

Wilson Tool International

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.

Web Watcher
Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.

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.

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.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: 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.

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