WINSTON & STRAWN LLP

NORTH AMERICA SOUTH AMERICA EUROPE ASIA

35 W. Wacker Drive
Chicago, IL 60601
T +1 (312) 558-5600
F +1 (312) 558-5700

VIA OVERNIGHT MAIL

February 8, 2023

Attorney General John M. Formella
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Privacy Incident

Attorney General Formella:

Winston & Strawn LLP ("Winston") represents Apex Tool Group, LLC ("ATG"), located at 910 Ridgebrook Road, Suite 200, Sparks, Maryland 21152, with respect to the privacy incident that is the subject of this letter. I am writing to inform this office of the incident pursuant to New Hampshire law, as it affected two (2) New Hampshire residents.

By way of background, on March 11, 2022, ATG observed unusual activity resulting in the inaccessibility of certain systems within its network. ATG immediately took steps to contain the threat and investigate the extent of this activity, including eradicating the underlying unauthorized access to its systems. In particular, ATG proactively disconnected ATG servers, networks, and applications to contain the issue and maintain the safety of its systems. ATG then took additional steps to enhance its security posture, including resetting network and administrative passwords and deploying additional endpoint detection and response technology.

ATG later determined that an unknown third party initially accessed its network on or around February 21, 2022. ATG also investigated what, if any, sensitive personal information may have been accessed or acquired in connection with the incident. Unfortunately, as of the close of its investigation on January 13, 2023, ATG could not definitively confirm whether any sensitive personal information was potentially impacted in connection with the incident. However, ATG acknowledges that it collects certain sensitive personal information from workforce members in the normal course of its business human resources functions, which may include the name, date of birth, Social Security number, government identification numbers (e.g., passports, driver's license and military identification numbers, etc.), and financial account numbers (e.g., provided to ATG for direct deposit purposes).

Out of an abundance of caution, ATG is providing notification to individuals in New Hampshire who may have had their sensitive personal information impacted by the incident. Such notification is scheduled for February 8, 2023. A sample notification is attached to this letter. In addition, ATG offered these individuals twenty-four months of credit monitoring and identity protection services through Equifax. Of note, ATG is not aware of any malicious misuse of any information as a result of the event.

WINSTON
&STRAWN
LLP

NORTH AMERICA SOUTH AMERICA EUROPE ASIA

35 W. Wacker Drive
Chicago, IL 60601
T +1 (312) 558-5600
F +1 (312) 558-5700

By providing the information in this letter, ATG expressly reserves all available rights, defenses, and privileges in connection with this incident. Furthermore, ATG does not admit or concede any liability or wrongdoing, and expressly reserves its right to contest or challenge any findings or conclusions of any investigation by this office or any other office or agency with appropriate jurisdiction. Finally, this notice is not, and does not otherwise constitute, a waiver of ATG's objection that New Hampshire lacks personal jurisdiction with respect to the incident.

It is my hope that this information will satisfy this office's need for information related to this incident. However, if this office requires any additional details, please contact me by telephone at

Sincerely,

Alessandra V. Swanson

Apex Tool Group
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>>

Dear <<Name 1>>:

Apex Tool Group ("ATG") is notifying relevant workforce members, including you, of a cybersecurity event that may have impacted some of their personal information. This notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On January 13, 2023, ATG concluded its investigation into the cybersecurity event that led to our information systems becoming impaired for a period of time. As you may know, on March 11, 2022, we observed unusual activity resulting in the inaccessibility of certain systems within our network. We immediately took steps to contain the threat and investigate the extent of this activity. We also retained leading cybersecurity experts and experienced cybersecurity legal counsel. With their help, we determined that an unknown third party initially accessed our network on or around February 21, 2022. We also confirmed that we eradicated the underlying unauthorized access to our systems on March 11, 2022. We then began investigating what, if any, sensitive personal information may have been accessed or acquired in connection with the incident.

What Information Was Involved? Unfortunately, as of the close of our investigation, we could not confirm if your sensitive personal information was potentially impacted in connection with the incident. However, we note that ATG collects certain sensitive personal information in our normal course of business human resources functions, which may include your name, date of birth, Social Security number, government identification numbers (*e.g.*, passports, driver's license and military identification numbers, etc.), and financial account numbers (*e.g.*, provided to ATG for direct deposit purposes). As such, because ATG values its workforce, and out of an abundance of caution, we are providing you with this notification and offering you credit monitoring and identity protection services, as described below. We are not aware of any malicious misuse of any information, including your sensitive personal information, as a result of the event.

What We Are Doing. ATG swiftly responded once it became aware of the event. When we learned of the incident, we decided to proactively disconnect ATG servers, networks, and applications to contain the issue and maintain the safety of our systems. We then took additional steps to enhance our security posture, including resetting network and administrative passwords and deploying additional endpoint detection and response technology. In addition, we also contacted and worked with law enforcement agencies and regulators following the incident.

As stated above, out of an abundance of caution, we are providing you access to credit monitoring and identity protection services through Equifax. For more information on how to sign up for complimentary 24-month protection, please see the attached *Steps You Can Take to Help Protect Personal Information.*

What You Can Do. While our investigation could not confirm that the incident impacted your sensitive personal information, we nevertheless encourage you to remain vigilant against identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and errors. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information.* To take advantage of the complimentary identity protection offered by Equifax, you will need to complete the activation process described therein. Your personalized activation information is below:

Your Activation Code: **<<Activation Code>>**
Your Enrollment Deadline: **May 31st, 2023**

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please ca

Sincerely,

[redacted]

Maggie Drozd
SVP, General Counsel
Apex Tool Group, LLC

Steps You Can Take to Help Protect Personal Information

Enroll in Credit Monitoring

Go to www.equifax.com/activate, enter your unique activation code, and complete the following steps:

1. Register:
   a. Complete the form with your contact information and click "Continue."
   b. If you already have an Equifax account, click the 'Sign in here' link under the "Let's get started" header.
   c. Once you have successfully signed in, you will skip to Step 4 ("Checkout").
2. Create Account:
   a. Enter your email address, create a password, and accept the terms of use.
3. Verify Identity:
   a. To enroll in your product, we will ask you to complete our identity verification process.
4. Checkout:
   a. Upon successful verification of your identity, you will see the Checkout Page.
   b. Click 'Sign Me Up' to finish enrolling.
5. You're done!
   a. The confirmation page shows your completed enrollment.
   b. Click "View My Product" to access the product features.

Review Your Credit Reports

We recommend you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

Place a Fraud Alert or Credit Freeze

Consumers can place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business must verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. If you wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to control who can access your personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover their information has been misused to file a complaint. You can obtain further information on filing such a complaint by using the contact information listed above.

You can file a police report if you experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state md.us.

For New Mexico residents, 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 bureaus 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 the violator. 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 by visiting 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 New York residents, the New York Attorney General may be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www ncdoj.gov.

For Oregon residents, the Oregon Department of Justice may be reached at 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.