

ALESSANDRA V. SWANSON
Partner
(312) 558-7435
ASwanson@winston.com

VIA EMAIL

May 30, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Notice of Privacy Incident

To Whom It May Concern:

Winston & Strawn LLP (“Winston”) represents Drilling Tools International, Inc. (“DTI”), 3701 Briarpark Drive, Suite 150, Houston, TX 77042, with respect to the privacy incident that is the subject of this letter (the “Privacy Incident”). I am writing to inform this office of the Privacy Incident pursuant to Maryland law, as it potentially impacted one (1) Maryland resident.

By way of background, on December 19, 2023, DTI detected a potential issue within its information technology systems. Out of an abundance of caution, DTI made the decision to proactively disconnect its systems to contain the potential issue and maintain the safety of its systems. DTI’s cybersecurity event response procedures were immediately enacted, which included engaging legal counsel and cybersecurity experts to help undertake a thorough investigation into the event.

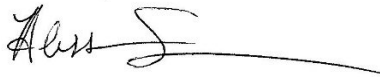
Through its investigation into the Privacy Incident, DTI determined that an unknown third party accessed its systems beginning on or around November 20, 2023 through December 19, 2023. DTI’s findings to date have further indicated that certain human resources files may have been impacted by the Privacy Incident. As of April 23, 2024, DTI confirmed that these files included sensitive personal information related to certain former and current DTI workforce members and/or their beneficiaries. This sensitive personal information may have included data that is collected by DTI in the normal course of human resources operations, such as name, Social Security number, government ID (such as a passport, driver’s license or other government-issued ID), financial account information and health or medical information, which may include health insurance identification numbers. Of note, DTI is not aware of any malicious misuse of any sensitive personal information as a result of the Privacy Incident.

On May 29, 2024, DTI mailed a notification letter to the individual in Maryland who may have had sensitive personal information impacted by the Privacy Incident; it is anticipated that the individual will receive this letter in the coming days. A sample notification letter is attached as Exhibit 1. In addition, DTI offered this individual credit monitoring and identity protection services through TransUnion. DTI also implemented additional safeguards and technical security measures to further protect and monitor their systems to help protect against a similar event from occurring.

By providing the information in this letter, DTI expressly reserves all available rights, defenses, and privileges in connection with the Privacy Incident. Furthermore, DTI 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 DTI's objection that Maryland lacks personal jurisdiction with respect to the Privacy Incident.

It is my hope that this information will satisfy this office's need for information related to the Privacy Incident. However, if this office requires any additional details, please contact me by telephone at (312) 558-7435 or via email at ASwanson@winston.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Aless S', followed by a long horizontal flourish line.

Alessandra V. Swanson

Exhibit: Sample Notification Letter

EXHIBIT 1
Sample Notification Letter

Drilling Tools International
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08534 -



May 29, 2024

Dear [REDACTED],

Drilling Tools International ("DTI") is notifying you about an event that may have involved some of your sensitive personal information. This notice explains the event, our response, and the additional steps you can take to protect your information, should you feel it necessary to do so.

On December 19, 2023, DTI detected a potential issue within our information technology systems. Out of an abundance of caution, we made the decision to proactively disconnect our systems to contain the potential issue and maintain the safety of our systems. Our cybersecurity event response procedures were immediately enacted, which included engaging legal counsel and cybersecurity experts to help undertake a thorough investigation into the event. With their help, we determined that an unknown third party accessed our systems beginning on or around November 20, 2023 through December 19, 2023. We also began an investigation to determine what, if any, sensitive personal information may have been affected by the event.

Our findings to date have indicated that certain human resources files may have been impacted by the event. On April 23, 2024, we confirmed that these files included some of your sensitive personal information. This sensitive personal information was collected by DTI from DTI workforce members in the normal course of human resources operations, including enrollment in certain benefits, and includes your



We are not currently aware of any malicious misuse of any information, including your sensitive personal information, as a result of the event. In addition, to help prevent something like this from happening again, we implemented additional safeguards and technical security measures to further protect and monitor our systems. However, out of an abundance of caution, we have secured Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in these services, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted, please provide the following unique code: [REDACTED]. In order to receive the monitoring services, you must enroll within 90 days from the date of this letter. The enrollment requires an Internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We also encourage you to remain vigilant to the possibility of fraud by reviewing your account statements and monitoring free credit reports for any unauthorized activity and reporting any such activity. Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

We understand that you may have questions about this event that are not addressed in this letter. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the representative with your unique code listed above.

Sincerely,

Leadership Team
Drilling Tools International, Inc.

ADDITIONAL RESOURCES

Review Account Statements and Credit Reports

We recommend you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, a consumer may be entitled every 12 months to one free copy of the consumer's 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. Consumers may wish to stagger their requests so that they receive free reports from one of the three credit bureaus every four months.

Place a Fraud Alert or Credit Freeze

A consumer 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. Victims of identity theft may be entitled to an extended fraud alert, which is a fraud alert lasting seven years. To place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, a consumer has 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 the consumer's name without the consumer's consent. However, please be aware that using a credit freeze to control who can access a consumer's personal and financial information in the consumer's credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application the consumer makes regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, a consumer cannot be charged to place or lift a credit freeze on your credit report. The following information will need to be provided to request a credit freeze: (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 the consumer is a victim of identity theft.

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

Other Steps You Can Take

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. In particular, the Federal Trade Commission 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 below.

You can file a police report in the event of 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 of the identity theft. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

For Residents of Maryland: The Maryland Attorney General may be contacted at 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; and consumer@oag.state.md.us.

For Residents of North Carolina: 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 Residents of New York: The Office of the New York State Attorney General may be contacted at 1-800-771-7755 or <https://ag.ny.gov/contact-attorney-general-letitia-james>.

For Residents of West Virginia: A consumer has the right to ask that nationwide consumer reporting agencies place "fraud alerts" in the consumer's file to let potential creditors and others know that the consumer may be a victim of identity theft, as described above. A consumer also has the right to place a security freeze on the consumer's credit report, as described above.

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.

A Summary of Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The major rights under the FCRA are summarized as follows: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file; (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited; (8) You must give your consent for reports to be provided to employers; (9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (10) You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization; (11) You may seek damages from violators; and (12) Identity theft victims and active-duty military personnel have additional rights. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.