JacksonLewis

Jackson Lewis P.C.
Park Center Plaza I, Suite 400
6100 Oak Tree Blvd.
Cleveland, OH 44131
(216) 750-0404 Main
(216) 750-0826 Fax
www.jacksonlewis.com

VIA FIRST-CLASS MAIL
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification[1]

May 2, 2023

Dear Sir or Madam:

We are writing to notify your office of a criminal cyberattack impacting Morristown Drivers Service, Inc. ("MDS"). MDS was the subject of a criminal ransomware attack (the "Incident") that may have impacted certain files containing personally identifiable information ("PII"). MDS immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope, the impact on its information systems, and the identities of those the Incident may have affected.

On or about February 27, 2022, we determined that the threat actor(s) may have accessed PII in the affected files from the period of January 11-13, 2023. The affected files may have contained . We have found no evidence that this information was misused.

The investigation identified one (1) New Hampshire resident that may have been affected. Out of an abundance of caution, and in accordance with applicable law, we provided notice to the affected individual on or around April 7, 2023, in the form enclosed as Exhibit A, so that they could take steps to minimize the risk that their information will be misused.

As set forth in the enclosed letter, MDS has taken numerous steps to protect the security of the personal information under its control and to prevent the occurrence of similar future incidents. Since discovering the Incident, MDS has reset all passwords, installed and hardened new firewalls, installed new EDR software with ransomware detection, installed new network analytics tools, hardened virtual server clusters, implemented encrypted offsite backups, and is in the process of reviewing and updating its existing data security policies and procedures.

[1] Please note that, by providing this letter, MDS is not agreeing to the jurisdiction of the State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent actions.

MDS will continue to monitor this situation and will update you on any significant developments. If you require any additional information on this matter, please contact me.

Sincerely,

JACKSON LEWIS, P.C.
/s/ Jackson E. Biesecker

Morristown Drivers Service, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

April 7, 2023

Notice of Data Breach

Dear [redacted],

As a current or former employee of Morristown Drivers Service, Inc. (the "Company") we are writing to notify you of a data incident that may have involved your personal information.

What Happened

The Company was subject to a criminal cybersecurity attack on or around January 13, 2023 (the "Incident"). With assistance from third-party experts, the Company took immediate steps to secure its systems and investigate the nature and scope of the Incident. Through its investigation, the Company discovered that the Incident may have impacted personally identifiable information ("PII") related to you. We have found no evidence that your information was misused.

What Information Was Involved

The Incident may have resulted in unauthorized access to or acquisition of certain files that may have contained one or more of the following data elements: .

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we are also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services to help mitigate any potential for harm at no cost to you. Please see below for more information on enrollment in these services.

The Company endeavors to protect the privacy and security of sensitive information. We have worked diligently to determine how this incident happened and are taking appropriate measures to prevent a similar situation in the future. Since the Incident we have implemented a series of cybersecurity enhancements, including installation of additional endpoint detection and response software, installation of new firewalls, implementation of additional threat analysis protocols, and rebuilding affected servers.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Can Do

As with any data incident, we recommend that you remain vigilant and consider taking steps to avoid identity theft, obtain additional information, and protect your personal information. Common passwords or passwords you may be using on multiple accounts should be updated to new complex passwords for added security. The attached sheet describes additional steps you can take to protect your identity and personal information.

As an added precaution, we have arranged for credit monitoring services at no charge. These services provide you with alerts for [redacted] months from the date of enrollment when changes occur to your TransUnion 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll, please visit https://secure.identityforce.com/benefit/morristownds and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. To receive these services, please be sure to enroll by July 5, 2023. 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.

For More Information

If you have questions or concerns, please call our dedicated assistance line at , from 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. You will need to reference the enrollment code above when calling or enrolling online, so please do not discard this letter.

We sincerely apologize for this situation and any inconvenience it may cause you.

Sincerely,

Coleton Bragg
General Counsel
Morristown Drivers Service, Inc.

(Enclosure)

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

Recommended Steps to help Protect your Information

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

- Order Your Free Credit Report at www.annualcreditreport.com, call toll-free at , or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information.

- Place a Fraud Alert on Your Credit File. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

Equifax	P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

- If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

- The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

- *For District of Columbia Residents:* You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

- *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

- *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf

- *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

- *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

- *For Rhode Island Residents:* You may contact and obtain information from and/or report identity theft to your state attorney general at:

  Rhode Island Attorney General's Office
  150 South Main Street
  Providence, RI 02903
  Phone: (401) 274-4400
  Website: www.riag.ri.gov

  You have the right to obtain a copy of the applicable police report, if any, relating to this incident.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION