EXHIBIT 1

By providing this notice, Hilldrup Companies, Inc. ("Hilldrup") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On December 18, 2020, Hilldrup identified the presence of malware on certain computer systems in its environment. Hilldrup immediately commenced an investigation, with the assistance of third-party computer forensic specialists, to determine the full nature and scope of the incident and to secure its network. Through this investigation, Hilldrup determined that in connection with the malware event, an unknown actor accessed certain systems within its network on or about December 18, 2020. As a result, the unknown actor acquired certain information regarding current and former employees located within these systems. Hilldrup then worked with specialists to conduct a comprehensive review of the impacted systems to confirm the information acquired by the unknown actor and the identities of the impacted individuals. On or about March 24, 2021, Hilldrup's review first determined that certain employee data was present in the affected systems and was acquired by the unknown actor. Hilldrup then worked until April 11, 2021 to confirm the identities of the impacted individuals, prepare the formal written notification, and locate the necessary mailing address information. Hilldrup then moved quickly to provide notice to affected individuals.

The information impacted by this event varies by individual and for the Maine resident includes name and Social Security number.

Notice to Maine Resident

On April 27, 2021, Hilldrup began providing written notice of this incident to the affected individuals, which includes approximately one (1) Maine resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Hilldrup moved quickly to investigate and respond to the incident, assess the security of its systems, and identify and notify the affected individuals. Hilldrup also worked to implement additional safeguards and training to its employees. Hilldrup is providing written notice to those individuals who may be affected by this event. This notice includes an offer of complimentary access to credit monitoring and identity restoration services for twelve (12) months through TransUnion, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident.

Additionally, Hilldrup is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Hilldrup is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Hilldrup reported this event to federal law enforcement and cooperated with its investigation. Hilldrup also notified other state regulators, as appropriate.

EXHIBIT A

Hilldrup
Moving, Storage, Relocation & Logistics

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>>

Re: Notice of Data <<Variable Text 1>>

Dear <<Name 1>>:

Hilldrup Companies, Inc. ("Hilldrup") writes to inform you of an incident that may affect the security of some of your information. We are providing you with an overview of the incident, our response, and steps you may take to better protect yourself, should you wish to do so.

What Happened? On December 18, 2020, Hilldrup identified the presence of malware on certain computer systems in our environment. We immediately commenced an investigation to determine the full nature and scope of the incident and to secure our network. Through this investigation, we determined that in connection with the malware event, an unknown actor accessed certain systems within our network on or about December 18, 2020. As a result, the unknown actor acquired certain information regarding current and former employees located within these systems.

What Information Was Involved? We conducted a thorough review of the relevant systems to identify the types of information stored there and to whom it related. On or about March 24, 2021, our review first determined that certain employee information was present in the affected systems and was acquired by the unknown actor. We worked from that date until April 11, 2021 to confirm the identities of the impacted individuals, prepare the formal written notification, and locate the necessary mailing address information. The information impacted by this event included your name and <<Variable Text 2>>. While we have received no reports that identity theft or unauthorized use of the affected information has occurred, we are making you aware of this incident in an abundance of caution.

What We Are Doing. Hilldrup has strict security measures to protect the information in our possession, and we have implemented additional administrative and technical safeguards in our environment to further enhance our security posture. We are also implementing additional training and education to our employees to prevent similar future incidents.

As an added precaution, we are also offering you complimentary access to <<Variable Text 3>> months of credit monitoring and identity theft restoration services, through Epiq. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Your Information*." You may also activate the complimentary credit and identity monitoring services we are offering. Enrollment instructions are attached to this letter.

For More Information. If you have additional questions, please call 855-654-0935 between the hours of 9:00 a.m. and 9:00 p.m., Eastern Time, Monday through Friday (excluding U.S. holidays). You may also write to Hilldrup at 4022 Jefferson Davis Highway, Stafford, VA 22554.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Russ Watson

Russ Watson
Executive Vice President & Chief Administrative Officer
Hilldrup Companies, Inc.

Steps You Can Take to Help Protect Your Information

Enroll in Credit and Identity Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<Variable Text 3>> months provided through Epiq, by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR <<Variable Text>>-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<Variable Text 3>> months of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to 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. Should you wish to place a fraud alert, please contact any one 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 take control over who gets access to the 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 security 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, military identification, 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 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
888-298-0045	1-888-397-3742	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 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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order 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, D.C. 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. Hilldrup Companies, Inc. is located at 4022 Jefferson Davis Highway, Stafford, VA 22554.

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

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident.