EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Corval Group, Inc. ("Corval") located at 1633 Eustis Street, St. Paul, Minnesota 55108 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 November 16, 2020, a laptop was stolen out of a Corval employee's car. The employee reported the theft to Corval and Corval immediately began an investigation to determine the exact information that may have been stored on the laptop. Corval also reported the theft to local law enforcement. The investigation determined that personal information for a limited number of individuals may have been stored on the laptop. Although there is no evidence that any unauthorized individual has accessed or misused any of the personal information stored on the device, out of an abundance of caution, Corval is taking steps to notify individuals whose information may have been stored on the stolen laptop. Upon receipt of the list of individuals affected, Corval reviewed its internal records to confirm the identities and contact information for these individuals to ensure notification was provided as soon as possible. This internal review was completed on or about January 4, 2021. Our investigation into this event is ongoing, and additional information will be communicated, as needed.

The Maine resident's information that could have been subject to unauthorized access includes name, address, and financial account information.

Notice to Maine Resident

On or about January 26, 2021, Corval provided written notice of this incident to affected individuals, which includes 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, Corval moved quickly to investigate and respond to the incident, assess the security of Corval systems, and notify potentially affected individuals. Corval is also working to implement additional safeguards and training to its employees. Corval is providing access to credit monitoring services for 12 months through TransUnion to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Corval 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. Corval 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.

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 Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Corval Group, Inc. ("Corval") writes to inform you of a recent event that may affect the security of some of your personal information. While we are unaware of any actual or attempted misuse of your personal information, out of an abundance of caution, we are providing you with information about the incident, steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened? On November 16, 2020, a laptop was stolen out of a Corval employee's car. The employee reported the theft to Corval and we immediately began an investigation to determine the exact information that may have been stored on the laptop. This included reviewing the contents of the laptop to confirm what, if any, sensitive personal information may have been stored on the device. This review was completed on or about January 8, 2021. We also reported the theft to local law enforcement.

The investigation determined that personal information for a limited number of individuals may have been stored on the laptop. Although there is no evidence that any unauthorized individual has accessed or misused any of the personal information stored on the device, out of an abundance of caution, Corval is taking steps to notify individuals whose information may have been stored on the stolen laptop. Our investigation into this event is ongoing, and additional information will be communicated, as needed.

What Information Was Involved? The investigation determined that the stolen laptop may have contained information relating to you, including your <<b2b_text_1(DataElements)>>. At this time, we are unaware of any actual or attempted misuse of your information, and we are notifying you out of an abundance of caution.

What is Corval Doing? We take this matter, and the security and privacy of the sensitive information in our care very seriously. Upon learning of the theft, we immediately contacted law enforcement and began an investigation to determine what, if any, sensitive information may have been stored on the laptop. We are also reviewing our internal security policies and procedures.

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **April 27, 2021** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

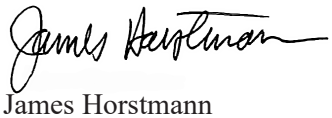
Additional information describing your services is included with this letter.

What Can You Do? You can activate the complimentary credit monitoring and identity restoration services we are offering. You can also review the included *Steps You Can Take to Safeguard Against Identity Theft and Fraud* for additional information on safeguarding against the misuse of your information.

For More Information. We understand you may have questions relating to this event and this letter. You can contact our dedicated assistance line at 1-XXX-XXX-XXXX Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time for any questions or concerns regarding this incident.

We apologize for any inconvenience this incident may cause you and remain committed to the privacy and security of information in our possession.

Sincerely,



James Horstmann
Chief Financial Officer
Corval Group Inc.

Steps You Can Take to Safeguard Against Identity Theft and Fraud

Monitor Your Accounts

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

You have the 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. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
www.equifax.com/personal/credit-report-services

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com/personal/credit-report-services

Additional Information

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). 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 California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For District of Columbia residents, the Office of the District of Columbia Attorney General can be contacted at 400 6th Street, NW, Washington, DC 20001; Phone (202) 727-3400; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: oag@dc.gov; or you may visit the website of the Office of the District of Columbia Attorney General at https://oag.dc.gov/.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or 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 agencies 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 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 Attorney General can be contacted at: 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 Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; or www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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

Kroll | A Division of DUFF&PHELPS

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 will 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.

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.