Kathleen B. Rice
kathleen.rice@faegrebd.com
Direct **+1 574 239 1958**

Faegre Baker Daniels LLP
202 South Michigan Street ▾ Suite 1400
South Bend ▾ Indiana 46601-2020
Main **+1 574 234 4149**
Fax **+1 574 239 1900**

April 24, 2017

VIA OVERNIGHT MAIL

Attorney General Joseph Foster
Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capital Street
Concord, NH 03301

Re: Notice of Security Incident

Dear Attorney General Foster:

We represent Donaldson Company, Inc. ("Donaldson"), and, pursuant to applicable state law, are writing on their behalf to notify you of a security incident involving the personal information of two residents of the state of New Hampshire.

On March 24, 2017, a Donaldson employee's company-issued, user ID and password-protected laptop was stolen from the employee's vehicle while it was located off Donaldson's premises. On March 29, 2017, Donaldson discovered that the laptop contained, in electronic form, certain Donaldson employees' personal information, specifically employee hiring information, employee number, name, birthdate, Social Security number, citizenship, and address.

The incident involved the personal information of 4,487 individuals, including two residents of the state of New Hampshire. Pursuant to state law, notice will be provided in writing, via U.S. mail, on April 24, 2017, to two state residents whose personal information was involved in the incident. A sample notice is attached hereto and includes information regarding the incident, how to protect against future fraudulent activity, and specific contact information for the national credit bureaus and the Federal Trade Commission.

Law enforcement has been notified of this theft and it is our understanding that their investigation continues. Donaldson promptly undertook an investigation, including working with third party computer service providers, to determine the nature of the information involved in this incident and to further protect personal information that Donaldson maintains from potential compromise. At this time,

we have no evidence that the personal information involved in this incident has been used for fraudulent purposes. Donaldson is notifying all affected employees and providing information to help them remain vigilant against any fraudulent activity, including one year of free identity theft protection services. Donaldson is also reviewing its policies and practices with respect to handling of personal information, including employee access to such information, to ensure similar incidents do not occur in the future.

If you have any questions or need further information, please contact me at (574) 239-1958, or kathleen.rice@faegrebd.com.

Very truly yours,

Kathleen B. Rice
Counsel

RICEK01

Enclosure

[Company Letterhead] [Notice must be in no smaller than 10-point font]

[Date]

(First Name)
(Address)
(City), (State) (Zip)

RE: Notice of an Incident Involving Your Personal Information

Dear (Name):

I am writing on behalf of Donaldson to inform you of an incident that may have involved your personal information. This letter provides you with information on the steps Donaldson has taken and the services Donaldson is offering to further guard against the misappropriation and misuse of your personal data.

What Happened? A Donaldson employee's company-issued laptop containing personal information related to you and others was stolen from a personal vehicle on March 24, 2017. We learned on March 29, 2017, that your personal information may have been involved and we immediately launched an investigation to determine the nature and scope of this event. We are working with appropriate third parties, including law enforcement, to assist with these efforts. Based on what we know so far, we do not have any reason to believe that your personal information, or anyone else's, was accessed at any time after the laptop was stolen.

What Personal Information Was Involved? The incident involved the following information: your name, address, birthdate, and Social Security number.

What We Are Doing? While we believe the risk your data will be accessed or compromised is low, we take the security of your personal information very seriously. Law enforcement is involved and a police report was filed. We are reviewing and improving our data handling policies and practices. Specifically, we are making improvements to the ways in which we store, transmit, and access personal information. Moreover, we are implementing enhanced training procedures to mitigate the risk of further incidents and unauthorized access to personal information.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call «DID_Phone» and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling «DID_Phone» using the following redemption code: {RedemptionCode}.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

What Can You Do? You can review the enclosed *Preventing Identity Theft and Fraud* for more information on ways to protect against the potential misuse of your information. You can also enroll to receive the credit monitoring services we are offering at no cost.

Again, we take the security of your information in our care very seriously and we regret any concern or inconvenience this incident may cause you. If you have additional questions, please call our dedicated assistance line at [ALLCLEAR DID], Monday through Saturday, 8 am – 8 pm CT.

Sincerely,

Sheila Kramer
Vice President, Human Resources

PREVENTING IDENTITY THEFT AND FRAUD

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. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office or state Attorney General and file a report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records and also to access some services that are free to identity theft victims.

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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-766-0008
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion
PO Box 2000
Chester, PA 19022-2000
1-888-680-7289
https://www.transunion.com/credit-freeze/place-credit-freeze

In order to request a security freeze, you will need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement to show proof of your current address. 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. If you are not a victim of theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail. Fees vary based on where you live, but commonly range from $5 to $20.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number and password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or individuals or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself by contacting 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); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement or your state Attorney General. The mailing of this notice was not delayed by law enforcement.

State-Specific Information

Rhode Island residents:

- Have a right to file and obtain a police report. If the police report is then provided to a credit bureau, it cannot charge you to place, lift, or remove a security freeze.
- Have the right to know that, to date, one Rhode Island resident has been identified as potentially affected by this incident.
- May contact the RI Attorney General's Office at (401) 274-4400, http://www.riag.ri.gov/, or 150 South Main Street, Providence, RI 02903, for additional information about preventing identity theft.

North Carolina residents:

- May contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077