Exhibit A

[redacted]

From: Carl James <cjames@bdi-usa.com>
Sent: Friday, March 30, 2018 6:21 PM
To: Carl James
Cc: Carl James
Subject: Potential Data Breach

Dear BDI Employees:

At approximately 4:46 pm on Friday, March 30, 2018, Bearing Distributors, Inc. (BDI) may have incurred a data breach. We have notified the IRS and all State Tax Agencies and the FBI Internet Crime Complaint Center. We have received an acknowledgement of our complaint from the Federation of State Tax Administrators and the FBI. At this time no other information is known as to the scope or effectiveness of the breach. Being a holiday weekend we may not have more information until later in the weekend or Monday.

We are investigating what credit monitoring can be provided as soon as possible. In the meantime, each of us should consider the following recommended steps from both the IRS and the Federal Trade Commission to protect ourselves. We are not authorized to do these steps on your behalf:

1. Consider placing a credit freeze with each of the following three (3) credit agencies. A credit freeze makes it more difficult for someone to open a new account in your name. If you decide not to place a credit freeze, consider placing a fraud alert with these credit agencies. This can be done online at the following internet sites or telephone numbers:

   www.Equifax.com/CreditReportAssistance or 1-800-525-6285
   www.Experian.com/fraudalert or 1-888-397-3742
   www.TransUnion.com/fraud or call 1-800-680-7289

2. Do not give any information to anyone-by phone, email, text-or in person. Do not believe anyone who calls, emails or texts you and/or threatens you to provide personal information or to make any payments for any reason.

We will update you as soon as additional information or instruction is known.

Sincerely,

Carl James
President and CEO

Mobile; 1-330-719-7714

[redacted]

From: Carl James <cjames@bdi-usa.com>
Sent: Saturday, March 31, 2018 4:15 PM
To: Carl James
Cc: Carl James
Subject: BDI Data Breach Updated Communication

TO: Team Members Employed by Bearing Distributors, Inc. (BDI) in 2017

DATE: March 31, 2018

RE: Follow-Up Communication Regarding Data Security Incident

We write as a follow up to our March 30, 2018 email communication, to provide additional information about the data security incident. As you are aware, on Friday, March 30, 2018, BDI was the victim of an email spoofing attack by an individual pretending to be me, BDI's President and CEO. A request was made from what appeared to be a legitimate BDI email address for 2017 employee W-2 information. Copies of 2017 employee IRS W-2 forms were obtained before we discovered that the request was made from a fraudulent account. We discovered the fraudulent nature of the request within minutes and have been working tirelessly to investigate and to mitigate the impact of the attack.

Please note that this incident affects you only if you were employed by BDI in 2017. If your employment did not begin with BDI until 2018, then your information has not been impacted.

The confidentiality, privacy, and security of our employee information is one of our highest priorities. While our investigation is ongoing, we felt it important to provide you with additional information about this incident; and, what we are doing to investigate and respond, as quickly as possible. Here are some actions that we are taking and that we encourage you to take:

- Identity Protection. As a precaution, for those individuals affected by this incident, we are arranging to provide complimentary (free) access to credit monitoring and identity restoration services. As it is a holiday weekend, we will provide instructions for enrolling in these services by close of business Monday, April 2, 2018. ***We strongly encourage you to act to take advantage of these free identity protections services.*** It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service. Branch and Department Leaders will provide time on Monday for to each of us to do this. Help will be available from the support desk if needed.
- Notice to Affected Individuals. We will be mailing information to all impacted current and former BDI team members.
- Notice to Law Enforcement and the IRS. We notified federal and local law enforcement of the incident, and we will be notifying any necessary state Attorneys General as well. We look forward to cooperating with the FBI and state law enforcement agencies in their investigations of this incident. We also are reporting this incident to the IRS and state tax authorities so that they may take steps to monitor for attempts to file fraudulent tax returns using BDI employee information.
- Filing of 2017 Tax Returns. ***We encourage you to file your 2017 tax return as soon as possible, if you have not already done so.*** You can contact the IRS at http://www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information. You should discuss

with your accountant and the IRS whether you should file the IRS Form 14039, Identity Theft Affidavit, with a paper copy of your return, and mail according to the instructions. A copy of this form can be found at https://www.irs.gov/pub/irs-pdf/f14039.pdf or https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

If you find that you are blocked from filing your tax return-we will have information next week on what to do.

- Employee Training. Unfortunately, even the best technology cannot prevent all cyber-attacks, particularly those designed to trick employees into providing sensitive company information. We will continue to provide, and improve upon, our information security awareness and training programs for all employees.

We apologize for any inconvenience this incident causes you. Please know that we are working diligently to remedy this incident and to prevent any similar incidents from occurring in the future. If you have any questions about the contents of this notice or about the incident, please contact me at 330-719-7714.

Sincerely,

Carl James, President/CEO

Mobile: 1-330-719-7714

[redacted]

From: Carl James
Sent: Monday, April 2, 2018 5:17 PM
To: Carl James <cjames@bdi-usa.com>
Cc: Carl James <cjames@bdi-usa.com>
Subject: Data Breach Update/Credit Monitoring Services

Dear BDI Team Members Employed in 2017:

We write as a follow up to our prior communications regarding a recent email spoofing attack that resulted in the inadvertent disclosure of 2017 BDI employee W-2 information. Per our email from Saturday, March 31, 2018 BDI is offering you as a safeguard, free access to an online three-bureau credit monitoring service (*my*TrueIdentity) for 24 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

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 following 12-letter Activation Code [redacted], 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, three-bureau 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 following 6-digit telephone pass code **697789** 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 **August 10, 2018.** 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.

Once you are enrolled, you will be able to obtain 24 months of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change 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 to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

BDI is mailing notice of this incident to the mailing address we have on file for you. In the meantime, if you have questions or concerns, please call our dedicated assistance line at **855-386-9201** (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m. ET.

Again, we sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Carl James
President and CEO

Exhibit B

Return Mail Processing Center
PO 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 Breach

Dear <<Name 1>>:

Bearing Distributors, Inc. (BDI) is writing as a follow up to our prior communications regarding the recent data security incident that affects the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can better protect against the possibility of misuse of your personal information, should you feel it is appropriate to do so.

What Happened? On March 30, 2018, we discovered that our company was the victim of an email spoofing attack that same day by an individual pretending to be our President and CEO. A request was made from what appeared to be a legitimate BDI email address for 2017 employee W-2 information. Unfortunately, copies of 2017 employee IRS W-2 forms were provided before we discovered that the request was made from a fraudulent account. We discovered the fraudulent nature of the request within minutes on March 30, 2018 and have been working tirelessly to investigate and to mitigate the impact of the attack and communicate with you regarding the incident.

What Information Was Involved? A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information related to you as a BDI employee: (1) name; (2) address; (3) Social Security number; and (4) wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. BDI has stringent security measures in place to protect the security of information in our possession. At this time, we do not believe that the individual who sent the fraudulent email accessed our computer network or that our IT systems were otherwise compromised by this attack. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We have contacted the IRS, state taxing authorities, FBI, and local law enforcement regarding this incident. We will also be notifying state Attorneys General, as required.

As a precaution, BDI is providing you with access to 24 months of complimentary credit monitoring and identity restoration services through TransUnion. The cost of this service will be paid for by BDI. To the extent you have not already done so, it is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. You can review the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud*. You can also enroll to receive the free credit monitoring and identity restoration services described above, to the extent you have not already done so.

In addition, if you have not already done so, we encourage you to file your 2017 tax return as soon as possible. If you become aware of a fraudulent tax return filed in your name, you should discuss with your accountant and the IRS whether you should file the IRS Form 14039, Identity Theft Affidavit, with a paper copy of your return, and mail according to the instructions. A copy of this form can be found at: https://www.irs.gov/pub/irs-pdf/f14039.pdf, or https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 855-386-9201 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m. ET.

BDI takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Carl James
President and CEO
Mobile Phone: 1-330-719-7714

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Monitoring. As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*my*TrueIdentity) for 24 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

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 following 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, three-bureau 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 following 6-digit telephone pass code **<<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 **<<Insert Date>>**. 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.

Once you are enrolled, you will be able to obtain 24 months of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change 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 to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

File Your Tax Return. We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit http://www.taxadmin.org/state-tax-agencies.

Monitor Your Accounts

Credit Reports. 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, 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.

Fraud Alerts. 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 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. 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, lift, 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. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, 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 proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud 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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. Approximately one (1) Rhode Island resident may be impacted by this incident.