<<Date>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Breach

Dear <<First Name>>:

We write to share important information with you about a data security incident that has affected your personal information. We regret that this incident occurred and take the security of your personal information seriously. We are providing this notice to you so you know what we are doing and the steps you can take to protect your information should you feel it is appropriate to do so.

What Happened? We have conducted an investigation, with the assistance of a leading cybersecurity firm, into a cyberattack carried out by cyber criminals that has targeted our systems. On November 16, 2020, DJO learned that the attacker staged and likely exfiltrated a limited amount of data from DJO's systems. We investigated and reviewed the affected data and learned on November 25, 2020 that your personal information was affected. Based on our investigation, we understand that this activity occurred between November 8, 2020 and November 9, 2020. We do not believe that your personal information has been be misused against you.

What Information Was Involved? The types of personal information within the exfiltrated files varied by individual. Examples of such personal information include, but are not limited to: Name, Social Security number, driver's license number or other government-issued identification number, medical or health insurance information, benefits enrollment information, health care claims information, financial account/payment card information, birth or marriage certificate, digital/electronic signature, work-related evaluations, and date of birth.

What We Are Doing. DJO regularly reviews and updates the measures it takes to protect your personal information. In response to this incident, we have further reviewed and strengthened our data security measures to protect against further incidents. We strive to continually improve our data security and maintain a secure environment for confidential and personal information.

While, as noted above, we have no evidence that your personal information has been misused, as a precaution, we are providing you with access to 24 months of *my*TrueIdentity credit monitoring and identity restoration services at no cost to you, through Transunion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit monitoring companies.

If you enroll, you will be able to obtain an initial 3-in-1 credit report and credit scores along with 24 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. 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 dark web internet identity monitoring, the ability to lock and unlock your TransUnion credit report, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Certain policy limitations and exclusions may apply.)

What You Can Do: We encourage you to enroll in the free *my*TrueIdentity services by going to www.mytrueidentity.com and entering the following 12-letter Activation Code: <<Activation Code>>. Please note the deadline to enroll is March 31, 2021.

If you have questions about your online credit monitoring benefits, need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at 1-844-787-4607, Monday through Friday: 8:00am to 9:00pm ET, Saturday and Sunday: 8:00am through 5:00pm ET.

We encourage you to take full advantage of this service offering.

For More Information: For general questions about the incident please contact DJO's HR Direct team at HRDirect@djoglobal.com or (800) 681-1777. You also may consult the resources included on the enclosed form, which provides additional information about protecting your personal information online.

We would like to reiterate that the security of your personal information is one of our highest priorities. We sincerely regret any inconvenience caused to you by this incident.

Sincerely,

[Name]

[Title]

Steps You Can Take to Protect Against 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. 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

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

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. Under federal law, you cannot be charged to place, lift or remove a security freeze. 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. To find out more on how to place a security freeze, you can use the following contact information:

Equifax	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
800-349-9960	888-397-3742	888-909-8872

Websites:
www.equifax.com/personal/credit-report-services/credit-freeze
www.experian.com/freeze/center.html
www.transunion.com/credit-freeze

To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail.:

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, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. 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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. 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 by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or 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. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

You should also know that you have the right to file a police report if you ever experience identity 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. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission. This notice has not been delayed by law enforcement.

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 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.

District of Columbia Residents: You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
441 4th Street NW
Suite 1100 South
Washington, D.C. 20001
(202) 727-3400
https://oag.dc.gov/

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: You may obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
Telephone: 1-888-743-0023.
www.oag.state.md.us/Consumer

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 a 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. You can 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.

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General
Consumer Frauds & Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
www.ncdoj.gov

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.