WSGR Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

1700 K Street, NW, Fifth Floor
Washington, D.C. 20006-3817
PHONE 202.973.8800
FAX 202.973.8899
www.wsgr.com

December 19, 2017

Attorney General Joseph Foster
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

DJI Technology, Inc. ("DJI") cares deeply about the security of its products and protecting the privacy of its consumers. This letter is to inform you of a security breach that affected a small number of its customers, including three (3) New Hampshire residents.

On September 27, 2017, DJI was informed by an independent security researcher that data on one of DJI's servers located in the U.S. was accessible to unauthorized users. DJI took immediate steps to investigate this matter and prevent further unauthorized access. Based on a preliminary investigation, DJI believes that other individuals may have accessed the information before September 27, 2017. DJI has taken steps to remediate this issue and prevent such an intrusion from occurring in the future. DJI has also engaged an outside forensic firm to assist with the investigation, which is ongoing. Given the continuing nature of the investigation, it is possible that additional facts may come to light in the future.

The information involved includes personal information, including information contained in scanned photo identification uploaded by users to DJI's servers. Such personal information may include: full name, address, date of birth, photo, and identification number (e.g., passport number or driver's license number). At this time, DJI does not believe the information includes credit card, bank account, or other financial information. The investigation is still ongoing and if other material facts are uncovered, DJI will provide information as necessary to supplement this notification.

Enclosed is a sample notification letter, which will be sent to affected individuals soon. Please do not hesitate to contact me if you have any additional questions.

Very truly yours,

WILSON, SONSINI, GOODRICH & ROSATI
Professional Corporation

Christopher N. Olsen

NOTICE OF DATA BREACH

[DATE]

Dear [NAME],

Please read this letter as it has important information about your information. DJI Technology, Inc. ("DJI") takes the protection of your information seriously. For this reason, we are contacting you directly to explain the circumstances of an incident that may involve your information.

What Happened

On September 27, 2017, DJI was informed by an independent security researcher that data on one of DJI's servers located in the U.S. was accessible to unauthorized users. DJI took immediate steps to investigate this matter and prevent further unauthorized access. Based on a preliminary investigation, DJI believes that other individuals may have accessed the information before September 27, 2017. DJI has taken steps to remediate this issue and prevent such an intrusion from occurring in the future. DJI has also engaged an outside forensic firm to assist with the investigation, which is ongoing. Given the continuing nature of the investigation, it is possible that additional facts may come to light in the future.

What Information Was Involved

The information involved includes personal information, including information contained in scanned photo identification uploaded by users to DJI's servers. Such personal information may include: full name, address, date of birth, photo, and identification number (e.g., passport number or driver's license number). At this time, DJI does not believe the information includes credit card, bank account, or other financial information. As mentioned above, the investigation is still ongoing and if other material facts are uncovered, DJI will provide information as necessary to supplement this notification.

What Are We Doing

We are continuing to investigate this incident and are taking steps to help prevent such an incident from happening again in the future including conducting a review of technological, administrative, and physical safeguards designed to protect the security, confidentiality, and integrity of personal information and engaging a third party forensic expert.

What Can You Do

We urge you to be vigilant for incidents of fraud and identity theft and closely review or monitor your bank statements and credit reports.

Please refer to the attached Identity Protection Reference Guide that details steps you can take to help protect your information against potential misuse, including the option to place a fraud alert or a security freeze on your credit file. Below are the addresses and phone numbers for the credit reporting agencies.

Equifax	**Experian**	**TransUnion Fraud Victim Assistance Division**
P.O. Box 740241	P.O. Box 9532	P.O. Box 2000
Atlanta, Georgia 30374-0241	Allen, Texas 75013	Chester, PA 19016-2000
888-766-0008	888-397-3742	888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

You may also contact the FTC regarding issues of identity theft at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
www.ftc.gov/idtheft/

Other Important Information

Please see the below Identity Protection Reference Guide for other important information.

For More Information

If you have any questions about this incident please call (818) 235-0789. We apologize for any inconvenience this may have caused you.

Sincerely,

DJI Technology Inc.
(818) 235-0789
435 Portage Avenue, Palo Alto CA 94406

IDENTITY PROTECTION REFERENCE GUIDE

In addition to carefully reviewing your financial institution and credit card statements, we recommend that you consider the additional steps stated below.

Security Freeze

Some state laws allow you to place a fraud alert or a security freeze on your credit reports. This would prohibit a credit reporting agency from releasing any information from your credit report without your written permission. You should be aware, however, 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 believe you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, the agency cannot charge you for placing, lifting, or removing a security freeze on your credit reports. In all other cases, a credit reporting agency may charge you up to $10.00 each time you place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you may send a written request to each of the three credit reporting agencies noted below. It should include the following information:

- Full name (including middle initial as well as Jr., Sr., III, etc.);
- Social Security number;
- Date of birth;
- Addresses for the previous five (5) years;
- Proof of current address;
- A legible copy of a government issued identification card;
- A copy of any relevant police report, investigation report, or complaint to a law enforcement agency concerning identity theft; and
- If you are not a victim of identity theft, include payment by check, money order, or credit card. Do not send cash through the mail.

Equifax	**Experian**	**TransUnion Fraud Victim Assistance Division**
P.O. Box 740241	P.O. Box 9532	P.O. Box 2000
Atlanta, Georgia 30374-0241	Allen, Texas 75013	Chester, PA 19016-2000
888-766-0008	888-397-3742	888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

Free Credit Reports. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to: Annual Credit Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three national credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.

- When you receive your credit report, carefully review it. Look for accounts you did not open.

- Review the "inquiries" section and look for names of creditors from whom you have not requested credit. Be aware, however, that some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case.
- Review the "personal information" section for any inaccuracies (such as home address and Social Security number).
- If you see anything that you do not understand, call the credit bureau at the telephone number on the report.
- Errors in this information may indicate potential identity theft.
- You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.
- If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.
- If there is information on your credit report that the credit bureau cannot explain, you should call the creditors and report it to your local police or sheriff's office because it may indicate criminal activity.

Fraud Alerts. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any of the toll-free numbers of the credit reporting agencies provided above. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus.

Reporting of Identity Theft & Obtaining Police Report.
Depending on that state in which you reside, you may have a right to obtain a copy of a police report of the incident. Please note this letter has not been delayed as a result of a law enforcement investigation.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, New Mexico, Puerto Rico, and Vermont residents: Under the Fair Credit Reporting Act, you are entitled to one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of you the credit reporting agencies directly to obtain such additional report(s).

In addition, if you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authority, your state Attorney General, and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or fraudulently opened. Fill in and submit the FTC's Identity Theft Affidavit available at www.ftc.gov/idtheft when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

For more information about how to protect yourself from becoming a victim of identity theft, contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
www.ftc.gov/idtheft/

For Maryland Residents. You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina Residents. You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Iowa Residents. You are advised to report any suspected identity theft to local law enforcement or to the Iowa Attorney General.

For Oregon Residents. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.