NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
1301 McKinney, Suite 5100
Houston, Texas 77010-3095
United States of America

Tel +1 713 651 5151
Fax +1 713 651 5246

RECEIVED
MAR 2 0 2023
CONSUMER PROTECTION

March 14, 2023

Via Certified Mail
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Security Incident

Dear Sir or Madam:

I am writing on behalf of my client, Inland Technologies Holdings Inc. ("Inland"), to inform you that Inland was the target of a security incident that involved the personal information of approximately 26 New Hampshire residents.

On February 11, 2023, Inland discovered a security incident that impacted a limited number of systems. Inland launched an investigation and undertook countermeasures to contain the incident. In addition, leading cybersecurity firms were engaged to assist in responding and to conduct a thorough investigation of the incident. Inland also reported the event to law enforcement and has been supporting law enforcement's investigation.

Inland's investigation revealed that an unauthorized third party gained access to Inland's environment on February 7, 2023 via a user account. Once in the network, the unauthorized third party compromised certain credential and proceeded to deploy ransomware. While in Inland's environment, the unauthorized third party gained access to a limited portion of Inland's IT infrastructure, temporarily affecting some systems and rendering them inaccessible. Some of these systems contained personal information of Inland's, and certain Inland subsidiaries', employees. This information includes name, address, and Social Security number.

Inland notified affected residents by First Class mail on March 10, 2023, and will be offering 12 months of complimentary credit monitoring and identity theft protection services. Inland is also providing a toll-free hotline for individuals to call with any questions regarding the incident.

To prevent a similar occurrence in the future, we implemented numerous measures designed to enhance the security of our systems and data. If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Respectfully submitted,

Will Daugherty

Norton Rose Fulbright US LLP is a limited liability partnership registered under the laws of Texas.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients. Details of each entity, with certain regulatory information, are available at nortonrosefulbright.com.

[INSERT DATE]

[INSERT MAILING ADDRESS OR EMAIL]

Dear **[INSERT NAME]**,

RE: Notice of Data Security Incident

Inland Technologies and its subsidiaries Quantem Aviation Services and Integrated De-Icing Services (collectively "**Inland**") takes the privacy and security of personal information in our care seriously. Further to the communication that was sent to employees on February 15, 2023, we are writing to provide you with an update on the cybersecurity incident that Inland recently experienced and which may have impacted some of your personal information. Out of an abundance of caution, we are providing you with this letter to inform you of this incident, the steps we are taking to bolster the protection of personal information in our systems and steps that you can take to protect your information.

Why does Inland have my personal information?

As an employer, Inland collects a variety of personal information for benefits, HR, and employment-related purposes. This includes personal information of Inland employees, as well as of our subsidiaries' employees. Inland may have your personal information because you are a current or former employee of Inland or of one of our subsidiaries.

What happened?

On February 11, 2023, we discovered that an unauthorized third party gained access to a limited portion of our IT infrastructure, temporarily affecting some of our systems and rendering them inaccessible. Upon discovering this, we immediately undertook countermeasures to help prevent any further unauthorized activity. In addition, leading cybersecurity firms were engaged to assist in responding and to help conduct a thorough investigation of the incident. Inland also notified law enforcement.

The investigation revealed that an unauthorized third party accessed certain Inland systems on February 7, 2023.

What information was involved?

Inland conducted a review of the data involved and determined it contained some of your personal information, including your

What we are doing.

Upon learning of this incident, we moved quickly to respond to this incident with the assistance of third party cybersecurity experts. We are also continuing to support law enforcement's investigation. Additionally, to prevent a similar occurrence in the future, we implemented numerous measures designed to enhance the security of our systems and data.

What you can do.

Please review the "Additional Steps You Can Take" guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission

regarding identity theft protection and details regarding placing a fraud alert or security freeze on your credit file.

Furthermore, to guard against any potential misuse of your information, we are offering you **[INSERT 12 or 24 MONTHS]** months of credit monitoring services through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services on a fully complimentary basis. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

Your unique activation code to register for Cyberscout's services is:

[INSERT CODE]

To activate your account, please visit **[INSERT VENDOR'S WEBSITE]** and enter your unique activation code by **[VENDOR TO PROVIDE EXPIRY DATE]**.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-888-439-7443.

To prevent fraudulent access to your credit file, you will be subject to a verification and authentication process. You will be required to provide certain personal information such as your date of birth, address and telephone number in order to be successfully authenticated.

Upon completion of the enrollment process, you will have access to the following features:

- ✓ Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- ✓ Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- ✓ Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- ✓ Identity theft insurance of up to $1,000,000 in coverage to protect against potential damages related to identity theft and fraud
- ✓ Assistance with reading and interpreting credit reports for any possible fraud indicators.
- ✓ Assistance with answering any questions individuals may have about fraud.

For more information.

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact our dedicated call center at **[TransUnion to advise phone number]** between **[TransUnion to insert call center hours]** and one of our representatives will be happy to assist you.
Regards,

Roger Langille
Chief Executive Officer

ADDITIONAL STEPS YOU CAN TAKE

Free Credit Report. Regardless of whether you choose to take advantage of the complimentary identity monitoring, it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the three nationwide credit reporting companies is as follows

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain information from the credit reporting agencies and the FTC about security freezes.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the

nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

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. LPL Financial LLC is located at 1055 LPL Way, Fort Mill, SC 29715.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

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 Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of identity theft and obtaining a police report.
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.