

DUSTIN BERGER
Associate
(303) 352-1115
berger.dustin@dorsey.com

November 14, 2024

VIA ELECTRONIC MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Sir or Madam:

Dorsey & Whitney LLP represents Maxar Space LLC and Maxar Space Robotics LLC (Maxar) in connection with a recent security incident. We write on behalf of Maxar to provide the statutorily required notification of a data breach resulting from the security incident.

Description of Security Incident

Maxar's information security team learned that a hacker using a Hong Kong-based IP address targeted and accessed a system containing files with employee personal data. When Maxar became aware of this on October 11, 2024, it took immediate action to prevent further unauthorized access to the system. It also alerted and coordinated with law enforcement regarding the incident. Nevertheless, according to Maxar's investigation, the hacker likely had access to the files on the system from October 4, 2024 to October 11, 2024.

Number of Affected Residents & Information Involved

The incident involved the personal information of nine Maryland residents. The incident involved the compromise of files containing the following categories of personal data:

- Name
- Home address
- Social security number
- Business contact information (business phone, location, business email, etc.)
- Gender
- Employment status
- Employee number
- Job title
- Hire date, role start date, and, if applicable, termination date
- Supervisor
- Department

November 14, 2024
Page 2

The security incident did not involve any compromise of bank account information, dates of birth, or tax withholding information.

Remedial Steps Taken

Maxar subsequently decommissioned the affected system and moved the files involved to a new system that is not affected by the vulnerability involved in the security incident. Maxar is also in the process of scanning other servers for vulnerabilities.

Maxar has also retained a third-party information security consultant to assist it in searching the affected system for indicators of compromise and to help Maxar verify its conclusions regarding the scope of the security incident.

In addition, Maxar provided an informal email notification to all current employees on October 26, 2024 (approximately 90% of the affected individuals) to apprise them of the security incident and to provide information that they can use to protect themselves regarding the data breach. In particular, Maxar recommended that employees take advantage of IDShield, a credit monitoring and identity theft protection service already provided to employees as part of their employment benefits (at no cost to the employees). Former employees and departing employees will be provided with identity theft protection and credit monitoring through IDX. This coverage will be for 12 months for affected individuals in Maryland. Concurrent with this submittal, we are notifying all affected individuals via post, as described in the Individual Notification Information section below.

Maxar's technical investigation of the incident is ongoing. Maxar anticipates that, once the investigation completes, it will determine whether broader adjustments or changes are needed to its information security program.

We attaching a sample of the notification letter that is being concurrently sent to affected individuals.

For more information, please contact us at:

Dustin Berger
Dorsey & Whitney LLP (Denver)
Berger.Dustin@dorsey.com
720-261-0142

Alex Hontos
Dorsey & Whitney LLP (Minneapolis)
Hontos.Alex@dorsey.com
612-492-6634

Very truly yours,

November 14, 2024
Page 3

DORSEY & WHITNEY LLP


Dustin Berger
Associate

DB:mg

Attachment: Sample Data Breach Notification Letter

MAXAR SPACE SYSTEMS
P.O. Box 989728
West Sacramento, CA 95798-9728



November 15, 2024

Notice of Data Breach

Dear [REDACTED],

I write on behalf of Maxar Space Systems to inform you of a recent security incident involving your personal data.

What Happened

Our information security team discovered that a hacker using a Hong Kong-based IP address targeted and accessed a Maxar system containing certain files with employee personal data. When we discovered this on October 11, 2024, we took immediate action to prevent further unauthorized access to the system. Nevertheless, according to our investigation, the hacker likely had access to the files on the system for approximately one week before this action was taken.

What Information Was Involved

The files on the system contained the following categories of personal data:

- Name
- Home address
- Social security number
- Business contact information (business phone, location, business email, etc.)
- Gender
- Employment status
- Employee number
- Job title
- Hire date, role start date, and, if applicable, termination date
- Supervisor
- Department

These files did not contain any bank account information or dates of birth.

What We Are Doing

We are providing this notification to enable you to take action to protect yourself. In addition, we have notified law enforcement of the incident. As is required under the laws of some states, we note that this notification has

Enrollment Code: 12345678

To Enroll, Scan the QR Code Below:



 SCAN ME

Or Visit:
<https://app.idx.us/account-creation/protect>

not been delayed due to any law enforcement investigation. We are also taking additional actions as required by the laws of the states where residents were affected by this security incident.

In addition, we have retained an outside third party to assist us in investigating the incident and confirming that the circumstances that allowed the hacker's unauthorized access have been fully and permanently eliminated.

What You Can Do

In line with best practices, we strongly encourage you to take steps to protect yourself from identity theft and other misuse of your personal information:

1. Closely monitor your financial accounts, particularly including your account statements, and promptly contact your financial institution if you notice any unusual activity. You may also wish to contact your credit or debit card issuer to determine whether a new card should be issued and whether additional security or protective measures should be placed on your account(s).
 - Current Maxar employees should strongly consider enrolling in IDShield identity protection, which includes credit monitoring. Maxar pays for the cost of this service. You can connect with IDShield at <https://www.idshield.com/> or by phone at 1-833-690-6121. Maxar is also providing former employees with a full year (or longer, where required by law) of credit report monitoring.
 - For former Maxar employees, Maxar is offering identity protection and credit monitoring through IDX. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 15, 2025.
2. We strongly encourage you to report incidents of suspected identity theft to law enforcement.
3. You may also obtain a free copy of your credit report from each of the three major credit reporting agencies once every year by visiting <https://www.annualcreditreport.com> or by calling toll-free 877-322-8228.
4. You also may want to place a security freeze on your credit files by calling each of the three credit reporting agencies. Freezing credit files will prevent someone from using your personal information to open new accounts or borrow money in your name. Please understand that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card unless you temporarily or permanently remove the freeze.

You can contact the major credit reporting agencies using the information below.

Equifax

1-888-685-1111 (for fraud alerts: 1-888-766-0008, for security freezes: 1-800-685-1111)

P.O. Box 740241

Atlanta, GA 30374

<https://www.equifax.com/personal/credit-report-services/>

Experian

1-888-397-3742

P.O. Box 4500

Allen, TX 75013

<https://www.experian.com/help/>

Trans Union

1-800-916-8800

P.O. Box 2000

Chester, PA 19022

<https://www.transunion.com/credit-help>

We sincerely regret this security incident and any inconvenience it may cause you.

For More Information

If you have questions, you can contact us at privacy@maxar.com.

Sincerely,

Quincy Stott

General Counsel

Enclosure: Additional Information About Identity Protection



Additional Information About Identity Protection

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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

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: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

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

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.gov, Telephone: 1-401-274-4400

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