IceMiller
LEGAL COUNSEL

One American Square | Suite 2900 | Indianapolis, IN 46282-0200
Chicago Columbus DuPage County, Ill.
Indianapolis New York Philadelphia Washington, D.C.

December 6, 2021

WRITER'S DIRECT NUMBER: (312) 726-6220
DIRECT FAX: (312) 726-6292
EMAIL: Reena.Bajowala@icemiller.com

Via Electronic Mail

Office of the New Hampshire Attorney General
DOJ-CPB@DOJ.NH.gov
33 Capitol Street
Concord, NH 03301

RE: Security Breach Notification

Dear Attorney General:

On behalf of my client, Komatsu America Corp. ("Komatsu"), I am hereby submitting a written notification of an Information Security Incident, in compliance with N.H. Rev. Stat §§ 359-C:20(I)(b).

On September 22, 2021, Komatsu discovered that an unauthorized individual from outside Komatsu used improperly obtained credentials to access an employee's company email account and was able to bypass the multi-factor authentication (MFA). The unauthorized access occurred between September 20, 2021 and September 22, 2021. The email account belonged to a member of Komatsu's commercial account collections group.

Upon discovery of the incident, Komatsu engaged its internal experts and legal counsel to identify the scope of the incident. The investigation has not shown any evidence to suggest that the information in the email account was actually accessed, viewed or acquired by the unauthorized actor. The email account contained records that included name, address, date of birth, social security number, and financial account information. No other applications, accounts, systems or networks have been compromised.

Komatsu identified malicious message rules created by the unauthorized actor to discreetly delete all new inbound messages without discovery by the employee. The unauthorized actor also altered the multi-factor authentication (MFA) phone number used to gain access to the employee's email account.

Komatsu's review of the unauthorized actor's activities shows that the actor was likely targeting Komatsu's customers and business partners, and possibly to perpetrate fraudulent fund transfers. The unauthorized actor sent out email communications to contacts in the employee's

email account, and invited them to access an external website, with the likely intention of stealing additional credentials.

Komatsu forced a password reset for the impacted email account, reset the MFA method, and removed all unauthorized rules. In addition, Komatsu reviewed a large volume of emails and attachments within the employee's email account to identify any potential personal information that may have been accessed or acquired by the unauthorized actor. At this time, Komatsu has no information to believe that the unauthorized actor was targeting individuals' personal information or has any intention to commit identity deception, identity theft, or fraud.

Nonetheless, out of an abundance of caution, we are notifying **two (2)** New Hampshire residents. A copy of the notice that will be mailed to the New Hampshire residents on December 6, 2021, is attached herewith. Credit monitoring and identity theft protection services will be offered to the New Hampshire residents for a period of twelve (12) months.

Furthermore, Komatsu provided the employee with re-training on MFA controls, and will be modifying the MFA challenge to a more secure method across the organization.

If you require further information about this matter, please contact me by telephone at (312) 726-6220 or via email at reena.bajowala@icemiller.com.

Sincerely,

ICE MILLER, LLP

Reena R. Bajowala

Attachment: Copy of Individual Notification Letter

Komatsu America Corp
10300 SW Greenburg Rd., Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<Full Name>>
<<Address Line 1>>, <<Address Line 2>>
<<City>>, <<State>> <<Zip>>

December 6, 2021

Dear <<First Name>>,

Komatsu America Corp. ("Komatsu") takes the privacy and security of your personal information seriously. As such, we are contacting you to report an incident which may have involved some of your information. We want you to understand what happened, what we did to immediately address the issue, and what steps you can take to protect yourself.

What happened

On September 22, 2021, we were alerted that the email account of a Komatsu employee was breached by a cybercriminal. This unauthorized individual from outside Komatsu used improperly obtained credentials to access the employee's company email account and contacts.

What information was involved

The email account contained records that included your: <<PII types>>. We have no evidence to suggest that this information was actually accessed, viewed or acquired by the unauthorized individual.

What we are doing

As soon as we learned of the situation, we took action to secure the employee's email and prevent any further access. We also enabled additional security features to prevent similar incidents going forward.

We launched an investigation and engaged experienced and knowledgeable third party advisors to assist with the search for any personal information in the email account that could have been viewed. We recently completed our investigation and have determined that the compromised email account contained records that included some of your personal information.

The investigation has not revealed any access to, or misuse of your information, or any attempts at fraud or identity theft. Out of an abundance of caution, we are offering complimentary identity theft protection services through IDX, experts in data breach and recovery services. IDX services include: <<12/24 months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What you can do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect 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 March 6, 2022.

Please remain vigilant in monitoring your bills, account statements and financial transactions for incidents of fraud and identity theft, and promptly report any irregularities.

For more information

Although there is no evidence that your information was accessed as a result of this incident (our investigation simply notes that some of your personal information – as noted above – was found in the contents of the compromised email account), if you want to learn more about the steps you can take to protect against identity theft or fraud, please review the enclosed "Reference Guide" materials, go to https://app.idx.us/account-creation/protect or call 1-833-903-3648, toll free Monday through Friday from 9 am - 9 pm Eastern Time.

Sincerely,

Komatsu America Corp.

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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 or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
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.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place

the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. 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.

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: 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: 877-877-9392

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

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.