February 15, 2023

NH Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: MKS Instruments, Inc.
Data Breach Notification

To Whom This May Concern,

We, MKS Instruments, Inc. ("**MKSI**") are making this report to the Office of the New Hampshire Attorney General because we recently became aware of a security breach that may have resulted in the unauthorized acquisition of certain personal data. Details of the incident are as follows.

I. Brief Description of the Security Breach

On February 13, 2023 at 9.20 am Pacific Standard Time, MKSI became aware that a ransomware event on its systems that was focused on encrypting its business and manufacturing systems and making them unavailable to it may have also involved exfiltration of personal data.

On February 3, 2023, MKSI identified that it had become subject to a ransomware event and took immediate action to activate its incident response and business continuity protocols to contain the incident. MKSI initiated an ongoing investigation, alongside outside experts, and reported the issue to U.S. law enforcement. MKSI issued a public statement regarding the incident shortly after it was discovered, and has been in contact with personnel, customers, suppliers and other stakeholders about how MKSI is responding to the incident. The incident affected certain business systems, including production-related systems, and as part of the containment effort, MKSI elected to temporarily suspend certain operations. MKSI has been restoring various systems as soon as it determined that it was safe to do so, and will continue to do so as quickly and securely as possible until MKSI has returned its systems to normal operations.

II. Number of New Hampshire Residents being Notified and Date of Notification

MKSI has 203 employees in the state of New Hampshire. Therefore, we estimate that 203 New Hampshire residents have been affected by the breach and are notifying these residents accordingly with a notification date of February 16, 2023.

III. The Steps Taken to Remedy the Breach

After MKSI discovered that it was subject to a ransomware event, it took immediate action to activate its incident response and business continuity protocols to contain the incident. MKSI initiated an ongoing investigation, alongside outside experts, and reported the issue to U.S. law enforcement. MKSI issued a public statement regarding the incident shortly after it was discovered, and has been in contact with personnel, customers, suppliers and other stakeholders about how MKSI is responding to the incident.

The incident affected certain business systems, including production-related systems, and as part of the containment effort, MKSI elected to temporarily suspend certain operations. MKSI has been restoring various systems as soon as it determined that it was safe to do so, and will continue to do so as quickly and securely as possible until MKSI has returned its systems to normal operations. MKSI has required all personnel to change their work account passwords.

Additionally, MKSI has implemented the following measures since the breach occurred. It has reset system passwords twice, it has reset all user passwords, including service accounts, it has deployed Multi-Factor Authentication for local Multi-Factor Authentication to servers, and it has installed Sentinel One for additional monitoring. MKSI has also engaged third-party experts to assist with forensics, containment activities and restoring the network environment in a secure manner. Further, MKSI is taking steps to scan the dark web for indications of any third parties offering access to data that may have been exfiltrated.

* * * * *

If you have any further questions or concerns, please contact us at

Sincerely,

MKS Instruments, Inc.

MKS INSTRUMENTS, INC.
2 TECH DRIVE • SUITE 201 • ANDOVER, MA 01810-2434 • USA
P: +1.978.645.5500/+1.800.227.8766 • F: +1.978.557.5100
WWW.MKS.COM

MKS Instruments, Inc.
2 Tech Drive, Suite 201
Andover, MA 01810
United States

February 16, 2023

NOTICE OF DATA BREACH

We are contacting you because we recently became aware of a security breach that may have resulted in the unauthorized acquisition of certain personal data.

WHAT HAPPENED

On February 13, 2023 at 9:20 am Pacific Standard Time, we, MKS Instruments, Inc., the U.S. parent company of the MKS and Atotech group of companies which employs or did employ you, became aware that the ransomware event on our systems focused on encrypting our business and manufacturing systems and making them unavailable to us may have also involved exfiltration of personal data. While exfiltration of personal employee data has not been confirmed, we cannot rule it out and thus are providing notice.

WHAT WE ARE DOING

Upon learning of the ransomware event, we took immediate action to activate our incident response and business continuity protocols to contain the incident. We have initiated an ongoing investigation, alongside outside experts, and have reported the issue to U.S. law enforcement. We issued a public statement regarding the incident shortly after we discovered it, and have been in contact with personnel, customers, suppliers and other stakeholders about how we are responding to the incident. The incident affected certain business systems, including production-related systems, and, as part of the containment effort, we elected to temporarily suspend certain operations. We have been restoring our systems as soon as we determined that it was safe to do so, and will continue to do so as quickly and securely as possible until we have returned our systems to normal operations.

WHAT PERSONAL DATA WAS INVOLVED

We do not know of any concrete risks or threats to individual data subjects, but we cannot rule out that personal data, may have been exfiltrated. Our understanding is that, in similar prior cases affecting other companies, ransomware actors have appeared to refrain from using personal data against individuals. The types of personal data that may have been involved, where collection of such personal data is permitted by local law, include: Name, contact information, address, government ID numbers (including Social Security Number in the U.S.), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs (where MKS is required by law to collect), education, employment history, date of birth, gender, sexual orientation, bank account information, payment card information, information about compensation and equity, information about job position and time/hours worked, information about disabilities, health and medical conditions, employer union, health insurance information, basic information regarding your partner, children and emergency contacts (such as name, age, and contact details), if applicable.

WHAT YOU CAN DO

We encourage you to remain vigilant about any suspicious activity involving your personal data. For example, please do not open attachments or click on links in electronic communications from unknown senders, and please do not reveal personal or confidential information to unknown persons over the phone or other channels. If someone you think you recognize is asking you to take steps outside of your normal work functions, we recommend that you verify their identity before proceeding. If you receive any suspicious requests or communications at work, please report them to the IT service desk and wait for further instructions. **Please also follow the instructions in our password memo, sent to you separately.**

MKS Instruments, Inc.
2 Tech Drive, Suite 201
Andover, MA 01810
United States

February 16, 2023

OTHER IMPORTANT INFORMATION

To help relieve concerns and restore confidence following this incident, we will provide identity monitoring at no cost to you for 2 years. You will be sent details by mail as to how to activate your identity monitoring services and additional details regarding the services to be provided. You have up to 120 days to request and activate the monitoring services.

Additionally, please consider the following additional information:

- You may wish to visit the website of the U.S. Federal Trade Commission at http://www.consumer.ftc.gov/features/feature-0014-identity-theft or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC. The following website will direct you to your State Attorney General: https://.naag.org/find-my-ag/.

- You may have the right to obtain any police report filed related to this intrusion, and to file a police report and obtain a copy of it if you are the victim of identity theft.

- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 877-322-8228.

- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can 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. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may 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. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide information such as your: *(1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses over the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint*. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

    - Experian: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013

    - Equifax: 800-525-6285; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348

    - TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000

- You have relevant rights pursuant to the federal Fair Credit Reporting Act. For more information, please see the U.S. Federal Trade Commission's bulletin on Fair Credit Reporting Act rights available here: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

MKS Instruments, Inc.
2 Tech Drive, Suite 201
Andover, MA 01810
United States

February 16, 2023

FOR MORE INFORMATION

If you have further questions or concerns, please contact us at

If you would like to receive this notice in your local language, please contact your Human Resources representative.

Sincerely,

MKS Instruments, Inc.