Electronically Filed by Superior Court of California, County of Orange, 03/03/2023 03:21:44 PM.
30-2023-01310217-CU-MC-CXC - ROA # 2 - DAVID H. YAMASAKI, Clerk of the Court By A. Thau, Deputy Clerk.

COHELAN KHOURY & SINGER
Timothy D. Cohelan (SBN 60827)
tcohelan@ckslaw.com
605 C Street, Suite 200
San Diego, CA 92101
Telephone: (619) 595-3001/Facsimile: (619) 595-3000

KEEGAN & BAKER, LLP
Patrick N. Keegan (SBN 167698)
pkeegan@keeganbaker.com
2292 Faraday Avenue, Suite 100
Carlsbad, CA 92008
Telephone: (760) 929-9303/Facsimile: (760) 929-9260

Attorneys for Plaintiff JOHN DOE

Assigned for all purposes:
Judge Randall J. Sherman
Dept. CX105

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ORANGE

JOHN DOE, individually and on behalf of all others similarly situated, Plaintiff, vs. MKS INSTRUMENTS, INC.; and DOE DEFENDANTS 1-100; Defendants.	Case No.: 30-2023-01310217-CU-MC-CXC **CLASS ACTION COMPLAINT FOR DAMAGES, RESTITUTION, AND INJUNCTIVE RELIEF FOR VIOLATIONS OF:** **(1) THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CIVIL CODE §§ 56, *ET SEQ.*;** **(2) BREACH OF CALIFORNIA CONSUMER PRIVACY ACT, CIVIL CODE § 1798.150;** **(3) BREACH OF SECURITY NOTIFICATION LAW, CIVIL CODE § 1798.82; AND** **(4) BUSINESS AND PROFESSIONS CODE §§ 17200, *ET SEQ.*** **JURY TRIAL DEMANDED**

Plaintiff JOHN DOE (or "Plaintiff"), by and through his attorneys, bring this class action on behalf of himself individually and all others similarly situated, against Defendant MKS INSTRUMENTS, INC. and DOE DEFENDANTS 1-100 (collectively referred to as "Defendants"), and alleges upon information and belief as follows:

INTRODUCTION

1. This class action arises from the negligent and failure of Defendants to properly create, maintain, preserve, and/or store confidential, medical and personal information of Plaintiff[1] and all other persons similarly situated which allowed an unauthorized person to gain access to the computer network or data "systems" of Defendants on and prior to February 13, 2023, causing unauthorized access, acquisition, viewing, exfiltration, theft, use, release and disclosure of unencrypted medical and personal information of Plaintiff and other persons similarly situated, to at least one unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.* ("CMIA"), the California Consumer Privacy Act ("CCPA"), Civil Code § 1798.150, and the Business and Professions Code §§ 17200 *et seq*. Under the CCPA and the CMIA, Plaintiff, and all other persons similarly situated, have the right to expect that the confidentiality of their medical and personal information in possession of Defendants to be reasonably preserved and protected from unauthorized access, acquisition, viewing, exfiltration, theft, use, release and disclosure.

2. As alleged more fully below, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber security and data protection safeguards, failing to implement adequate and reasonable security controls and user authorization and authentication processes, failing to limit the types of data permitted to be transferred, failing to encrypt Plaintiff's and the Class' "medical information" as defined by Civil Code § 56.05(i), and "personal information" as defined by Civil Code § 1798.81.5, and to put into place reasonable or adequate computer systems and security practices to safeguard customers' and employees' medical and personal information, Defendants negligently created,

---

[1] California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases involving health information. Civil Code § 3427.3 (West 2011). Specifically, section 3427.3 provides, "The court having jurisdiction over a civil proceeding under this title shall take all steps ***reasonably necessary to safeguard the individual privacy and prevent harassment of a health care patient***, licensed health practitioner, or employee, client, or customer of a health care facility who is a party or witness in the proceeding, including granting protective orders. ***Health care patients***, licensed health practitioners, and employees, clients, and customers of the health care facility ***may use pseudonyms to protect their privacy***." Civil Code § 3427.3 (emphasis added). Here, a pseudonym has been used in place of the real name of Plaintiff because at all times relevant to this action, Plaintiff's medical information was subject to **Error! Main Document Only.**unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' statutory violations and Plaintiff has individual privacy concerns and a reasonable fear of harassment in light of the nature of the case.

maintained, preserved, and stored Plaintiff's and the Class (defined *infra*) members' medical and personal information, in possession of or derived from Defendants, in an unencrypted manner on and prior to February 13, 2023, allowing such information to be accessed, exfiltrated, stolen and viewed by at least one unauthorized third party ransomeware actor, without Plaintiff's and the Class members' prior written authorization, which constitutes unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a) and 56.101(a) of the CMIA. In fact, Defendant MKS INSTRUMENTS, INC.'s form letter, dated February 16, 2023, entitled "**NOTICE OF DATA BREACH**," signed by "MKS Instruments, Inc.," sent to Plaintiff and all other persons similarly situated, stating in part, "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," and informing him, in part, of "**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?** ... We have initiated an ongoing investigation, alongside outside experts, and have reported the issue to U.S. law enforcement…. 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 cannot rule out that personal data, may have been exfiltrated…. 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." An exemplar of Defendant MKS INSTRUMENTS, INC.'s form letter, dated February 16, 2023, entitled "**NOTICE OF DATA BREACH**," signed by "MKS Instruments, Inc.," that was submitted to the Attorney General of the State of California is attached hereto as **Exhibit A**.

3. Because the individually identifiable medical information and other personal identifying information of Plaintiff and the Class was subject to unauthorized access, "acquisition," "exfiltration," disclosure and viewing by at least one unauthorized third party "ransomeware actor" and in violation of the CMIA, Plaintiff, individually and on behalf of all others similarly situated, seeks from Defendants compensatory damages, punitive damages not to exceed three thousand dollars ($3,000), attorney's fees not to exceed one thousand dollars ($1,000), and the costs of litigation pursuant to Civil Code § 56.35, and nominal damages in the amount of one thousand dollars ($1,000) for each violation under Civil Code §56.36(b)(1) and actual damages, according to proof, for each violation pursuant to Civil Code § 56.36(b)(2). Additionally, because the individually identifiable personal information of Plaintiff and the Class was subject to unauthorized access, "acquisition," "exfiltration," disclosure and viewing by at least one unauthorized third party "ransomeware actor" in violation of the CCPA, Plaintiff, individually and on behalf of all others similarly situated, seeks from Defendants Plaintiff and the Class seek actual damages and injunctive relief pursuant to Civil Code § 1798.150(a)(1)(A) and Civil Code § 1798.150(b). Further, because Plaintiff also alleges Defendants' conduct violates Business & Professions Code §§ 17200, *et seq*., Plaintiff, individually and on behalf of others similarly situated, seeks injunctive relief and restitution from Defendants under Business and Professions Code § 17203.

4. This action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, on a large class of persons. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff

in relation to Plaintiff's stake in the matter, and therefore class certification is appropriate in this matter.

JURISDICTION AND VENUE

5. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class in the aggregate exceeds the $25,000 jurisdictional minimum of this Court. Further, the amount in controversy as to Plaintiff individually does not exceed $75,000.

6. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of Civil Procedure §§ 395(a) and 395.5 because Defendant MKS INSTRUMENTS, INC. is registered to do business in and does business in the State of California, and employs persons located in California and in this judicial district. Defendants have obtained medical information of Plaintiff and the Class in the transaction of business in the State of California and in this judicial district, which has caused both obligations and liability of Defendants to arise in the State of California and in this judicial district.

7. Further, this action does not qualify for federal jurisdiction under the Class Action Fairness Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies to this action because (1) more than two-thirds of the members of the proposed Class are citizens of the State of California, and (2) the parties are citizens of the State of California.

PARTIES

A. PLAINTIFF

8. Plaintiff JOHN DOE is and was at all times relevant to this action a resident of the State of California and citizen of the State of California. At all times relevant to this action, Plaintiff JOHN DOE was an employee of Defendant MKS INSTRUMENTS, INC. at its principal place of business located at 1791 Deere Avenue, Irvine, California, 92606-4814. During his employment, Plaintiff was required to and did provided his personal information and medical information, including his name, contact information, address, government ID numbers (including Social Security Number), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs, 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, information regarding his partner, children and emergency contacts (such as name, age, and contact details), to Defendant MKS INSTRUMENTS, INC., including prior to February 13, 2023. Additionally, Plaintiff received MKS's form letter, dated February 16, 2023, entitled "**NOTICE OF DATA BREACH**," signed by "MKS Instruments, Inc.," attached hereto as **Exhibit A**, stating in part, "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," and informing him, in part, of "**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?** ... We have initiated an ongoing investigation, alongside outside experts, and have reported the issue to U.S. law enforcement…. 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 cannot rule out that personal data, may have been exfiltrated…. 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.**" As a result, Plaintiff reasonably fears that disclosure and/or release of his medical and personal information created, maintained, preserved and/or stored on Defendants' computer "systems" or network could subject him to harassment or abuse.

B. DEFENDANTS

9. Defendant MKS INSTRUMENTS, INC. ("MKS") is registered to do business and does business in the State of California (Entity File No. 1024978), operates a principal place of business located at [1791 Deere Avenue, Irvine, California, 92606-4814], and with its registered agent of service of process COGENCY GLOBAL INC., 1325 J Street, Suite 1550, Sacramento, California 95814. MKS represents that the company manufactures and sells instruments, subsystems, process control solutions and specialty chemicals technology to a variety of industries, primarily semiconductor manufacturers, MKS employs more than 6,000 people and generates approximately $3 billion in annual revenue. MKS is publicly traded on the NASDAQ under the ticker symbol "MKSI." At all times relevant to this action, MKS was and is an employer, within the meaning of Civil Code § 56.20, who received, created, maintained, preserved, and stored personal information and medical information, as those terms are defined and set forth in the CCPA and the CMIA, including the names, contact information, address, government ID numbers (including Social Security Numbers), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs, 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 their partners, children and emergency contacts (such as name, age, and contact details), of Plaintiff and the Class (defined *infra*), and is subject to the requirements and mandates of the CCPA and the CMIA, including but not limited to Civil Code §§ 56.20, 56.21, and 56.245. On or about February 16, 2023, MKS caused a form letter, dated February 16, 2023, entitled "**NOTICE OF DATA BREACH**," signed by "MKS Instruments, Inc.," an exemplar of which is attached hereto as **Exhibit A**, to be submitted to the Attorney General of the State of California and to be mailed to Plaintiff and all others similarly situated. At all times relevant to this action, MKS employed Plaintiff and employs persons located in the California and in this judicial district.

10. At all times relevant to this action, MKS was and is a "business" within the meaning of Civil Code § 1798.140(c)(1), owns or licenses computerized data which includes Plaintiff's and the Class' personal information, within the meaning of Civil Code § 1798.82(h), collected Plaintiff's and the Class' personal information within the meaning of Civil Code § 1798.81.5(d)(1).

C. DOE DEFENDANTS

11. The true names and capacities, whether individual, corporate, associate, or otherwise, of Defendants sued herein as DOE DEFENDANTS 1 through 100, inclusive, are currently unknown to Plaintiff, who therefore sues the Defendants by such fictitious names under the Code of Civil Procedure § 474. Each of the Defendants designated herein as a DOE DEFENDANT is legally responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of court and/or amend this complaint to reflect the true names and capacities of the Defendants designated hereinafter as DOE DEFENDANTS 1 through 100 when such identities become known. Any reference made to a named Defendant by specific name or otherwise, individually or plural, is also a reference to the actions or inactions of DOE DEFENDANTS 1 through 100, inclusive.

/ / /

/ / /

D. AGENCY/AIDING AND ABETTING

12. At all times herein mentioned, Defendants, and each of them, were an agent or joint venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

13. Defendants, and each of them, aided and abetted, encouraged and rendered substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially assist the commissions of these wrongful acts and other wrongdoings complained of, each of the Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals, and wrongdoing.

FACTUAL ALLEGATIONS

14. At all times relevant to this action, including the period prior to and on February 13, 2023, MKS created, maintained, preserved, and stored records of the names, contact information, addresses, government ID numbers (including Social Security Numbers), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs, education, employment history, dates 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 their partners, children and emergency contacts (such as name, age, and contact details), of Plaintiff and the Class (which constitutes personal information as that term is defined and set forth in the CCPA, and medical information, as that term is defined and set forth in the CMIA), that Plaintiff and other Class members received from providers of health care, on its computer network or data "systems." As a result, at all times relevant to this action, including the period prior to and on February 16, 2023, MKS was and is a receipent of medical information within the meaning of Civil Code §

56.05(i), personal information, within the meaning of Civil Code § 1798.82(h), and personal information within the meaning of Civil Code § 1798.81.5(d)(1). As a result, at all times relevant to this action, including the period prior to and on February 13, 2023, Plaintiff and Class members were patients, within the meaning of Civil Code § 56.05(l), of providers of health care.

15. As a result, on or before February 13, 2023, Defendants possessed Plaintiff's and the Class' medical information, in electronic and physical form, in possession of or derived from Defendants, regarding their medical history, mental or physical condition, or treatment. Such medical information included or contained an element of personal identifying information sufficient to allow identification of Plaintiff and the Class, such as their names, contact information, addresses, government ID numbers (including Social Security Numbers), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs, education, employment history, dates 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 their partners, children and emergency contacts (such as name, age, and contact details), or other information that, alone or in combination with other publicly available information, reveals their identity.

16. At all times relevant to this action, including prior to and on February 13, 2023, pursuant to Civil Code § 56.245, MKS is and was a "recipient of medical information pursuant to an authorization as provided by this chapter" and was prohibited from "further disclos[ing] such medical information unless in accordance with a new authorization that meets the requirements of Section 56.21, or as specifically required or permitted by other provisions of this chapter or by law."

17. Alternatively, at all times relevant to this action, including prior to and on February 13, 2023, pursuant to Civil Code § 56.13, MKS is and was a "recipient of medical information pursuant to an authorization as provided by this chapter or pursuant to the provisions of subdivision (c) of Section 56.10" and was prohibited from "further disclos[ing] that medical information except

in accordance with a new authorization that meets the requirements of Section 56.11, or as specifically required or permitted by other provisions of this chapter or by law."

18. As an employer who receives personal and confidential medical information and/or an authorized recipient of personal and confidential medical information, MKS is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated or released without patients' authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.13, 56.20, and 56.245.

19. As an employer who receives personal and confidential medical information and/or an authorized recipient of personal and confidential medical information, MKS is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization[2] under Civil Code §§ 56.13, 56.20, and 56.245.

[2] An "authorization" is defined under the CMIA as obtaining permission in accordance with Civil Code §§ 56.13, 56.20, and 56.245. Under Civil Code §§ 56.11 and 56.21, an authorization for the release of medical information is valid only if it:
(a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.
(b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.
(c) Is signed and dated by one of the following:
(1) The patient. A patient who is a minor may only sign an authorization for the release of medical information obtained by a provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which the minor could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7 (commencing with Section 60).
(2) The legal representative of the patient, if the patient is a minor or an incompetent. However, authorization may not be given under this subdivision for the disclosure of medical information obtained by the provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which a minor patient could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7 (commencing with Section 60).
(3) The spouse of the patient or the person financially responsible for the patient, where the medical information is being sought for the sole purpose of processing an application for health insurance or for enrollment in a nonprofit hospital plan, a health care service plan, or an employee benefit plan, and where the patient is to be an enrolled spouse or dependent under the policy or plan.
(4) The beneficiary or personal representative of a deceased patient.
(d) States the specific uses and limitations on the types of medical information to be disclosed.
(e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.
(f) States the name or functions of the persons or entities authorized to receive the medical information.
(g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.
(h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.
(i) Advises the person signing the authorization of the right to receive a copy of the authorization.

20. As an employer who receives personal and confidential medical information and/or an authorized recipient of personal and confidential medical information, MKS is required by the CMIA to create, maintain, preserve, and store medical records in a manner that preserves the confidentiality of the information contained therein under Civil Code §§ 56.13, 56.20, and 56.245.

21. As an employer who receives medical information, MKS is required by the CMIA to take appropriate preventive actions to protect the confidential information or records against release consistent with MKS's obligations under the CMIA, under Civil Code §§ 56.13, 56.20, 56.245, and 56.36(e)(2)(E), or other applicable state law, including, but not limited to, all of the following:

i. Developing and implementing security policies and procedures.

ii. Designating a security official who is responsible for developing and implementing its security policies and procedures, including educating and training the workforce.

iii. Encrypting the information or records, and protecting against the release or use of the encryption key and passwords, or transmitting the information or records in a manner designed to provide equal or greater protections against improper disclosures.

22. Notwithstanding these duties, on or about February 16, 2023, MKS submitted to the Attorney General of the State of California and mailed to Plaintiff and the Class, a form letter, entitled "**NOTICE OF DATA BREACH**," dated February 16, 2023, signed by "MKS Instruments, Inc.," attached hereto as **Exhibit A**, stating in part, "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," and informing him, in part, of "**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?** ... We have initiated an ongoing investigation, alongside outside experts, and have reported the issue to U.S. law enforcement…. 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 cannot rule out that personal data, may have been exfiltrated…. 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.**"

23. Based upon MKS's form letter, dated February 16, 2023, entitled "**NOTICE OF DATA BREACH**," signed by "MKS Instruments, Inc.," attached hereto as **Exhibit A**, Plaintiff alleges on information and belief that at all times relevant to this action, including the period prior to and on February 13, 2023, MKS created, maintained, preserved, and stored Plaintiff's and the Class members' medical information on its computer network or data "systems."

24. Based upon MKS's form letter, dated February 16, 2023, entitled "**NOTICE OF DATA BREACH**," signed by "MKS Instruments, Inc.," attached hereto as **Exhibit A**, Plaintiff alleges on information and belief that at all times relevant to this action, including the period prior to February 13, 2023, a security breach "resulted in the unauthorized acquisition of certain personal data" containing Plaintiff's and the Class' medical information and personal information, including the names, contact information, addresses, government ID numbers (including Social Security Numbers), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs, education, employment history, dates 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 their partners, children and emergency contacts (such as name, age, and contact details), as determined by MKS's investigation, in an un-encrypted format, as represented by MKS in its form letter, dated February 16, 2023, entitled "**NOTICE OF DATA BREACH**," signed by "MKS Instruments, Inc.," attached hereto as **Exhibit A**. Thus, the cybercriminal accessed, "exfiltrated" and viewed Plaintiff's and the Class' un-encrypted medical information and personal information, including their names, contact information, addresses, government ID numbers (including Social Security Numbers), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs, education, employment history, dates 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 their partners, children and emergency contacts (such as name, age, and contact details), that, alone or in combination with other publicly available information, reveals their identity.

25. MKS had the resources necessary to protect and preserve confidentiality of Plaintiff's and the Class' medical information and personal information in their possession, but

neglected to adequately implement data security measures as required by the CCPA and the CMIA, despite their obligation to do so.

26. Additionally, the risk of vulnerabilities in its computer and data systems of being exploited by an unauthorized third party trying to steal Plaintiff's and the Class' medical information and personal information was foreseeable and/or known to MKS. The California Data Breach Report 2012-2015, issued in February 2016 by Attorney General, Kamala D. Harris, reported, "Malware and hacking presents the greatest threat, both in the number of breaches and the number of records breached" and "Social Security numbers and medical information – was breached than other data types." Moreover, as Attorney General further reported, just because "[e]xternal adversaries cause most data breaches, [] this does not mean that organizations are solely victims; they are also stewards of the data they collect and maintain. People entrust businesses and other organizations with their data on the understanding that the organizations have a both an ethical and a legal obligation to protect it from unauthorized access. Neglecting to secure systems and data opens a gateway for attackers, who take advantage of uncontrolled vulnerabilities." Regarding encryption, Attorney General instructed in California Data Breach Report 2012-2015, "As we have said in the past, breaches of this type are preventable. Affordable solutions are widely available: strong full-disk encryption on portable devices and desktop computers when not in use.[] Even small businesses that lack full time information security and IT staff can do this. They owe it to their patients, customers, and employees to do it now."

27. Further, it also was foreseeable and/or known to MKS that negligently creating, maintaining, preserving, and/or storing Plaintiff's and the Class' medical information and personal information, in electronic form, in its computer network or data "systems" in a manner that did not preserve the confidentiality of the information could have a devastating effect on them. As reported in the California Data Breach Report 2012-2015, "There are real costs to individuals. Victims of a data breach are more likely to experience fraud than the general public, according to Javelin Strategy & Research. In 2014, 67 percent of breach victims in the U.S. were also victims of fraud, compared to just 25 percent of all consumers."

28. To be successful, phishing relies on a series of affirmative acts by a company and its employees such as clicking a link, downloading a file, or providing sensitive information. Once criminals gained access to the email accounts of a company and its employees, the email servers communicated—that is, disclosed—the contents of those accounts to the criminals. "Phishing scams are one of the most common ways hackers gain access to sensitive or confidential information. Phishing involves sending fraudulent emails that appear to be from a reputable company, with the goal of deceiving recipients into either clicking on a malicious link or downloading an infected attachment, usually to steal financial or confidential information." (https://www.varonis.com/blog/data-breach-statistics/). As posted on April 21, 2020, the FBI had issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19 phishing scams targeting healthcare providers.

29. At all times relevant to this action, including the period prior to and on February 13, 2023, Defendants negligently created, maintained, preserved, and/or stored Plaintiff's and the Class' medical information and personal information, including Plaintiff's and the Class' names, contact information, addresses, government ID numbers (including Social Security Numbers), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs, education, employment history, dates 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 their partners, children and emergency contacts (such as name, age, and contact details), in electronic form, onto Defendants' its computer network or data "systems" in a manner that did not preserve the confidentiality of the information, and negligently failed to protect and preserve confidentiality of Plaintiff's and the Class' medical information and personal information in their possession against unauthorized disclosure and/or release, including but not limited to, by failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber security and data protection safeguards, failing to implement adequate and reasonable security controls and user authorization and authentication processes,

failing to limit the types of data permitted to be transferred, failing to encrypt Plaintiff's and the Class' "medical information" as defined by Civil Code § 56.05(i), and "personal information" as defined by Civil Code § 1798.81.5, and to put into place reasonable or adequate computer systems and security practices to safeguard customers' and employees' medical and personal information, and failing to have adequate privacy policies and procedures in place, as required by the CMIA, under Civil Code §§ 56.13, 56.20, 56.245, and 56.36(e)(2)(E), and according to their written representations to Plaintiff and the Class.

30. Had Defendants and/or its employees (presently unknown to Plaintiff) taken such appropriate preventive actions, fix the deficiencies in their computer network or data "systems," and adopted security measures as required by the CCPA and the CMIA prior to and on February 13, 2023, MKS could have prevented Plaintiff's and the Class' medical information and personal information in their computer network or data "systems" from being accessed, acquired, exfiltrated, stolen and viewed by at least one unauthorized third party "ransomeware actor."

31. On and before February 13, 2023, Defendants and/or its employees (presently unknown to Plaintiff), by negligently creating, maintaining, preserving, and storing Plaintiff's and the Class' medical information and personal information in their computer network or data "systems," allowed Plaintiff's and the Class' individually identifiable medical and personal information to be accessed, acquired, "exfiltrated," stolen and viewed by at least one unauthorized third party "ransomeware actor," without first obtaining an authorization, constituting a disclosure in violation of Civil Code §§ 56.10(a), 56.13, 56.245 and 56.26(a).

32. California law requires a business to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. Specifically, pursuant to Civil Code § 1798.82(a), "A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably

believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable." California law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General. On or about February 16, 2023, MKS caused a form letter, dated February 16, 2023, entitled "**NOTICE OF DATA BREACH**," signed by "MKS Instruments, Inc.," an exemplar of which is attached hereto as **Exhibit A**, to be submitted to the Attorney General of the State of California and to be mailed to Plaintiff and the Class, stating in part, "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," and informing him, in part, of "**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?** ... We have initiated an ongoing investigation, alongside outside experts, and have reported the issue to U.S. law enforcement…. 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 cannot rule out that personal data, may have been exfiltrated…. 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.**" Because MKS submitted its Notice of Data Breach form letter, dated February 16, 2023, to the Attorney General of the State of California and mailed it to Plaintiff and members of the Class, MKS has determined and has conceded that Plaintiff's and the Class' identifiable personal information and medical information contained in MKS's computer network and data "systems" was either not encrypted at all, or if it was encrypted, the encryption has been breached by the unauthorized third party or parties. Additionally, because MKS submitted its Notice of Data Breach letter, dated February 16, 2023, to the Attorney General of the State of California and mailed it to Plaintiff and members of the Class, MKS has conceded that Plaintiff's and the Class' personal information and medical information contained in MKS's computer network and data "systems," was unencrypted and thus, the unauthorized third party or parties who accessed Plaintiff's and the Class' personal information and medical information contained in MKS's computer network and data "systems," was able to and did actually view Plaintiff's and the Class' personal information and medical information contained in MKS's computer network and data "systems." As a result, MKS was negligent for failing to encrypt or adequately encrypt Plaintiff's and the Class' electronic personal information and medical information contained in its computer network or data "systems."

33. MKS's form letter submitted to the Attorney General of the State of California and mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, further states, "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." Other than offering its apology and future promise of "identity monitoring at no cost to you for 2 years," MKS's form letter does nothing to further protect Plaintiff and the Class from future incidents of identity theft despite the severity of the unauthorized access, viewing, exfiltration, theft, disclosure and release of their electronic medical and personal information caused by MKS's violations of its duty to implement and maintain reasonable security procedures and practices. To date, other than offering its apology and future promise of "identity monitoring at no cost to you for 2 years," MKS has not offered any monetary compensation for the unauthorized disclosure and/or release of Plaintiff's and the Class' electronic medical information under the CMIA or personal information under the CCPA. In effect, MKS is shirking its responsibility for the harm it has caused, while shifting the burdens and costs of its wrongful conduct onto its employees and customers, i.e. Plaintiff and the Class.

CLASS ACTION ALLEGATIONS

34. Plaintiff brings this action on behalf of herself individually and on behalf of all others similarly situated. The putative class that Plaintiff seeks to represent is defined as follows:

> Class: All persons to whom MKS Instruments, Inc. sent a Notice of Data Breach letter, dated on or about February 16, 2023, an exemplar of which is attached hereto as **Exhibit A**.

The officers, directors, and employees of MKS are excluded from the Class. The officers, directors, and employees of any "affiliate," "principal" and "subsidiary" of MKS, as defined in the Corporations Code §§ 150, 175, and 189, respectively, are excluded from the Class. Plaintiff reserves the right under California Rule of Court 3.765 to amend or modify the Class definition with greater particularity or further division into subclasses or limitation to particular issues as warranted, and as additional facts are discovery by Plaintiff during his future investigations.

35. This action is properly maintainable as a class action. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. While the exact number of the Class members is unknown to Plaintiff at this time. The disposition of the claims of the members of Class through this class action will benefit both the parties and this Court. In addition, the Class is readily identifiable from information and records in the possession of MKS and its agents, and the Class is defined in objective terms that make the eventual identification of Class members possible and/or sufficient to allow members of the Class to identify themselves as having a right to recover.

36. There is a well-defined community of interest among the members of the Class because common questions of law and fact predominate, Plaintiff's claims are typical of the members of the Class, and Plaintiff can fairly and adequately represent the interests of the Class.

37. Common questions of law and fact exist as to all members of the Class and the Class and predominate over any questions affecting solely individual members of the Class and the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a) Whether Defendants possessed Plaintiff's and the Class' medical and personal identifying information prior to and on February 13, 2023;

b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's and the Class' medical and personal identifying information, in electronic form, onto Defendants' computer network or data "systems," prior to and on February 13, 2023;

c) Whether Defendants implemented and maintained reasonable security procedures and practices to protect Plaintiff's and the Class' medical and personal identifying information, in electronic form, within Defendants' computer network or data "systems," prior to and on February 13, 2023;

d) Whether Plaintiff's and the Class' medical and personal identifying information, in electronic form, within Defendants' computer network or data "systems," prior to

and on February 13, 2023, was accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party;

e) Whether Plaintiff's and the Class' medical and personal identifying information, in electronic form, within Defendants' computer network or data "systems," prior to and on February 13, 2023, was accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party without the prior written authorization of Plaintiff and the Class, as required by Civil Code §§ 56.13, 56.20 and 56.245;

f) Whether Defendants' creation, maintenance, preservation and/or storage of Plaintiff's and the Class' medical and personal identifying information, in electronic form, within Defendants' computer network or data "systems," accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party was permissible without written authorization from Plaintiff and the Class or under any exemption under Civil Code §§ 56.13, 56.20 and 56.245;

g) Whether Defendants' creation, maintenance, preservation and/or storage of Plaintiff's and the Class' medical and personal identifying information, in electronic form, within Defendants' computer network or data "systems," accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party constitutes a release in violation of Civil Code §§ 56.13, 56.20 and 56.245;

h) Whether Defendants' notice that Plaintiff's and the Class' medical and personal identifying information was accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party, provided the minimum amount information required by statute;

i) Whether the timing of Defendants' notice that Plaintiff's and the Class' medical and personal identifying information was accessed, viewed, exfiltrated and/or publicly exposed by an unauthorized third party, was given in the most expedient time possible and without reasonable delay;

j) Whether Defendants' conduct constitute unlawful, fraudulent or unfair practices in violation of Business and Professions Code §§ 17200, *et seq.*; and

k) Whether Plaintiff and the Class are entitled to actual, nominal or statutory damages, injunctive relief and/or restitution.

38. Plaintiff's claims are typical of those of the other Class members because Plaintiff, like every other Class member, was exposed to virtually identical conduct and now suffer from the same violations of the law as other Class members.

39. Plaintiff will fairly and adequately protect the interests of the Class. Moreover, Plaintiff has no interest that is contrary to or in conflict with those of the Class she seeks to represent. In addition, Plaintiff has retained competent counsel experienced in class action litigation to further ensure such protection and intend to prosecute this action vigorously.

40. The nature of this action and the nature of laws available to Plaintiff and the members of Class make the use of the class action format a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class for the claims alleged and the disposition of whose claims in a class action will provide substantial benefits to both the parties and the Court because:

a) If each member of the Class were required to file an individual lawsuit, MKS would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual member of the Class with its vastly superior financial and legal resources;

b) The costs of individual suits could unreasonably consume the amounts that would be recovered;

c) Proof of a common business practice or factual pattern which Plaintiff experienced is representative of that experienced by the Class and will establish the right of each of the members to recover on the causes of action alleged;

d) Individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation;

e) MKS has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making it appropriate to render judgment with respect to the Class as a whole in this litigation; and

f) The disposition of the claims of the members of Class through this class action will produce salutary by-products, including a therapeutic effect upon those who indulge in unlawful practices, and aid to legitimate business enterprises by curtailing unlawful competition.

41. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for the Defendants in the State of California and would lead to repetitious trials of the numerous common questions of fact and law in the State of California. Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action. As a result, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

42. Notice to the members of the Class may be made by e-mail or first-class mail addressed to all persons who have been individually identified by Defendants and who have been given notice of the data breach.

43. Plaintiff and the Class have suffered irreparable harm and damages because of Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff and the Class will continue to be damaged and to suffer by the unauthorized disclosure and/or release of their medical and personal identifying information, thereby allowing these violations of law to proceed without remedy.

44. Moreover, Plaintiff's and the Class' individual damages are insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied. In addition, Defendants have acted or refused to act on grounds generally applicable to Plaintiff and the Class, thereby making appropriate final injunctive relief with respect to, the Class as a whole.

/ / /

/ / /

/ / /

/ / /

FIRST CAUSE OF ACTION
Violations of the Confidentiality of Medical Information Act
California Civil Code §§ 56, et seq.
(On Behalf of Plaintiff and the Class Against All Defendants)

45. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if fully stated herein.

46. At all times relevant to this action, including on and before February 13, 2023, Defendants are employers and/or other authorized recipients of personal and confidential medical information as defined and set forth in the California Confidentiality of Medical Information Act, California Civil Code §§ 56, *et seq.* (the "CMIA") and maintained and continue to maintain "medical information," within the meaning of Civil Code § 56.05(i), of Plaintiff and Class members who are similarly situated employees and "patients" within the meaning of Civil Code § 56.05(1).

47. At all times relevant to this action, including on and before February 13, 2023, Defendants lawfully came into possession of Plaintiffs' and Class members' personally identifiable medical information, including their names, contact information, addresses, government ID numbers (including Social Security Numbers), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs, education, employment history, dates 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 their partners, children and emergency contacts (such as name, age, and contact details), and had a duty to exercise reasonable care in preserving the confidentiality of this information subject to the requirements and mandates of the CMIA, including but not limited to Civil Code §§ 56.13, 56.20, 56.21, 56.245, 56.35, and 56.36. At all times relevant to this action, including on and before February 13, 2023, Plaintiff and the Class had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(i), created, maintained, preserved, and stored in MKS's computer network or data "systems." Further, at all times relevant to this action, including on and before February 13, 2023, Plaintiff and

the Class are "patients" within the meaning of Civil Code § 56.05(l), and fear that disclosure and/or release of their medical information could subject them to harassment or abuse.

48. As a result, at all times relevant to this action, including on and before February 13, 2023, Defendants and/or unknown employees negligently created, maintained, preserved, and/or stored Plaintiff's and the Class' individual identifiable "medical information," within the meaning of Civil Code § 56.05(i), including Plaintiff's and Class members' their names, contact information, addresses, government ID numbers (including Social Security Numbers), work login credentials/passwords, marital status, veteran status, nationality, immigration status, race, religious beliefs, education, employment history, dates 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 their partners, children and emergency contacts (such as name, age, and contact details), in MKS's computer network or data "systems," in a manner that did not preserve the confidentiality of the information, and negligently failed to protect and preserve confidentiality of electronic medical information of Plaintiff and the Class in its possession against disclosure and/or release, including but not limited to, by failing to invest in cyber security and data protection safeguards, failing to implement adequate and reasonable security controls and user authorization and authentication processes, failing to limit the types of data permitted to be transferred, failing to encrypt Plaintiff's and the Class' "medical information" as defined by Civil Code § 56.05(i), and "personal information" as defined by Civil Code § 1798.81.5, and to put into place reasonable or adequate computer systems and security practices to safeguard customers' and employees' medical and personal information, and failing to have adequate privacy policies and procedures in place, as required by the CMIA, under Civil Code §§ 56.13, 56.20, 56.21, 56.245, 56.35, and 56.36, and according to their written representations to Plaintiff and the Class.

49. Due to MKS's negligent creation, maintenance, preservation and/or storage of Plaintiff's and the Class' electronic medical information in MKS's computer network or data "systems," MKS allowed Plaintiff's and the Class' individually identifiable medical information to

be accessed and actually viewed by at least one unauthorized third party on or before February 13, 2023, without first obtaining an authorization within the meaning of Civil Code §§ 56.11 and 56.21, constituting a disclosure in violation of Civil Code §§ 56.13, 56.20 and 56.245.

50. Due to MKS's negligent creation, maintenance, preservation and/or storage of Plaintiff's and the Class' electronic medical information in MKS's computer network or data "systems," MKS allowed Plaintiff's and the Class' individually identifiable medical information to be accessed and actually viewed by at least one unauthorized third party on or before February 13, 2023, constituting a release in violation of Civil Code §§ 56.13, 56.20 and 56.245.

51. As a result of MKS's above-described conduct in violation of the CMIA, Plaintiff and the Class have suffered damages from the unauthorized access, use, disclosure and/or release of their individual identifiable medical information.

52. As a direct and proximate result of MKS's above-described conduct in violation of the CMIA, including Civil Code § 56.20, Plaintiff and the Class are entitled to recover "compensatory damages, punitive damages not to exceed three thousand dollars ($3,000), attorney's fees not to exceed one thousand dollars ($1,000), and the costs of litigation" pursuant to Civil Code § 56.35.

53. As a result of MKS's above-described conduct in violation of the CMIA, Plaintiff and the Class seek compensatory damages, punitive damages not to exceed three thousand dollars ($3,000), attorney's fees not to exceed one thousand dollars ($1,000), and the costs of litigation according to proof pursuant to Civil Code § 56.35.

54. As a direct and proximate result of MKS's above-described conduct in violation of the CMIA, Plaintiff and the Class are entitled to recover, "against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: (1) ... nominal damages of one thousand dollars ($1,000). In order to recover under this paragraph, it shall not be necessary that the plaintiff suffered or was threatened with actual damages. (2) The amount of actual damages, if any, sustained by the patient."

55. As a result of MKS's and/or its employees' above-described conduct in violation of the CMIA, Plaintiff and the Class seek nominal damages of one thousand dollars ($1,000) for each

violation under Civil Code §56.36(b)(1), and actual damages suffered, according to proof, for each violation under Civil Code § 56.36(b)(2) from all Defendants.

SECOND CAUSE OF ACTION
Breach of California Consumer Privacy Act
Civil Code § 1798.150
(On Behalf of Plaintiff and the Class Against All Defendants)

56. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if fully stated herein.

57. Pursuant to Civil Code § 1798.150(a)(1), "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action ....."

58. Defendants are organized for the profit or financial benefit of their owners and collects Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5 as defined by Civil Code § 1798.140.

59. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5 from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5.

60. Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5 was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendants' violation of its duty under the CCPA.

61. Defendants knew, or should have known, that their network computer systems and data security practices were inadequate to safeguard Plaintiff's and the Class' "personal

information" as defined by Civil Code § 1798.81.5 and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5, such as encrypting Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5 so in the event of a data breach Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5 cannot be read by an unauthorized third party. As a result of the failure to implement reasonable security procedures and practices, Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5 was subject to an unauthorized access and exfiltration, theft, or disclosure.

62. As a direct and proximate result of Defendants' violation of its duty under the CCPA, Plaintiff and the Class seek injunctive or declaratory relief from all Defendants pursuant to Civil Code § 1798.150(a)(1)(B) to ensure that Defendants hereinafter adequately safeguard Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5 by implementing reasonable security procedures and practices. This relief is important because Defendants still possess Plaintiff's and the Class' "personal information" as defined by Civil Code § 1798.81.5. Plaintiff and the Class have an interest in ensuring that their "personal information" as defined by Civil Code § 1798.81.5 is reasonably protected in the future.

63. As a direct and proximate result of Defendants' violation of its duty under the CCPA, Plaintiff and the Class seek actual damages pursuant to Civil Code § 1798.150(a)(1)(A) and Civil Code § 1798.150(b) from all Defendants.

64. On March 2, 2023, Plaintiff's counsel sent a CCPA notice letter to MKS's registered service agent, and if within the 30 days of deliver of such CCPA notice letter, MKS does not actually cure the noticed violation and provides Plaintiff with an express written statement that the violations have been cured and that no further violations shall occur (which Plaintiff believes any such cure is not possible under these facts and circumstances), Plaintiff and the Class shall seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident pursuant to Civil Code § 1798.150(b) from all Defendants.

THIRD CAUSE OF ACTION
Breach of California Security Notification Laws
California Civil Code § 1798.82
(On Behalf of Plaintiff and the Class Against All Defendants)

65. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if fully stated herein.

66. Pursuant to Civil Code § 1798.82(a), "A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable."

67. Civil Code § 1798.82 further provides, "(h) For purposes of this section, 'personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (4) Medical information. (5) Health insurance information. (i) .... (2) For purposes of this section, 'medical information' means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. (3) For purposes of this section, 'health insurance information' means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records."

68. MKS conducts business in California and owns or licenses computerized data which includes the personal information, within the meaning of Civil Code § 1798.82(h), of Plaintiff and the Class.

69. MKS's notification letter mailed to Plaintiff and the Class failed to provide, at a minimum, (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred, in violation of Civil Code § 1798.82(d)(2)(C).

70. Thus, Plaintiff and the Class have been injured by fact that Defendants did not provide all of the information minimally required by Civil Code § 1798.82(d), and by fact that Defendants did not disclose to them that their unencrypted personal information was, or was reasonably believed to have been, acquired by an unauthorized person in the most expedient time possible and without reasonable delay in violation of Civil Code § 1798.82(a). Defendants' delays providing all of the information required by Civil Code § 1798.82(d) and in informing in the most expedient time possible and without reasonable delay as required by Civil Code § 1798.82(a), have prevented Plaintiff and the Class from taking steps in the most expedient time possible to protect their unencrypted personal information from unauthorized use and/or identify theft.

71. Plaintiff and the Class seek recovery of their damages pursuant to Civil Code § 1798.84(b) and injunctive relief pursuant to Civil Code § 1798.84(e) from all Defendants.

FOURTH CAUSE OF ACTION
Unlawful and Unfair Business Acts and Practices in Violation of California Business & Professions Code §17200, *et seq*.
(On Behalf of Plaintiff and the Class Against All Defendants)

72. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if fully stated herein.

73. The acts, misrepresentations, omissions, practices, and non-disclosures of Defendants as alleged herein constituted unlawful and unfair business acts and practices within the meaning of California Business & Professions Code §§ 17200, *et seq*.

74. By the aforementioned business acts or practices, Defendants have engaged in "unlawful" business acts and practices in violation of the aforementioned statutes, including Civil Code §§ 56.13, 56.20, 56.245, 1798.82, and 1798.150. Plaintiff reserves the right to allege other

violations of law committed by Defendants which constitute unlawful acts or practices within the meaning of California Business & Professions Code §§ 17200, *et seq*.

75. By the aforementioned business acts or practices, Defendants have also engaged in "unfair" business acts or practices in that the harm caused by Defendants' failure to maintain adequate information security procedures and practices, including but not limited to, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions, failing to put into place reasonable or adequately computer systems and security practices to safeguard patients' identifiable medical information including access restrictions and encryption, failing to have adequate privacy policies and procedures in place that did not preserve the confidentiality of the medical and personal information of Plaintiff and the Class in their possession, and failing to protect and preserve confidentiality of medical and personal information of Plaintiff and the Class in their possession against disclosure and/or release, outweighs the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous, unethical, deceitful and offensive, and causes substantial injury to Plaintiff and the Class.

76. Plaintiff and the Class have suffered an injury in fact by acquiring less in their transactions with Defendants than they otherwise would have if Defendants would had adequately protected the confidentiality of their medical and personal identifying information.

77. The aforementioned unlawful, fraudulent and unfair business acts or practices conducted by Defendants have been committed in the past and continues to this day. Defendants have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or publicly issued comprehensive corrective notices to Plaintiff and the Class, and have not corrected or enacted adequate privacy policies and procedures to protect and preserve confidentiality of medical and personal identifying information of Plaintiff and the Class in their possession.

78. Because of Defendants' aforementioned conduct, Plaintiff and the Class have no other adequate remedy of law in that absent injunctive relief from the Court and Defendants are likely to continue to injure Plaintiff and the Class.

79. Pursuant to Business & Professions Code § 17203, Plaintiff and the Class seek an order of this Court for equitable and/or injunctive relief in the form of requiring Defendants to

correct its illegal conduct that is necessary and proper to prevent Defendants from repeating their illegal and wrongful practices as alleged above and protect and preserve confidentiality of medical and personal identifying information of Plaintiff and the Class in Defendants' possession that has already been accessed, exfiltrated, exfiltrated, stolen and viewed by at least one unauthorized third party because by way of Defendants' illegal and wrongful practices set forth above. Pursuant to Business & Professions Code § 17203, Plaintiff and the Class further seek an order of this Court for equitable and/or injunctive relief in the form of requiring Defendants to publicly issue comprehensive corrective notices.

80. Because this case is brought for the purposes of enforcing important rights affecting the public interest, Plaintiff and the Class also seek the recovery of attorneys' fees and costs in prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and other applicable law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully request that the Court grant Plaintiff and the proposed Class the following relief against Defendants, and each of them:

As for the First Cause of Action

1. For compensatory damages, punitive damages not to exceed three thousand dollars ($3,000), attorney's fees not to exceed one thousand dollars ($1,000), and the costs of litigation according to proof to Plaintiff individually and to each member of the Class pursuant to Civil Code § 56.35;
2. For actual damages according to proof to Plaintiff individually and to each member of the Class per violation pursuant to Civil Code § 56.36(b)(2);
3. For nominal damages in the amount of one thousand dollar ($1,000) per violation to Plaintiff individually and to each member of the Class and the Class pursuant to Civil Code § 56.36(b)(1);

/ / /

/ / /

/ / /

As for the Second Cause of Action

4. For actual damages according to proof to Plaintiff individually and to each member of the Class and the Class pursuant to Civil Code § 1798.150(a)(1)(A) and Civil Code § 1798.150(b);
5. For injunctive or declaratory relief pursuant to Civil Code § 1798.150(a)(1)(B);

As for the Third Cause of Action

6. For damages according to proof to Plaintiff individually and to each member of the Class and the Class pursuant to California Civil Code § 1798.84(b);
7. For injunctive relief pursuant to California Civil Code § 1798.84(e);

As for the Fourth Cause of Action

8. For an order awarding Plaintiff and the Class restitution of all monies wrongfully acquired by Defendants by means of such unlawful, fraudulent and unfair business acts and practices;
9. For injunctive relief in the form of an order instructing Defendants to prohibit the unauthorized release of medical and personal identifying information of Plaintiff and the Class, and to adequately maintain the confidentiality of the medical and personal identifying information of Plaintiff and the Class;
10. For injunctive relief in the form of an order enjoining Defendants from disclosing the medical and personal identifying information of Plaintiff and the Class without the prior written authorization of each Plaintiff and the Class member;

As to All Causes of Action

11. That the Court issue an Order certifying this action be certified as a class action on behalf of the proposed Class, appointing Plaintiff as representative of the proposed Class, and appointing Plaintiff's attorneys, as counsel for members of the proposed Class;
12. For an award of attorneys' fees as authorized by statute, including, but not limited to, the provisions of California Code of Civil Procedure § 1021.5, and as authorized under the "common fund" doctrine, and as authorized by the "substantial benefit" doctrine;
13. For costs of the suit;
14. For prejudgment interest at the legal rate; and

15. Any such further relief as this Court deems necessary, just, and proper.

Dated: March 3, 2023

KEEGAN & BAKER LLP

By: _____
Patrick N. Keegan, Esq.
Attorney for Plaintiff

DEMAND FOR JURY TRIAL

Plaintiff and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

Dated: March 3, 2023

KEEGAN & BAKER LLP

By: _____
Patrick N. Keegan, Esq.
Attorney for Plaintiff

Exhibit A

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 privacy@mksinst.com.

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

Sincerely,

MKS Instruments, Inc.