LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

April 13, 2018

VIA ELECTRONIC SUBMISSION

Attorney General Xavier Becerra
Attorney General's Office
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550

Re: Notification of Data Security Incident

Dear Attorney General Becerra:

We represent Inogen, Inc. ("Inogen") in connection with a recent data security incident which is described in greater detail below. Inogen takes the privacy and security of the information in its control very seriously and is taking steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On March 14, 2018, Inogen learned that messages within an employee email account may have been accessed without authorization and that some of those messages may have contained personal information belonging to some Inogen rental customers. As soon as Inogen discovered this incident, Inogen took steps to secure customer information. Inogen also required all email users to change their passwords and implemented multi-factor authentication for remote email access. Finally, Inogen launched an investigation and engaged a leading forensics firm to determine what happened and whether customer information contained within the email account had been accessed or acquired without authorization. It appears that customer names, addresses, telephone numbers, email addresses, dates of birth, dates of death, Medicare identification numbers, insurance policy information, and/or the type of medical equipment provided may have been accessed.

2. Number of California residents affected.

Inogen notified 3,251 California residents of this data security incident. Notification letters were mailed via first class U.S. mail on April 13, 2018. A sample copy of a notification letter provided to potentially impacted individuals is included with this letter.

3. Steps taken relating to the incident.

Inogen has taken affirmative steps to prevent a similar situation from arising in the future and to protect the privacy and security of all sensitive information in its possession. These steps have included working with a leading forensics firm to investigate this data security incident, implementing multi-factor authentication for remote email access, reducing administrative access to Outlook 365, and changing all user and administrative passwords.

4. Contact information.

Inogen is committed to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (971) 712-2795, or by e-mail at Sean.Hoar@LewisBrisbois.com.

Sincerely,

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure

inogen

C/O ID Experts
PO Box 10444
Dublin, Ohio 43017

To Enroll, Please Call:
(888) 235-5166
Or Visit:
https://ide.myidcare.com/inogen
Enrollment Code: <<CODE>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS 1>> <<ADDRESS 2>>
<<CITY>>, <<STATE>> <<ZIP>>

April 13, 2018

Subject: Notice of Data Breach

To The Next Of Kin Of <<FIRST NAME>> <<LAST NAME>>:

I am writing to inform you of a data security incident that may have affected your family member's personal information. We take the privacy and security of all personal information very seriously and regret any concern this incident may cause. This letter contains information about steps you can take to protect your family member's personal information and about resources we are making available to help.

What happened? Inogen learned on March 14, 2018 that messages within an email account belonging to an Inogen employee may have been accessed without authorization and that some of those messages may have contained some of your family member's personal information. As soon as we discovered this incident, we took steps to secure your family member's personal information. We also required all email users to change their passwords and implemented multi-factor authentication for remote email access. Finally, we launched an investigation and engaged a leading forensics firm to determine what happened and whether customer information contained within the email account had been accessed or acquired without authorization. While we have no evidence that your family member's information has been misused, out of an abundance of caution, we are informing you of the incident and providing you with the resources described in this letter.

What Information Was Involved? The incident may have involved your family member's name, address, telephone number, email address, date of birth, date of death, Medicare identification number, insurance policy information, and/or the type of medical equipment provided.

What Are We Doing? We take the security of all personal information that we store in our systems very seriously. As soon as we learned of this incident, we took the steps referenced above. We are also taking additional steps to enhance the security of personal information in order to prevent similar incidents from occurring in the future. In addition, we are offering identity theft protection services for a period of twelve (12) months at no cost through ID Experts® and are providing you with additional information about steps that you can take to protect your family member's personal information.

What You Can Do: While we are not aware of the misuse of any information potentially involved in this incident, we are notifying you out of an abundance of caution. Also, to help relieve concerns and to restore confidence following this incident, we have engaged ID Experts® to provide identity theft protection services at no cost. IDExperts® is a leader in risk mitigation and response. These services include twelve (12) months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery. The deadline to enroll in these services is July 13, 2018. We also recommend that you review the additional information provided with this letter about steps you can take to protect your family member's personal information. Credit monitoring may not be applicable if a deceased flag has been placed on your family member's credit file.

We encourage you to contact ID Experts® with any questions and to enroll in these free services by calling (888) 235-5166 or by going to https://ide.myidcare.com/inogen and using the Enrollment Code provided above. ID Experts® representatives are available Monday through Friday from 5 am - 5 pm Pacific Time. Please note the deadline to enroll is July 13, 2018. We encourage you to take full advantage of this service.

For more information: We sincerely regret any inconvenience or concern that this incident may cause you and remain dedicated to protecting all information. If you have any questions or need assistance, please call ID Experts® at (888) 235-5166 from 5:00 A.M. to 5:00 P.M. PST, Monday through Friday.

Sincerely,

Alex Tzoumas
Vice President, Internal Audit & Risk Management
Inogen, Inc.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion
P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Free Annual Report
P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf