DANA HOWARD
DIRECT DIAL: (859) 231-3018
dana.howard@skofirm.com

300 WEST VINE STREET
SUITE 2100
LEXINGTON, KY 40507-1801
MAIN: (859) 231-3000
FAX: (859) 253-1093

April 25, 2023

VIA ELECTRONIC MAIL TO IDTHEFT@OAG.STATE.MD.US

Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Brown:

In accordance with Md. Code Ann., Com. Law § 14-3504, we are writing on behalf of our client, Piramal Pharma Solutions, Inc. ("Piramal"), to notify you of a data security incident.

On March 23, 2023, Piramal's parent company, Piramal Pharma Solutions ("PPS"), learned that a local server at its Canadian subsidiary's facility in Aurora, Canada was not accessible. An investigation revealed that files on the local server were encrypted with lockbit ransomware. PPS immediately engaged IT professional, InfoSec, and PPS's security monitor partner to respond to and perform a full investigation of the incident. As a result of the investigation, PPS learned that an unauthorized actor accessed certain Piramal files and data stored on the local server.

Upon learning of the unauthorized access, PPS undertook a thorough review of the potentially affected data. On April 4, 2023, PPS determined and notified Piramal that data belonging to Piramal may have been impacted by this incident, including personal information. The information accessed without authorization during the incident varies by individual but may have included the full name, address, date of birth, and Social Security number of one (1) Maryland resident.

In accordance with Md. Code Ann., Com. Law § 14-3504,[1] Piramal will mail a notification letter to the one (1) Maryland resident whose personal information may have

[1] Notwithstanding its compliance with the Maryland notification statute, Piramal reserves any and all defenses and

been involved in the incident. The letter will be dispatched via U.S. Mail on April 26, 2023. A copy of the notification letter is enclosed.

Piramal and its parent company, PPS, understand the importance of protecting personal information and deeply regret the occurrence of the incident. To help protect the affected individuals, Piramal and PPS are offering free identity theft protection services. Further, Piramal and PPS are providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Please do not hesitate to contact me if you have any questions regarding this matter.

Very truly yours,

Dana R. Howard

DH:PTE

Enclosure

objections to claims relating to this incident, including, but not limited to, lack of personal jurisdiction.

Piramal Pharma Solutions, Inc.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB07388

[redacted]
[redacted]
[redacted], MD [redacted]

April 26, 2023

NOTIFICATION OF DATA BREACH

Dear [redacted]:

Piramal Pharma Solutions, Inc. ("Piramal") is writing to you today to provide information regarding a data security incident involving the computer systems and networks of our parent company Piramal Pharma Solutions ("PPS"), (the "Incident"). The Incident impacted certain data of Piramal, including information about Piramal's employees at its Lexington, Kentucky facility. Specifically, the exposed data involved personally identifiable information (PII) with some combination of your name, address, social security number, and/or date of birth. The purpose of this letter is to inform you of the contents of the data exposed during the Incident, the possible effects the Incident may have on your data security, and precautionary measures that Piramal and PPS have taken to help alleviate concerns you may have.

WHAT HAPPENED?

Beginning on or about March 23, 2023, files contained on a local server at PPS's Canadian subsidiary's facility in Aurora, Canada, were encrypted by ransomware. Through investigation, it was determined that the cyber attacker also gained access to a limited number of other files on PPS's global network, including certain files of Piramal.

WHAT INFORMATION WAS INVOLVED?

Through investigation, it was determined that the accessed files included information about you, including **your name, contact information, social security number, and/or birth date**, and that such files may have been exfiltrated. Piramal has reported the Incident to law enforcement.

WHAT ARE WE DOING?

PPS and Piramal have made immediate enhancements to its systems, security, and practices. Additionally, PPS has engaged appropriate experts to assist in conducting a full review of the security practices and systems to ensure that enhanced security protocols are in place going forward. Piramal is committed to helping those individuals who may have been impacted by this unfortunate situation.

In response to the Incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 1 year from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud, as well as a $1,000,000 insurance reimbursement policy. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

WHAT YOU CAN DO.

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/piramal** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted].

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

OTHER IMPORTANT INFORMATION.

Regardless of whether you choose to enroll in these credit monitoring services, we strongly urge you to consider the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)	**Equifax (1-800-525-6285)**	**TransUnion (1-800-680-7289)**
P.O. Box 4500	**P.O. Box 740241**	**P.O. Box 2000**
Allen, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
www.experian.com	www.equifax.com	www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report,** we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Piramal

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

Maryland resident may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, by sending an email to idtheft@oag.state.md.us, or by calling 410-576-6491.

FOR MORE INFORMATION

Cyberscout representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. ET, Monday through Friday, excluding holidays. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

While Cyberscout representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with Piramal regarding this incident. If so, please call Simon Scholte at 859-[redacted] from 9:00 a.m. to 4:30 p.m. EST, Monday through Friday, excluding holidays.

At Piramal we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Simon Scholte
Vice President – Lexington Site Head