

EXHIBIT 1

By providing this notice, Pharmaceuticals International, Inc. (“PII”) does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 22, 2024, PII became aware of suspicious activity occurring within its computer environment (the “Event”). Upon learning of this activity, PII promptly launched an investigation into the nature and scope of the Event with the assistance of third-party cybersecurity and digital forensics specialists. The investigation determined that, in relation to the activity, certain information was accessed and acquired by an unauthorized actor between July 22, 2024, and July 29, 2024. In response, PII conducted a comprehensive review of the contents of data to confirm what information was impacted and to whom it related. PII then analyzed the underlying documents to validate the records and confirm address information for the individuals. This review was recently completed.

The information that could have been subject to unauthorized access includes name and Social Security number. While PII is unaware of any identity theft or fraud related to this Event, they are providing notification out of an abundance of caution.

Notice to Nebraska Resident

On December 22, 2025, PII provided written notice of this incident to one (1) Nebraska resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the Event, PII moved quickly to investigate and respond to the incident, assess the security of PII systems, and identify potentially affected individuals. PII is also working to implement additional safeguards and cybersecurity training for its employees. PII is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, PII is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud. PII is 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.

PII is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A



<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



<<Date>> (Format: Month Day, Year)

<<b2b_text_1 (NOTICE OF DATA BREACH)>>

Dear <<first_name>> <<last_name>>:

Pharmaceuticals International, Inc. (“PII”) is writing to notify you of a recent incident that may affect the privacy of some of your information. PII takes the protection of your information very seriously, and although we have no evidence of identity theft or fraud as a result of this incident, this letter provides you with information about the incident, our response, and steps you may wish to take to protect against possible misuse of your information.

What Happened? On July 22, 2024 PII identified suspicious activity occurring within its computer environment. Upon learning of this activity, PII immediately took steps to secure their environment and initiated an investigation into the nature and scope of the activity, with the assistance of cybersecurity specialists. The investigation determined that, in relation to the activity, certain information was accessed and acquired by an unauthorized actor between July 22, 2024, and July 29, 2024. In response, we conducted a comprehensive review of the contents of the impacted information to confirm what information was impacted and to whom it related. We recently completed this review and determined that information relating to you was impacted.

What Information Was Involved? The investigation determined that your name and Social Security number may have been impacted. We are unaware of any identity theft or fraud related to this event and we are notifying you in an abundance of caution.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this event very seriously. We immediately took steps to secure our environment and initiated a comprehensive incident response. We also reviewed our security policies and procedures and are assessing our existing security measures to reduce the risk of similar future events.

Although we are unaware of any identity theft or fraud resulting from this incident, PII is offering you access to <<Monitoring Term Length (Months)>> months of complimentary credit monitoring and identity protection services through Kroll. Details of this offer and instructions on how to enroll in the services may be found in the attached *Steps You Can Take to Help Protect Your Personal Information*. If you would like to enroll in these services you will need to follow the attached instructions, as we are unable to enroll you automatically.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and to immediately report any suspicious activity or incidents of suspected identity theft or fraud to your bank or other financial institution(s). Additional information may be found in the attached *Steps You Can Take to Help Protect Your Personal Information*.

For More Information. If you have questions regarding this incident, you may contact our dedicated assistance line at (844) 354-1388, Monday through Friday, between the hours of 9:00 AM and 6:30 PM Eastern Time, excluding U.S. holidays. You may also write to PII at 10819 Gilroy Rd., Hunt Valley, MD 21031.

Sincerely,

Ryan Schwartz
Director
Pharmaceuticals International, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll, please visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax

<https://www.equifax.com/personal/credit-report-services/>

1-888-298-0045

Equifax Fraud Alert, P.O. Box
105069 Atlanta, GA 30348-5069

Equifax Credit Freeze, P.O. Box
105788 Atlanta, GA 30348-5788

Experian

<https://www.experian.com/help/>

1-888-397-3742

Experian Fraud Alert, P.O. Box 9554,
Allen, TX 75013

Experian Credit Freeze, P.O. Box
9554, Allen, TX 75013

TransUnion

<https://www.transunion.com/data-breach-help>

1-833-799-5355

TransUnion Fraud Alert, P.O. Box
2000, Chester, PA 19016

TransUnion Credit Freeze, P.O. Box
160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.