

October 2, 2024

**CONFIDENTIAL COMMUNICATION
VIA EMAIL**

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Incident

Dear Sir or Madam:

We are writing on behalf of our client, RK Pharma Inc. ("**RK Pharma**")¹, to inform you of a systems issue RK Pharma experienced which resulted in the encryption of certain of its network systems and servers.

On August 7, 2024, RK Pharma experienced a systems outage that it quickly discovered had been caused by the encryption of certain of its network systems servers. In response, RK Pharma took its system offline to prevent further impact and launched an internal investigation by engaging expert forensics consultants. While investigating the nature and extent of the incident, RK Pharma worked carefully to determine which systems could be brought back online and took proactive measures to contain and mitigate systems issues, including purchasing new equipment and performing forensic scans on all systems. As counsel, we have also notified and are working with law enforcement in its investigation of the threat actor.

From its investigation, RK Pharma has determined that the outage resulted from a cyberattack on August 7, 2024, that was intended to encrypt network servers, prevent employees from accessing company systems, and cause business disruption. While there was no evidence that specific information was targeted, due to the widespread nature of the attack, coupled with limited forensic details due to the unfortunate nature of these kinds of encryption events, the investigation revealed that certain personal information may have been impacted. RK Pharma is notifying individuals whose personal information may have been impacted out of an abundance of caution. Depending on the relationship of the individual to RK Pharma, the personal information may have included: names, addresses, social security numbers, passport numbers, driver's license numbers, financial account information, health insurance information for worker's compensation claims, and dates of birth.

¹ RK Pharma is based in Pearl River, New York.

October 2, 2024
Page 2

Because of this discovery, we are now reaching out to notify your office of the incident. From the investigation, it appears that one Maryland resident may have been impacted by the incident. Notifications to the impacted individual in Maryland was sent out by mail on or about October 2, 2024. A sample copy of that notice is enclosed.

Even though RK Pharma has no evidence that any personal information has been fraudulently used as a result of this incident, out of an abundance of caution, RK Pharma is offering impacted individuals 24 months of free fraud detection monitoring and identity theft protection through Experian, the data breach and recovery services expert, via their IdentityWorks™ product. Further, in its written notification, RK Pharma has provided impacted individuals with detailed information regarding additional steps they can take to protect themselves and their personal information.

We assure you that our client, RK Pharma, takes this issue, and the privacy and security of its employees, very seriously. If you have any questions or require further information, please feel free to contact me at krollins@sheppardmullin.com or (212) 634-3077.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kari M. Rollins", with a stylized flourish at the end.

Kari M. Rollins
for SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

Attachment: Sample Notification Letter



Return Mail Processing
PO Box 999
Suwanee, GA 30024

116*****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



October 2, 2024

Dear Sample A. Sample:

Re: Notice of Data Incident

We are writing to let you know about a cyber-attack that may involve certain of your personal information. This notice explains what happened, what information may have been affected, what measures we are taking in response, and steps you can take to protect yourself.

What Happened

On August 7, 2024 we discovered that our systems were experiencing an issue that prevented employees from accessing certain systems and servers. In response, we immediately launched an internal investigation and engaged outside expert consultants. At the same time, we took proactive measures to contain and mitigate the systems issue, including by taking certain aspects of our network and servers down. We also contacted law enforcement and have been cooperating with them since.

From our investigation, supported by our external experts, we discovered the systems outage was caused by a cyber-attack that encrypted some network servers. Based on our investigations we believe it is possible that the attack that caused the systems outage may have impacted certain personal information, as described below. Our investigation has not revealed evidence of fraudulent data use. However, we want to provide you with information you can use to proactively take steps to protect yourself and your information.

What Information Was Involved

Our investigation has revealed that certain network servers and systems were encrypted during the attack. Some of these encrypted systems held, among other things, electronic files which contained certain of your personal information. As a result, we believe it is possible that the encryption event may have incidentally impacted personal information that we maintain about you. Which specific information of yours was impacted depends on the data we maintain about you either as an employee or a dependent of an employee, but may have included: name, address, social security number, financial account information for employees that joined prior to 2020, passport numbers, driver's license numbers, tax information, date of birth, and health insurance information for employees who may have submitted a worker's compensation claim.

What We Are Doing

As noted, as soon as we discovered the systems issue, we immediately launched an internal investigation and engaged the assistance of outside forensic experts and experienced cyber-consultants. At the same time, we took proactive measures to contain and mitigate the systems issue, including by taking certain aspects of our network and equipment down, restoring our systems from new servers unaffected by the

systems outage and performing additional forensic scans on our systems. Through our cybersecurity counsel, we also contacted law enforcement and have been working with them to uncover information about the attackers.

We take this matter seriously, and in addition to the steps already described, RK Pharma is offering you 24 months of **free** fraud detection and identity theft protection. If you wish to take advantage of these services, activation instructions are below.

What You Can Do

Though we have no evidence that any of your personal information has been misused, we encourage you to remain vigilant by reviewing their account statements and credit reports closely. At the end of this letter, we have provided you with additional information regarding steps you can proactively take to further protect yourself and your personal information. It describes information about (1) reporting suspicious activity or suspected identity theft, (2) credit reports, (3) fraud alerts, (4) credit/security freezes, and (5) information about taxes. We encourage you to review that additional information.

Free Credit Monitoring and Identity Theft Protection: Even though we have no evidence that your personal information has been fraudulently used or publicly disclosed, as a precautionary measure, we are offering to provide you with 24 months of free identity monitoring, fraud consultation, and identity theft restoration services through Experian's IdentityWorks™ product. To take advantage of these free services, please follow the steps below:

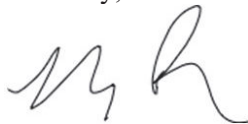
- Ensure that you enroll by December 31, 2024. Your code will not work after this date.
- Visit the Experian IdentityWorks™ website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, please contact Experian's customer care team at 833-918-5937 by December 31, 2024. Be prepared to provide engagement number B132270 as proof of eligibility for the identity restoration services by Experian.

For More Information

We take seriously the security and privacy of your information, and deeply regret any inconvenience this may cause. If you have any questions, please call us at 833-918-5937, toll-free Monday through Friday from 8 am – 8 pm Central (excluding major U.S. holidays).

Sincerely,



Mary Pruce
Head of Human Resources, RK Pharma Inc.

Additional Steps You Can Take to Protect Your Personal Information

Report Suspicious Activity or Suspected Identity Theft. If you detect any unauthorized or suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. If you suspect any identity theft has occurred, you can contact your local law enforcement by filing a police report or the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT (1-877-438-4338), by writing to the FTC at 600 Pennsylvania Avenue, NW Washington DC 20580, or online at www.ftc.gov. You can also contact your state Attorney General (information for some specific AGs is listed below):

- Maryland residents may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us>, by sending an email to idtheft@oag.state.md.us, or by calling 410-576-6491.
- New York residents may wish to review information on security breach response and identity theft prevention and protection information provided by the New York Attorney General at <https://ag.ny.gov/internet/privacy-and-identity-theft> or by calling 1-800-771-7755 and by the New York Department of State, Division of Consumer Protection at <https://dos.ny.gov>, or by calling 800-697-1220.
- North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/>, by calling 877-566-7226, or by writing to 9001 Mail Service Center, Raleigh, NC 27699.

Contacting the Internal Revenue Service: If you believe you are the victim of tax fraud or that somebody has filed or accessed your tax information, you should immediately contact the IRS or state tax agency as appropriate. For the IRS, you can use Form 14039 (<https://www.irs.gov/pub/irs-pdf/f14039.pdf>). You can also call them at 800-908-4490 (Identity Theft Hotline). Information on how to contact your state department of revenue to make similar reporting may be found by going to <http://www.taxadmin.org/state-tax-agencies>.

Credit Reports/Fraud Alerts/Credit and Security Freezes: Under federal law, you are entitled to one free copy of your credit report every 12 months. You can request a free credit report once a year at www.annualcreditreport.com, by calling (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. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

As a precautionary step, to protect yourself from possible identity theft you can place a fraud alert on your bank accounts and credit file. A fraud alert tells creditors to follow certain procedures before opening a new account in your name or changing your existing account. You may call any one of the three major credit bureaus listed below to place a fraud alert on your file. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. All three credit reports will be sent to you, free of charge, for your review.

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. 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 apply for a new credit card, loan, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze on your file you

may be required to provide the consumer reporting agency with information that identifies you including your Social Security Number. There may be a fee for this service based on state. To put a security freeze on your credit file contact the consumer reporting agencies listed below.

You may also contact the three U.S. credit reporting agencies as follows:

Agency	Credit Report Contact	Fraud Alert Contact	Credit/Security Freeze Contact
TransUnion LLC	TransUnion LLC Consumer Disclosure Center, P.O. Box 1000, Chester, PA 19016; (800) 888-4213; https://www.transunion.com	TransUnion Fraud Victim Assistance, P.O. Box 2000, Chester, PA 19016; (800) 680-7289; https://www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 160, Woodlyn, PA 19094; (888) 909-8872; https://www.transunion.com/credit-freeze/
Experian	P.O. Box 2002, Allen, TX 75013; (888) 397-3742; https://www.experian.com/consumer-products/free-credit-report.html	Experian, P.O. Box 9554, Allen, TX 75013; (888) 397-3742; https://www.experian.com/fraud/center.html	P.O. Box 9554, Allen, TX 75013; (888) 397-3742; https://www.experian.com/freeze/center.html
Equifax Information Services LLC	Equifax Information Services LLC, P.O. Box 740241, Atlanta, GA 30374; (866) 349-5191; https://www.equifax.com/personal/credit-report-services/	Equifax Information Services LLC, P.O. Box 105069, Atlanta, GA 30348-5069; (800) 525-6285; https://www.equifax.com/personal/credit-report-services/	Equifax Information Services LLC, P.O. Box 105788, Atlanta, GA 30348-5788; (888) 298-0045 or (800) 349-9960; https://www.equifax.com/personal/credit-report-services/

IRS Identity Protection PIN: The IRS offers an Identity Protection PIN, which is a six digit number that prevents someone else from filing a tax return using your Social Security number. The Identity Protection PIN is known only to you and the IRS. For more information and to obtain an Identity Protection PIN, please visit the IRS website at <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.