KING & SPALDING

King & Spalding LLP
1180 Peachtree Street N.E.
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100
www.kslaw.com

Phyllis B. Sumner
Direct Dial: +1 404 572 4799
Direct Fax: +1 404 572 5100
psumner@kslaw.com

October 8, 2021

To: Tom Miller
Office of the Iowa Attorney General
consumer@ag.iowa.gov

Re: Notice of Data Breach Affecting ReproSource

Dear Attorney General Miller,

I write on behalf of ReproSource Fertility Diagnostics, Inc. ("ReproSource" or "Company") regarding a security incident. On August 8, 2021, an unauthorized party accessed the ReproSource network. The Company discovered ransomware on the morning of August 10, and in less than an hour severed all network connection activity and contained the incident. ReproSource immediately launched a comprehensive investigation to determine the cause and scope of the incident, retained leading cybersecurity experts to assist with its investigation, confirmed containment of the ransomware, and quickly and securely recovered operations. Additionally, the Company promptly notified law enforcement.

While the Company's investigation did not confirm that the unauthorized party acquired data in the incident, out of an abundance of caution, we are notifying individuals whose personal information may have been accessed. ReproSource undertook an extensive analysis of its files to determine which individuals and data may have been affected, and on September 24, 2021, the Company began identifying individuals potentially affected. Although our data analysis is ongoing, in the interest of initiating notifications, we are in the process of informing individuals whose personal information may have been affected and offering them a one-year free subscription to Kroll's identity monitoring services.

Based on its investigation to date, ReproSource has determined that personal information in files that may have been accessed or acquired without authorization included: names, addresses, phone numbers, email addresses, dates of birth, billing and health information, such as CPT codes, diagnosis codes, test requisitions and results, test reports and/or medical history information, health insurance or group plan identification names and numbers, and other information provided by individuals or by treating physicians. For a small group of individuals, personal information may have included driver's license numbers, passport numbers, social security numbers, financial account numbers and credit card numbers.

We began mailing notifications on October 8, 2021. Because our data analysis remains ongoing, we have not yet been able to determine the final number of Iowa residents impacted. To

date, we have identified approximately 74 Iowa residents who may have been impacted by the incident. As our analysis progresses, we will keep your office informed if we identify additional Iowa residents.

ReproSource has enhanced its cybersecurity by adding additional monitoring and detection tools as safeguards against ransomware and other cyber threats.

Unaddressed copies of the letters are attached. ReproSource has also established a call center to answer patients' questions ((855) 732-0717).

ReproSource remains committed to protecting its patients' personal information and assisting those who may have been affected by this incident. ReproSource is providing notices to individuals pursuant to 45 CFR §§ 164.400-414 and applicable state laws. By virtue of this notice, the Company does not waive any rights and reserves all rights under such laws. Please do not hesitate to contact me if you have any questions regarding this letter.

Sincerely,

Phyllis B. Sumner

Enclosures

ReproSource®
Illuminating Pathways to Reproductive Health™

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you about a data security incident that may have affected the privacy of some of your personal information. We want you to understand the steps we have taken to address this issue and additional steps that can be taken to protect your personal information. This letter explains the incident and offers you assistance for safeguarding your information, including complimentary identity monitoring services.

What Happened

On August 8, 2021, an unauthorized party accessed the ReproSource network. We discovered ransomware on the morning of August 10, and in less than an hour we severed all network connection activity and contained the incident. We immediately launched a comprehensive investigation to determine the cause and scope of the incident. We retained leading cybersecurity experts to assist with our investigation, confirmed containment of the ransomware, and quickly and securely recovered operations. Additionally, we promptly notified law enforcement.

While our investigation did not confirm that the unauthorized party acquired data in the incident, out of an abundance of caution, we are notifying individuals whose personal information may have been accessed.

We undertook an extensive analysis of our files to determine which individuals and data may have been affected and, on September 24, 2021, we identified individuals potentially affected. Although our data analysis is ongoing, in the interest of initiating notifications, we are sending you this notice and providing the services outlined in this letter.

What Information Was Involved

Based on our investigation to date, some of your personal information was in files that may have been accessed or acquired without authorization. This information included your name and one or more of the following: address, phone number, email address, date of birth, billing and health information, such as CPT codes, diagnosis codes, test requisitions and results, test reports and/or medical history information, health insurance or group plan identification names and numbers, and other information provided by you or your treating physician. As previously noted, since our data analysis is ongoing, we will follow up with you as appropriate if we identify other types of personal information that may have been accessed.

What We Are Doing

As discussed above, upon learning of the attack, we immediately severed all network connection activity and contained the incident. We also enhanced our cybersecurity by adding additional monitoring and detection tools as safeguards against ransomware and other cyber threats.

What You Can Do

To help relieve concerns following this incident, we have secured the services of Kroll Inc. to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **January 6, 2022** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

Additional information describing your services is included with this letter.

Please review the "Additional Resources" section included with this letter below. This section describes additional steps you can take to help protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

More Information

ReproSource is committed to data protection. We regularly review our physical and electronic safeguards to protect personal information, and we will continue to take appropriate steps to safeguard patient information and our systems.

We greatly value our relationship and deeply regret any inconvenience or concern this may have caused. If you have questions, please call **(855) 732-0717,** Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Sincerely,

ReproSource

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.