Fisher Broyles

Edmund F. Brown, Esq.
Partner
Galleria at PNC Plaza
20 S. 3 Street, Suite 210
Columbus, Ohio 43215
Direct: (614) 245-8418
Edmund. brown@fisherbroyles.com

www.fisherbroyles.com

June 29, 2023

Via E-mail Delivery (DOJ-CPB@doj.nh.gov)
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Breach

Dear Consumer Protection Section:

This firm represents ARx Patient Solutions and its affiliate pharmacy, ARx Patient Solutions Pharmacy ("ARx" or the "Company"). Enclosed please find the *Notice of Data Breach* with respect to a security incident involving the Company's information.

It was determined that in March of 2022, an employee M365 account was compromised and accessed by an unauthorized third party. On discovery of the incident, ARx disabled the account, contained the disruption, engaged an industry-leading cybersecurity firm to complete an investigation and accelerated implementation of key initiatives to strengthen our systems and security protocols. Based on findings from the investigation, ARx has determined that certain personal information belonging to 191 New Hampshire residents was contained in files within the M365 account and potentially accessed by an unauthorized third party.

Based on a thorough investigation of the data, it was determined that information related to individual's

. Based on our investigation and dark web monitoring, there is no evidence of misuse of any of this information.

In addition, to provided direct notice to the impacted New Hampshire residents on or about June 30, 2023, ARx will provide substitute breach notification, consisting of conspicuous posting of the notice on the Company's Web site and notification to media nationwide. A draft of the notification letter being sent to New Hampshire residents is attached as Exhibit A. The notification outlines the nature of the incident, the steps that ARx took to remediate the incident and offers complimentary identify protection and credit monitoring services to the affected individuals. The letter also contains specific instructions for enrolling in the free services previously described.

Should you have any questions or concerns, please contact me directly at or at

Sincerely,

Edmund F. Brown, Partner
FisherBroyles, LLP

EXHIBIT A

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

Parent or Guardian of
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

ARx Patient Solutions, in cooperation with its affiliate pharmacy, ARx Patient Solutions Pharmacy, greatly appreciates the opportunity to deliver therapy initiation and patient support programs. We also take our data security responsibilities seriously and have information to share on a data security incident we experienced. This letter shares information on what happened, what information was involved and what actions we've taken and are currently engaged in.

What Happened.

It was determined that in March of 2022, an employee email account was compromised and accessed by an unauthorized third party. On discovery of the incident, we disabled the account, contained the disruption, engaged an industry-leading cybersecurity firm to complete an investigation and accelerated implementation of key initiatives to strengthen our systems and security protocols. Based on findings from the investigation, ARx Patient Solutions has determined that personal information belonging to your child was contained in files within the email account and potentially accessed by an unauthorized third party.

What Information Was Involved.

Based on a thorough investigation of the data, it was determined that information related to individual's

. Based on our investigation and dark web monitoring, there is no evidence of misuse of any of this information.

What We Have Done.

Following the incident, the account was secured. ARx Patient Solutions also strengthened systems and protocols for our employees, patients and customers by implementing XDR and threat monitoring systems, proactive vulnerability management programs, active systems scanning and significant investments in the Security Operations department and policy additions.

What We Are Doing.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration 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.

Visit to activate and take advantage of your Minor Identity Monitoring services.
*You have until **<<b2b_text_6(activation deadline)>>** to activate your Minor Identity Monitoring services.*
Membership Number: **<<Membership Number s_n>>**

EXHIBIT A

For more information about Kroll and your Identity Monitoring services, you can visit . Additional information describing your services is included with this letter.

What You Can Do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your child's identity, 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 child's credit file.

For More Information.

If you have questions, please call , Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your child's membership number ready.

Protecting your child's information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction. We apologize for any inconvenience or concern this may have caused. Please know that we have taken steps to prevent this from happening again in the future. The safety and security of your personal information remains a top priority of ARx Patient Solutions.

Sincerely,

Kelly Williams
Privacy Officer

EXHIBIT A

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 **1-877322-8228**.

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, 1-877566-7226.

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

EXHIBIT A

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:

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

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 activate services, a U.S. Social Security number and U.S. residential address is required.

EXHIBIT A

<<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>>,

ARx Patient Solutions, in cooperation with its affiliate pharmacy, ARx Patient Solutions Pharmacy, greatly appreciates the opportunity to deliver therapy initiation and patient support programs. We also take our data security responsibilities seriously and have information to share on a data security incident we experienced. This letter shares information on what happened, what information was involved and what actions we've taken and are currently engaged in.

What Happened.

It was determined that in March of 2022, an employee email account was compromised and accessed by an unauthorized third party. On discovery of the incident, we disabled the account, contained the disruption, engaged an industry-leading cybersecurity firm to complete an investigation and accelerated implementation of key initiatives to strengthen our systems and security protocols. Based on findings from the investigation, ARx Patient Solutions has determined that personal information belonging to you was contained in files within the email account and potentially accessed by an unauthorized third party.

What Information Was Involved.

Based on a thorough investigation of the data, it was determined that information related to individual's

may have been accessed. Based on our investigation and dark web monitoring, there is no evidence of misuse of any of this information.

What We Have Done.

Following the incident, the account was secured. ARx Patient Solutions also strengthened systems and protocols for our employees, patients and customers by implementing XDR and threat monitoring systems, proactive vulnerability management programs, active systems scanning and significant investments in the Security Operations department and policy additions.

What We Are Doing.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll 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, fraud consultation, and identity theft restoration.

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>>**

EXHIBIT A

For more information about Kroll and your Identity Monitoring services, you can visit Additional information describing your services is included with this letter.

What You Can Do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, 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.

For More Information.

If you have questions, please call (, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering demonstrate our continued commitment to your security and satisfaction. We apologize for any inconvenience or concern this may have caused. Please know that we have taken steps to prevent this from happening again in the future. The safety and security of your personal information remains a top priority of ARx Patient Solutions.

Sincerely,

Kelly Williams
Privacy Officer

EXHIBIT A

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 **1-877322-8228**.

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, 1-877566-7226.

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

EXHIBIT A

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

You will 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'll 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.

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.