

JacksonLewis

Jackson Lewis P.C.
666 Third Avenue
New York NY 10017-4030
(212) 545-4000 Main
(212) 972-3213 Fax
jacksonlewis.com

DIRECT DIAL: (212) 545-4063
EMAIL ADDRESS: DAMON.SILVER@JACKSONLEWIS.COM

July 6, 2022

VIA FIRST-CLASS MAIL

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



Re: **Data Incident Notification**

Dear Sir or Madam:

We are writing to notify your office of a data security incident affecting three (3) Maryland residents. We are submitting this notice as counsel for Practice Resources, LLC, 1001 West Fayette St., Suite 400, Syracuse, NY 13204 ("PRL"), and on behalf of the following additional entities, to which PRL provides professional services:

FamilyCare Medical Group, PC ("FCMG")
Upstate Community Medical, PC ("UCM")

On April 12, 2022, PRL was subject to a ransomware attack ("Incident"). With assistance from third-party experts, it took immediate steps to secure its systems and investigate the nature and scope of the Incident. As part of its extensive investigation, PRL worked diligently to identify any PII that may have been subject to unauthorized access or acquisition as a result of the Incident. PRL has not found any evidence that personal information was misused as a result of the Incident.

On May 4, 2022, PRL informed FCMG and UCM that the Incident may have resulted in unauthorized access to or acquisition of their data. On or about May 16, 2022, PRL determined that this data may have included PII related to current or former employees of PRL, FCMG, or UCM who reside in Maryland. The categories of PII involved in the Incident are names, dates of birth, and social security numbers.

Out of an abundance of caution, and in accordance with applicable law, PRL will provide notice to the affected Maryland residents, in the forms enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused. Additionally, PRL has arranged for the individuals to enroll in free credit monitoring and related services for 12 months, including identity theft insurance up to \$1,000,000 as well as identity recovery and restoration services.

PRL treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, PRL has taken a number of steps to further secure its

systems. Specifically, it has replaced or rebuilt from scratch all of the systems impacted by the Incident; has deployed endpoint detection and response within its environment and will continue to utilize this solution on a going forward basis; and is in the process of transitioning to Microsoft 365, enabling multi-factor authentication, upgrading to an air-gapped backup solution, and thoroughly reviewing and upgrading its data security policies and procedures.

PRL will continue to monitor this situation and will update you on any significant developments. If you require any additional information on this matter, please contact me.¹

Sincerely,

JACKSON LEWIS P.C.

/s/ Damon W. Silver
Damon W. Silver

Enclosures

¹ Please note that PRL, FCMG, and UCM are not, by submitting this letter, agreeing to the jurisdiction of State of Maryland, nor waiving their right to challenge jurisdiction in any subsequent actions.

EXHIBIT “A”



To Enroll, Please Call:
1-833-940-2458
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

July 5, 2022

Incident Notice

Dear <<First Name>> <<Last Name>>,

What Happened

On April 12, 2022, Practice Resources, LLC (“PRL”) was subject to a ransomware attack (the “Incident”). With assistance from third-party experts, we took immediate steps to secure our systems and investigate the nature and scope of the Incident. As part of our extensive investigation, we worked diligently to identify any personally identifiable information (“PII”) that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about May 16, 2022, we determined that the Incident may have impacted PII related to you. However, we have not found any evidence that your information was misused.

What Information Was Involved

The Incident may have resulted in unauthorized access to or acquisition of employment records containing your name, date of birth, and social security number.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we have arranged for IDX to provide you 12 months of free credit monitoring and related services. To enroll, please visit <https://app.idx.us/account-creation/protect> or call 1-833-940-2458. Your enrollment code is <<enrollment code>>. To receive these services, please be sure to enroll by October 5, 2022.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, we have implemented a series of cybersecurity enhancements and will soon roll out others.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

For More Information

Depending on the circumstances, we may be providing this notice on our own behalf and/or on behalf of an entity to which we provide professional services. Those entities are listed here <https://www.prldocs.com/wp-content/uploads/2022/06/PRL-List-of-Employers-on-Whose-Behalf-PRL-is-Notifying.pdf>. If you have questions or concerns, please call our dedicated assistance line at 1-833-940-2458, Monday through Friday from 6 am - 6 pm Pacific Time. We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

David Barletta
President / Chief Executive Officer
Practice Resources, LLC

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:
 - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
 - You can also receive information from these agencies about avoiding identity theft, such as by placing a “security freeze” on your credit accounts.
 - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
 - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax
P.O. Box 740256
Atlanta, GA 30374
(866) 510-4211
psol@equifax.com
www.equifax.com

Experian
P.O. Box 2390
Allen, TX 75013
(866) 751-1323
Databreachinfo@experian.com
www.experian.com/

TransUnion
P.O. Box 1000
Chester, PA 19022
(800) 888-4213
<https://tudatabreach.tnwreports.com/>
www.transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a “security freeze” on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement or the attorney general, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

4. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, marylandattorneygeneral.gov.
5. *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to https://www.ffnm.org/_kcms-doc/1254/38712/Credit-Freeze-Q-A-New-Mexico-Sept-2017.pdf.

6. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
7. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

UPSTATE

COMMUNITY MEDICAL

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-940-2458

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: [XXXXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

July 5, 2022

Incident Notice

Dear <<First Name>> <<Last Name>>,

What Happened

On April 12, 2022, Practice Resources, LLC ("PRL") was subject to a ransomware attack (the "Incident"). PRL (1001 West Fayette Street, Suite 400, Syracuse, New York 13204; 866.310.2409) is a third-party vendor of Upstate Community Medical, P.C. ("UCM") (4900 Broad Rd, Syracuse, NY 13215; 315.492.5011) that aids with payroll processing, among other things. With assistance from third-party experts, PRL took immediate steps to secure its systems and investigate the nature and scope of the Incident. As part of its extensive investigation, PRL worked diligently to identify any personally identifiable information ("PII") that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about May 16, 2022, it was determined that the Incident may have impacted PII related to you. Significantly, PRL has not found any evidence that your information was misused.

What Information Was Involved

The Incident may have resulted in unauthorized access to or acquisition of employment records containing your name, date of birth, and social security number.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, PRL has arranged for IDX to provide you 12 months of free credit monitoring and related services. To enroll, please visit <https://app.idx.us/account-creation/protect> or call 1-833-940-2458. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Your enrollment code is <<enrollment code>>. To receive these services, please be sure to enroll by October 5, 2022.

UCM and PRL treats all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, PRL has implemented a series of cybersecurity enhancements and will soon roll out others and UCM reviewed its system infrastructure and determined there were currently no issues.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

If you have questions or concerns, please call the PRL dedicated assistance line at 1-833-940-2458, Monday through Friday from 6 am - 6 pm Pacific Time. We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

Amy M. Rhone
Upstate Community Medical P.C. Executive Director

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:
 - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
 - You can also receive information from these agencies about avoiding identity theft, such as by placing a “security freeze” on your credit accounts.
 - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
 - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax
P.O. Box 740256
Atlanta, GA 30374
866-510-4211
psol@equifax.com
www.equifax.com

Experian
P.O. Box 2390
Allen, TX 75013
866-751-1323
Databreachinfo@experian.com
www.experian.com/

TransUnion
P.O. Box 1000
Chester, PA 19022
800-888-4213
<https://tudatabreach.tnwreports.com/>
www.transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a “security freeze” on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling 877-438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement or the attorney general, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

4. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, marylandattorneygeneral.gov.
5. *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to https://www.ffnm.org/_/kcms-doc/1254/38712/Credit-Freeze-Q-A-New-Mexico-Sept-2017.pdf.

6. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State's Division of Consumer Protection, 800-697-1220 or <https://dos.ny.gov/consumer-protection>.