



May 19, 2022

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

MAILED
MAY 19 2022 PM 12:03
U.S. DEPARTMENT OF JUSTICE

Via Certified Mail; Return Receipt Requested:

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Cybersecurity Incident Involving PAR, Inc.

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents PAR, Inc. (“PAR”), a publisher of psychological assessment materials, with respect to a recent data privacy incident that was first discovered by PAR on March 21, 2022 (hereinafter, the “Incident”). PAR takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of New Hampshire residents being notified, and the steps that PAR has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On March 21st, 2022, PAR was subject to a data security incident that impacted its information systems. Upon discovery of the incident, PAR promptly engaged a team of cyber security professionals to assist with the recovery of its business services, and to conduct a forensic investigation to fully determine the scope and the overall impact of the incident. After a thorough investigation, PAR concluded some sensitive personal information from its systems may have been accessed by an unauthorized actor.

Although PAR is unaware of any fraudulent misuse of information, it is possible that individuals’ name, address, and Social Security Number may have been exposed as a result of this unauthorized activity.

As of this writing, PAR has not received any reports of related identity theft since the date of the incident (March 21, 2022 to present).

2. Number of New Hampshire residents affected.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com



A total of 13 New Hampshire residents have been potentially affected by this incident. Notification letters to individuals were mailed on May 19, 2022 by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

PAR is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, PAR moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. In response to the Incident, PAR is enhancing the security monitoring of their information technology systems, and has implemented additional security procedures to prevent unauthorized system access and has removed archival personal information from its legacy ERP database.

Although PAR is not aware of any actual or attempted misuse of the affected personal information, PAR offered 12 months of complimentary credit monitoring and identity theft restoration services through Kroll to all individuals to help protect their identity. Additionally, PAR provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact information

PAR, Inc. remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

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

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

Re: NOTICE OF DATA INCIDENT

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

Out of an abundance of caution, PAR, Inc. ("PAR"), is writing to inform you of a data security incident that may have resulted in an unauthorized access of your personal information. PAR sincerely apologizes for this incident and any problems it may cause you. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the events, steps that PAR is taking in response, and resources available to help you protect against the potential misuse of your information.

Why Do We Have Your Information?

PAR has your information because we have or had a business relationship with you that required issuance of tax reporting to the Internal Revenue Service.

What Happened?

PAR recently discovered that an unauthorized user gained access to its corporate computer systems that store historical information related to financial transactions we have conducted with you in the past. In 2021, PAR migrated to a new ERP system which runs our finance and operations transactions. However, a legacy database file that contains your name, address, and social security number was stored in an archive location on our corporate network. PAR recently discovered that an unauthorized user gained access to this network file location. This unauthorized access occurred on or about March 21, 2022 (the "Incident"). PAR terminated the unauthorized access, and promptly commenced an internal investigation to determine the nature and scope of the Incident. The investigation involved hiring an outside information security company that conducted an extensive forensic investigation. To date, there is no evidence that anyone's personal information has been obtained, leaked, or otherwise compromised. However, PAR has decided to notify any individual whose data was stored in the compromised system out of an abundance of caution. In addition, PAR is offering complimentary identity monitoring services to help protect you from the potential misuse of your personal information.

What Information Was Involved?

The personal information that may have been accessed by an unauthorized actor includes your name, address, and Social Security number. No other personally identifiable information ("PII") was stored on the potentially compromised system.

Please note that PAR has received no indication that your information has been used by the unauthorized actor or by any unauthorized party to commit fraud. PAR is providing notice to you out of an abundance of caution.

What We Are Doing

PAR values the privacy of your information and will continue to do everything it can to protect it. PAR has implemented additional security procedures to prevent unauthorized system access and your personal information has been removed from our legacy ERP database.

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, Web Watcher, \$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 <<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.

Additional information describing your services is included with this letter.

What You Can Do

You may activate the identity monitoring services we are making available to you. Once again, PAR is making these services available to you at no cost; however, you will need to activate these services yourself. **The deadline to activate is <<b2b_text_6(activation deadline)>>**. PAR would like to reiterate that, at this time, there is no evidence that your information was misused. However, PAR encourages you to take full advantage of the services offered.

Enclosed with this letter you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information. PAR encourages you to activate the services offered and to remain vigilant against incidents of identity theft and fraud. Such vigilance includes reviewing account statements and credit reports for suspicious activity. Individuals are encouraged to report any suspicious activity to the affiliated institutions immediately.

For More Information:

The protection of your information is a top priority, and PAR, Inc. sincerely regrets any concern or problem that this matter may cause. If you have any questions, please do not hesitate to call Travis or Donna at 813-968-3003. PAR values our relationship with you and we vow to do everything we can to help protect the security and privacy of your personal information in the future.

Sincerely,

Travis White, PhD
President and COO
PAR, Inc.

Donna Drackett
EVP and Chief Financial Officer
PAR, Inc.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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.

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.

\$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.

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Furthermore, to help protect your deceased family member, there are steps you can take to request a copy of your deceased family member's credit report. An executor or surviving spouse can place a request to any of the three credit reporting agencies for a copy of the deceased individual's credit report. An executor or surviving spouse can also request that the following two notices be placed on a deceased individual's credit report:

- "Deceased – Do not issue credit"; or
- "If an application is made for credit, please notify the following person(s) (e.g. surviving relative, executor/trustee of the estate and/or local law enforcement agency – notifying the relationship)."

Contact information for the three nationwide credit reporting companies is as follows:

Equifax
PO Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
PO Box 6790
Fullerton, CA 92834
www.transunion.com
1-800-680-7289

For more information regarding identity theft and the deceased, please visit <http://www.idtheftcenter.org> and search for "FS 117 - Identity Theft and the Deceased - Prevention and Victim Tips." You should also notify the Social Security Administration and Internal Revenue Service of the death of your family member and that you received this letter.

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960

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

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
1-800-909-8872

www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<http://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov