



**OGLETREE, DEAKINS, NASH, SMOAK &
STEWART, P.C.**

Attorneys at Law

Truist Plaza
401 Commerce Street, Suite 1200
Nashville, TN 37219-2446
Telephone: 615-254-1900
Facsimile: 615-254-1908
www.ogletree.com

Benjamin W. Perry
benjamin.perry@ogletree.com

August 23, 2024

Via Email

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

To Whom It May Concern:

I am writing on behalf of our client, Perry Johnson, Inc. (“PJI”), to notify you of a data incident involving Maryland residents. Please note that, by providing this notice, PJI does not waive any rights or defenses, including regarding the applicability of Maryland law, the applicability of the Maryland data breach notification statute, or personal jurisdiction.

Between March 27, 2023, and May 2, 2023, PJI experienced a data security incident wherein an unauthorized actor gained access to PJI’s systems. Law enforcement was notified, and PJI retained a cybersecurity firm to contain the threat, assist with PJI’s internal investigation, and determine the cause and scope of the incident. The investigation determined that the actor obtained initial access using compromised credentials. The actor subsequently engaged in network reconnaissance, privilege escalation, and lateral movement. During this time, the actor installed and executed a tool commonly associated with data exfiltration. The investigation concluded that the period of unauthorized access ended on or about May 2, 2023, when the cybersecurity firm began deploying SentinelOne, an endpoint detection and response system, across the network.

On June 14, 2024, the cybersecurity firm preliminarily concluded that the files contained the personal information of Maryland employees, vendors, and/or contractors. The cybersecurity firm completed this phase of its investigation on June 26, 2024. Although the investigation was unable to conclusively determine whether employee, vendor, or contractor data, if any, was actually accessed or acquired, PJI has provided notice out of an abundance of caution to those employees, vendors, and contractors whose personal information was identified to date as having been contained on the affected systems, including eight Maryland residents. A sample copy of the individual notification letter is enclosed.

PJI is offering affected individuals two years of complimentary credit monitoring and other consumer protection services, including fraud loss reimbursement insurance coverage. PJI has also implemented additional security features, such as additional endpoint protection and monitoring. The company is

August 23, 2024

Page 2

also continuing to evaluate ways to further enhance the security of its systems and to minimize the likelihood of similar events occurring in the future.

Thank you for your time and attention to this matter. Please let us know if you have any questions or concerns regarding this notice or the incident.

Sincerely

A handwritten signature in black ink, appearing to read 'B. Perry', with a long horizontal flourish extending to the right.

Benjamin W. Perry

P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<Enrollment Code >>

To Enroll, Scan the QR Code Below:



Or Visit:

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

August 23, 2024

Notice of Data Breach

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

Perry Johnson, Inc. (“PJI”) is writing to inform you about an incident that may have affected the security of your personal information. While there is currently no indication that any identity theft has occurred as a result of this incident, some of your personal information was included on the systems that were impacted by this incident, so we want to let you know what happened, what is being done to address it, and the complimentary identity monitoring services we are offering.

What happened?

PJI provides administrative and technical support to certain companies, including a company where you were an employee, vendor, or contractor. In this role, PJI maintained certain personal information about those companies’ employees, contractors, and/or vendors. Between March 27, 2023, and May 2, 2023, PJI experienced a data security incident wherein an unauthorized actor gained access to PJI’s systems. Law enforcement was notified of the incident, and PJI began an internal investigation and retained a cybersecurity firm to contain the threat, assist with its investigation, and determine the scope of the incident.

On June 14, 2024, the cybersecurity firm preliminarily concluded that the impacted systems contained files that included some of your personal information. The cybersecurity firm completed this phase of the investigation on June 26, 2024. Although the investigation was unable to conclusively determine whether employee, vendor, or contractor data, if any, was actually accessed or acquired, PJI is providing notice to individuals whose personal information was contained on the affected systems out of an abundance of caution.

What information was involved?

Although we cannot conclusively determine whether the unauthorized party actually accessed or acquired your personal information, our investigation has determined that the affected systems contained files that included your <<Variable Data 1>>.

What we are doing.

Since becoming aware of this incident, we have been evaluating our notification obligations and taking steps to inform potentially impacted individuals of this incident. We are continuing to evaluate our cybersecurity controls to enhance our security measures and minimize the likelihood of similar events occurring in the future. As an added precaution and to relieve concerns, we have secured the services of IDX to provide identity monitoring at no cost to you. Your identity monitoring services include 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement

policy, and fully managed ID theft recovery services. Please note, the deadline to enroll is November 23, 2024. These services are described in more detail in the “Recommended Steps to help Protect your Information” section included with this letter.

What you can do.

In addition to completing your enrollment with IDX, we encourage you to remain vigilant against incidents of identity theft and fraud, such as by regularly reviewing your account statements with all of your financial institutions. You may contact the Federal Trade Commission for information regarding fraud or identity theft at 877-382-4357, 400 7th St., SW Washington, DC 20024, or consumer.ftc.gov. You may also be eligible for a free credit report at www.annualcreditreport.com, or contact the major credit reporting agencies at:

Equifax
www.equifax.com
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374

Experian
www.experian.com
(888) 397-3742
P.O. Box 2104
Allen, TX 75013-0949

TransUnion
www.transunion.com
(833) 395-6938
P.O. Box 1000
Chester, PA 19022

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. The enclosed resources also provide information about fraud alerts and security freezes.

For more information.

We understand that you may have questions about the incident that are not addressed in this letter. If you have additional questions, please call 1-800-939-4170, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays, or go to <https://app.idx.us/account-creation/protect> for assistance or any additional questions you may have. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online, so please do not discard this letter.

We regret this incident and apologize for any inconvenience or concern that it may cause you.

Sincerely,

Perry Johnson, Inc.



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.