



**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

July 22, 2024

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

To Whom It May Concern:

I am writing on behalf of our client, Perry Johnson Mortgage Company, Inc., to notify you of a potential data incident involving Maryland residents.

Between March 27, 2023 and May 2, 2023, a vendor providing IT administrative and technical support to PJM experienced a data security incident wherein an unauthorized actor gained access to the vendor's systems. The vendor began an internal investigation and retained a cybersecurity firm to contain the threat, assist with its investigation, and determine the scope of the incident.

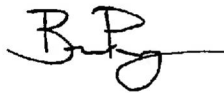
Although PJM was aware of the incident at the time, PJM had no reason to believe any consumer mortgage data was affected. Nevertheless, the vendor notified PJM in May 2024 that certain PJM consumer data may have been backed up on an affected system. PJM promptly took steps to confirm this information and identify the scope and nature of the data contained on the affected system through a data mining process with an outside vendor. On June 14, 2024, the investigation preliminarily concluded that the impacted systems contained files that included the personal information of Maryland residents, and this data mining review was completed on June 26, 2024. Although the investigation was unable to conclusively determine what PJM data, if any, was actually acquired, PJM is notifying the three affected Maryland residents by U.S. Mail on July 26, 2024, including an offer of complimentary credit monitoring to those individuals. A sample copy of the individual notification letter is enclosed.

PJM's vendor believes the incident has been contained. PJM's vendor continues to monitor its systems for any suspicious activity and has also implemented additional security features, such as additional endpoint protection and monitoring. PJM's vendor has indicated that it is continuing to evaluate ways to further enhance the security of its systems. PJM is likewise evaluating its cybersecurity controls to enhance its security measures and minimize the likelihood of similar events occurring in the future.

July 22, 2024
Page 2

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 horizontal line extending to the right.

Benjamin W. Perry

Enclosure: Sample Individual Notification



<<Return Address>>
<<City>>, <<State>> <<Zip>>

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

<<Date>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

Notice of Data Breach

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

Perry Johnson Mortgage Company, Inc. ("PJM") 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 we are doing to address it, and the complimentary identity monitoring services we are offering.

What happened?

Between March 27, 2023 and May 2, 2023, a vendor providing IT administrative and technical support to PJM experienced a data security incident wherein an unauthorized actor gained access to the vendor's systems. The vendor began an internal investigation and retained a cybersecurity firm to contain the threat, assist with its investigation, and determine the scope of the incident.

Although PJM was aware of the incident at the time, PJM did not believe any consumer mortgage data was affected. Nevertheless, the vendor notified PJM in May 2024 that certain PJM consumer data may have been backed up on an affected system. PJM promptly took steps to confirm this information and identify the scope and nature of the data contained on the affected system. On June 14, 2024, the investigation preliminarily concluded that the impacted systems contained files that included some of your personal information, and the forensics firm completed its investigation on June 26, 2024. Although the investigation was unable to conclusively determine what PJM data, if any, was actually accessed or acquired, PJM is providing notification 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 viewed or acquired your personal information, our investigation has determined that the affected systems contained files that included your <<Variable Data Elements>>.

What we are doing.

When we learned that PJM data was present on the systems affected by this incident, we promptly began our own investigation and moved quickly to notify potentially impacted individuals. In addition, we are in the process of evaluating 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. These services are described in more detail in the "Additional Resources" 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:

<u>Equifax</u>	<u>Experian</u>	<u>TransUnion</u>
www.equifax.com	www.experian.com	www.transunion.com
(800) 685-1111	(888) 397-3742	(833) 395-6938
P.O. Box 740241	P.O. Box 2104	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013-0949	Chester, PA 19022

These resources can 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 <<Toll-Free Number>>, Monday through Friday from 8:00 a.m. to 5:30 p.m. Eastern Time, excluding major U.S. holidays.

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

Sincerely,

Perry Johnson Mortgage Company, 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 <<Toll-Free Number>> 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.

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 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

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.