

August 18, 2023Writer's Direct Contact
+1 (212) 336-4038
KMathews@mofo.com**Via E-Mail (IDTheft@oag.state.md.us)****Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202*****RE: Notice of Data Security Event***

To Whom It May Concern:

On behalf of Consumer Reports, I am writing to inform you about a recent incident in which personal information relating to Maryland residents was accessed by an unauthorized third party.

Specifically, on May 31, 2023, Progress Software Corporation ("Progress") announced that its MOVEit Transfer product was impacted by a zero-day vulnerability that enabled unauthorized access to the MOVEit application. See MOVEit Transfer Critical Vulnerability (May 2023) - Progress Community: <https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023>. Pension Benefit Information, LLC ("PBI"), a vendor used by PNC Bank, which is Consumer Reports' annuity management vendor, used MOVEit Transfer software.

On July 24, 2023, we were notified by PNC that, on May 29, 2023, information relating to the annuitants of Consumer Reports was accessed by an unauthorized third party as a result of the MOVEit vulnerability. Thereafter, PNC provided Consumer Reports with a list of affected individuals and we derived their states of residence. According to PNC, PBI determined through its investigation that the third party accessed the name, address, social security number, and date of birth relating to Consumer Reports annuitants.

Consumer Reports does not use MOVEit Transfer software and our systems were not exposed to the MOVEit vulnerability. There is no indication Consumer Reports systems or environments were impacted by the vulnerability within the MOVEit Transfer application. Similarly, there is no indication that there was any unauthorized access to Consumer Reports systems, which remain operational and secure. PNC has indicated that it has paused the provision of customer data to PBI until appropriate safeguards are put in place to address the vulnerability identified in their MOVEit File Transfer Software.

August 17, 2023

Page Two

PBI is notifying the twenty (20) Maryland residents impacted by this incident on August 18, 2023. PBI is also providing these individuals with an offer for complimentary credit monitoring and identity restoration services through Kroll. Additionally, according to PNC, PBI filed state regulatory notifications including the following language: "We write to notify your office of a security event that may have affected the security of certain personal information relating to approximately <<number of data subjects>> <State>> residents that PBI was processing for one of PBI's business clients ("Client") on behalf of that Client's customers." The "Client" in PBI's language is PNC. Consumer Reports is a customer of PNC. PBI is not our direct vendor and we do not have a direct relationship with them. PNC does.

Attached is a sample of the near final letter that PBI is providing to Maryland residents and a sample of the letter that Consumer Reports is providing to Maryland residents.

Please do not hesitate to contact me at kmathews@mofo.com if you have any questions.

Sincerely,

Kristen J. Mathews
Partner

[First][Last Name]
[Address]

Dear [First][Last Name]

We are writing to notify you of a recent data security incident involving the Benefits vendor, Pension Benefit Information, LLC (“PBI”), used by Consumer Reports’ vendor, PNC Bank, and PBI’s use of MOVEit Transfer software. As announced by Progress Software Corporation (“Progress”) and reported in the press, Progress’s MOVEit Transfer product was impacted by a zero-day vulnerability that enabled unauthorized access to the MOVEit application. (See <https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft>). Unfortunately, this incident has impacted a number of annuitants, including you. The information that was downloaded includes your name, date of birth, social security number and resident state/zip code.

We expect that PBI will begin to provide notices directly to impacted individuals on or about August 18, 2023, and offer one to two years of credit monitoring, fraud consultation and Identity Theft Restoration services. Attached is a copy of the letter that PBI will send to impacted individuals.

At Consumer Reports, we take data privacy and security very seriously. Our annuitants’ privacy is of utmost importance to us and we have been working diligently to address this issue. Please see the attached FAQs, which may help to answer any additional questions that you have.

If you have any other questions, please do not hesitate to contact me at (914) 378-2604.

Kind regards,

Nancy Smith
Manager, Major & Planned Gifts

FREQUENTLY ASKED QUESTIONS

1. What happened?

- At the end of May, a company by the name of Progress Software released a statement indicating that their MOVEit Transfer software contained a vulnerability, which was exploited by cybercriminals.
- Consumer Reports does not use MOVEit Transfer software and its systems were not exposed to the MOVEit vulnerability.

- Pension Benefit Information, LLC (“PBI”), a benefits vendor used by Consumer Reports’ vendor, PNC Bank (“PNC”), informed PNC that PBI used the MOVEit Transfer software to accept and transfer files, and PBI’s systems were compromised. On July 24, 2023, PNC informed Consumer Reports that, unfortunately, Consumer Reports data, which includes annuitant data, was impacted, alongside the data of other PBI customers.
- The data accessed for impacted individuals includes name, date of birth, social security number, resident state/zip code.

2. Who is PBI?

- PBI is a third-party vendor that many financial institutions use, including PNC, to, among other things, manage annuitant information. We use PNC to administer Consumer Reports’ annuity program.

3. What steps has Consumer Reports taken?

- Upon becoming aware of this event, Consumer Reports immediately took steps to confirm with PNC that PBI had remediated the software vulnerability and confirmed their systems were not further impacted.
- We expect that PBI will begin to provide notice to impacted individuals directly on August 18, 2023, and offer one to two years of credit monitoring, fraud consultation and Identity Theft Restoration services, the length of the offered service as described in PBI’s notice.
- Consumer Reports takes the privacy of our annuitant information very seriously, and we have controls in place with our vendors to prevent these incidents where possible and respond if there is an incident. We will continue to work with our vendor to remediate this incident.

4. Will PNC continue to use PBI?

- PNC has paused providing customer data to PBI until appropriate safeguards are put in place to address the vulnerability identified in their MOVEit File Transfer Software.
- PBI has informed PNC that PBI has installed the required security patches to remediate the vulnerability in the data transfer software, conducted its own forensics investigation, contacted law enforcement, and engaged an independent forensics firm that determined there was no further impact to their systems as a result of the threat actor’s exploit.



<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

<<Date>>

<<Notice of Data Breach>>

Dear <<Name 1>> <<Name 2>>:

Pension Benefit Information, LLC (“PBI”) provides audit and address research services for insurance companies, pension funds, and other organizations<<, including <<Data Owner>>. PBI is providing notice of a third-party software event that may affect the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability’s impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the server at the time of the event: name and <<Data Elements>>.

What We Are Doing. We take this event and the security of information in our care seriously. Upon learning about this vulnerability, we promptly took steps to patch servers, investigate, assess the security of our systems, and notify potentially affected customers and individuals associated with those customers. In response to this event, we are also reviewing and enhancing our information security policies and procedures.

While we are unaware of any identity theft or fraud as a result of this event, as an additional precaution, PBI is offering you access to <<12/24>> months of complimentary credit monitoring and identity restoration services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors for the next twelve to twenty-four months and to report suspected identity theft incidents to the institution. Please also review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that we are offering.

For More Information. If you have additional questions, you may call our toll-free assistance line at <<Kroll Call Center Number>> Monday through Friday from 9:00 am to 6:30 pm Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402.

Sincerely,

John Bikus
President
Pension Benefit Information, LLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Kroll's Monitoring Services

To help relieve concerns and restore confidence following this event, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<12/24>> months. 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.¹

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Information

- **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.
- **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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

¹ 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.

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this event. 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 New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately [X] Rhode Island residents that may be impacted by this event.