FIDELITYLIFE

Fidelity Life Association
1350 E. Touhy Avenue Suite 205W
Des Plaines, IL 60018
T|F: 312.379.2397

August 15, 2023

RCVD AUG 21 2023

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

RE: Fidelity Life Association – Third-Party Vendor (PBI Research Services) Security Incident Connected to MOVEit Transfer Software

Dear Sir/Madam:

I am notifying you that Fidelity Life Association, an insurance company domiciled in Illinois, recently learned of a security incident involving unauthorized access to our customers' personally identifiable information caused by our vendor's subcontractor—PBI Research Services ("PBI")—using the MOVEit Transfer software. As has been documented extensively in the media, this software contained a zero-day vulnerability that a threat actor exploited to gain access to hundreds of companies' data. The incident involving PBI potentially impacted dozens of insurers, governmental entities, and other companies that used PBI for legally required death master file searches. Fidelity Life Association itself did not, and does not use, the MOVEit application—our computer systems were not impacted by the incident. But, unfortunately, PBI was one of the companies that fell victim to the vulnerability. We are continuing the gather information about this incident, and we will update this notice with additional details as necessary. As of today, our understanding is as follows:

1. **When did the incident occur?** The unauthorized access occurred between May 29th and May 30th.

2. **What happened?** A threat actor exploited a vulnerability in the MOVEit Transfer software used by our vendor's subcontractor, PBI. We rely on the vendor to help with insurance-policy management, and our vendor engaged PBI to perform death audits—specifically, to query against the Social Security Administration's Death Master File to identify any deaths that have not been reported to us. PBI reported the incident to our vendor on June 4, and our vendor informed us on June 6. In early July, PBI informed us that some of our data was affected. On July 19, PBI provided us a list of affected individuals and their addresses.

3. **How was the incident discovered?** Progress Software, the provider of MOVEit Transfer software, disclosed a vulnerability in their software on May 31, 2023. Following that announcement, PBI began conducting a manual review to determine which files were affected. PBI subsequently concluded that some files belonging to Fidelity Life Association were impacted.

FIDELITYLIFE[SM]

Fidelity Life Association
1350 E. Touhy Avenue Suite 205W
Des Plaines, IL 60018
T|F: 312.379.2397

4. **Has data been recovered?** Our understanding is that the data has not yet been recovered from the threat actor. But the attack has not materially impacted our operations because we have copies of the information.

5. **What is the source of the incident?** The incident stems from a vulnerability in the MOVEit Transfer software. While we do not conclusively know the threat actor's identity, there have been public reports of the CL0P ransomware group taking credit for exploiting the vulnerability in the MOVEit Transfer software.

6. **Have we notified law enforcement?** We have not alerted law enforcement because we were informed that PBI notified the FBI shortly after learning of the incident.

7. **What data was acquired?** The affected information involved individuals' names, birthdates, addresses, and Social Security numbers.

8. **How long did the compromise last?** Our understanding is that the threat actor may have had access to the data between May 29th and May 30th.

9. **How many residents were affected?** We believe that 2,681 Iowa residents were affected by this incident.

10. **Have we identified any failures in our controls or procedures?** We have not identified any failures in our controls or procedures. This attack exploited a vulnerability in software used by many companies, but Fidelity Life Association does not use MOVEit software.

11. **What remediation has been done?** We are working with PBI to ensure that affected individuals are notified (and given credit monitoring). Our understanding is that PBI will mail those notices in August. We are also alerting appropriate regulators and monitoring ongoing developments with the MOVEit Transfer software vulnerability. Additionally, we are ensuring that our vendors (and their subcontractors) are deploying appropriate patches for the vulnerability. We also know that the PBI engaged a leading forensic firm to investigate, and that firm concluded—with high confidence—that (1) the incident has been contained, (2) PBI has remediated the issue, and (3) the threat actor is no longer in PBI's environment.

12. **What investigation steps have we undertaken?** We engaged experienced outside counsel to advise us on our rights and obligations, and we have worked with our vendor to understand the nature and scope of this incident. We also have monitored the remediation efforts (which include mailing notices to our affected customers).

13. **How are we notifying people?** PBI is sending notices on our behalf. In those notices, PBI is including complimentary credit monitoring for the affected individuals.

We have attached a template of the notice being sent to our customers.

FIDELITYLIFE℠

Fidelity Life Association
1350 E. Touhy Avenue Suite 205W
Des Plaines, IL 60018
T|F: 312.379.2397

If you have questions or need additional information regarding this incident, please contact Colman McCarthy at cdmccarthy@shb.com or 816-559-2081.

Sincerely,

John Buchanan
EVP & General Counsel

<<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 identity monitoring 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 Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also activate the identity 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 a.m. to 6:30 p.m. 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 HELP PROTECT PERSONAL INFORMATION

Activate Your 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

- **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.
- **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

[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.

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. 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 [#] Rhode Island residents that may be impacted by this event.

Fidelity Life Association
1350 E. Touhy Avenue, Suite 205W
Des Plaines, IL 60018

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

50319$0110 C196