Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

July 11, 2023

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Security Event

To Whom it May Concern:

We represent Pension Benefit Information, LLC ("PBI") located at 333 South Seventh Street, Suite 2400, Minneapolis, Minnesota 55402. PBI provides audit and address research services for insurance companies, pension funds, and other organizations.

We write to notify your office of a security event that may have affected the security of certain personal information relating to approximately two thousand five hundred sixty-three (2,563) Iowa residents that PBI was processing for one of PBI's business clients ("Client") on behalf of that Client's customers. By providing this notice, PBI does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa security event notification statute, or personal jurisdiction.

Nature of the Security Event

On or around May 31, 2023 and again in June 2023, Progress Software Corporation publicly disclosed zero-day vulnerabilities that impacted its MOVEit Transfer software. As a user of that software, PBI moved quickly to apply available patching, which was first available June 2, 2023, and undertook recommended mitigation steps. PBI promptly launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the potential impact of the vulnerabilities' presence on its MOVEit Transfer servers and on the data housed on the servers. The investigation determined that a threat actor exploited a zero-day vulnerability, accessed one of PBI's MOVEit Transfer servers on May 29, 2023 and May 30, 2023, and exfiltrated certain data

from that MOVEit Transfer server during that time. PBI subsequently undertook a time-consuming and detailed review of the data stored on the server at the time of the event to understand the contents of that data and to which business clients that data relates. Through this review, PBI determined that certain information related to residents of Iowa affiliated with certain customers of its Client was present on the server at the time of the event.

PBI's investigation determined that the information involved in this event that could have been subject to unauthorized access by the threat actor includes the impacted person's name, partial mailing address, Social Security number, and date of birth.

Notice to Iowa Residents

On or about June 4, 2023, PBI began to provide notice of this event to potentially affected business clients with an offer to provide notification services to potentially impacted individuals on their behalf and at their direction. On or about July 12, 2023, Client will begin to provide PBI's written notice of this event to approximately two thousand five hundred sixty-three (2,563) Iowa residents impacted by the event who are affiliated with some of Client's customers.

Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning about this event, PBI moved quickly to investigate and respond, assess the security of PBI's systems, including its MOVEit Transfer servers, and notify potentially affected PBI business clients. PBI is providing access to credit monitoring and identity restoration services for two (2) years, through Kroll, to individuals affiliated with the Client's impacted customers whose personal information was involved in this event, at no cost to these individuals. The Client is also establishing a toll-free call center for notified individuals affiliated with its impacted customers to address any questions related to this event.

Additionally, PBI is providing potentially affected individuals affiliated with its Client's impacted customers with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. PBI is also providing individuals with information on how to place fraud alerts and credit freezes on their credit files, 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 encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

PBI, on behalf of Client, is providing written notice of this event to appropriate governmental regulators, as necessary, and to the three nationwide consumer reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/jls

EXHIBIT A

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>> <<Date>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Notice of Data Breach

Dear <<Name 1>>,

We at Pension Benefit Information, LLC ("PBI") are contacting you to provide important information about a recent data event. You are receiving this letter because PBI provides audit and address research services for Fidelity Investments, the provider of administrative services for retirement plans at <<Client Name>>. This letter is informing you of a global third-party software event that impacted PBI and 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. Please note that this incident is not the result of any breach at Fidelity Investments or <<Client Name>>.

What Happened? On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software, disclosed a vulnerability in their software that could be 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 an unauthorized 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 and have concluded that information about you was involved in the incident.

What Information Was Involved? Our investigation determined that the following types of information related to you were downloaded by the third party: <<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 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. 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. Fidelity has indicated that your accounts at Fidelity continue to be covered by Fidelity's Customer Protection Guarantee, the details of which are available online at: https://nb.fidelity.com/public/nb/default/resourceslibrary/articles/fidelitycustomerprotectionguarantee.

<<Client ID>> <<Unique Record Identifier>>

For More Information. If you have additional questions, you may call Fidelity toll free at **1-800-610-7100** Monday through Friday from 8:30 am to 8 pm Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402.

If you need assistance with the credit monitoring services offered through Kroll, call Kroll at **1-833-680-7832** Monday through Friday from 8 am to 8 pm Eastern time or visit Kroll's website at login.krollmonitoring.com/about-us.

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 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.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by October 4, 2023. Your Activation Code will not work after this date.
2. Visit Enroll.krollmonitoring.com/redeem to activate your identity monitoring services.
3. Provide Your Activation Code: **<<Enter Activation Code>>** and Your Verification ID: **SF-009864**

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

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 can help you determine if it's 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 can 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 1772 Rhode Island residents that may be impacted by this event.