Cynthia J. Larose
617 348 1732
cjlarose@mintz.com

One Financial Center
Boston, MA 02111
617 542 6000
mintz.com

September 6, 2023

VIA E-MAIL TRANSMISSION (CONSUMER@AG.IOWA.GOV)

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 5039-0106

Re: Notice Pursuant to Iowa Code Chapter 715C

Dear Attorney General Raoul:

We are writing on behalf of Delaware Life Insurance Company (the "Company") to advise you of a third-party security incident at a vendor of the Company that may affect the security of personal information relating to approximately 2,224 Iowa residents. By providing this notice, the Company does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

On June 20, 2023, the Company was notified[1] by its third-party vendor, Pension Benefit Information, LLC (known as PBI Research Services or PBI), that its customer data in PBI's possession was subject to unauthorized access in connection with a global security incident involving Progress Software Corporation's MOVEit Transfer software. PBI is a third-party vendor used by the Company to satisfy regulatory obligations to identify the death of insureds and contract holders to determine if benefits are payable. PBI is a leading provider to insurance companies of these services. Please see PBI's summary of the incident provided with this letter as Exhibit A[2].

Like many organizations, PBI utilizes MOVEit Transfer to securely transfer information on behalf of its clients. PBI informed the Company that the following customer data elements were stored within its impacted MOVEit Transfer server which had been unlawfully accessed: name, date of birth, Social Security number, and the contract or policy number.

This PBI/MOVEit incident impacts policy holders and contract holders. The incident did not impact any of the Company's systems or network.

PBI has informed the Company that it (through Kroll, LLC) is offering the impacted customers 2 years of free credit monitoring, fraud consultation, and identity theft restoration through Kroll, LLC. 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. Kroll was

[1] The PBI incident summary document (Exhibit A) is dated June 16, 2023 and was emailed by PBI to the Company on June 19, 2023. The Company was closed for the Juneteenth federal holiday and the notice was not received by the Company until June 20, 2023.
[2] Please note that this incident is not related to the ransomware incident reported to your office by the Company on July 28, 2023.

engaged by PBI to establish a dedicated assistance line for individuals who may have questions about this incident.

The Company has been advised by Kroll that the mailing of notification letters to impacted Iowa residents will begin on September 6, 2023 and be completed by September 8, 2023. A sample breach notification template (Exhibit B) is included for your information.

Please contact the undersigned at cjlarose@mintz.com or 617-348-1732 should you need further information or have any additional questions.

Sincerely,

Cynthia J. Larose
Member
Attachments

Exhibit A

MOVEit Transfer Data Event Summary **June 16, 2023**

Starting in late May, the federal government, state governments, universities, health care organizations, and enterprise corporations in the United States and across the globe were impacted by a cyberattack. Progress Software, owner of the MOVEit application file transfer software, had a zero-day vulnerability that was exploited by cyber criminals. A zero-day event indicates it was a previously unknown vulnerability. According to publicly available reporting, those responsible for the event accessed personal information of potentially millions of people across previously mentioned victims. PBI Research Services ("PBI") uses the MOVEit Transfer software to accept and share files. While PBI was impacted, the cyber criminals did not gain access to PBI's core systems or software.

PBI values our client relationships and is working quickly and diligently to assess the impact of this event and communicate with clients. Below is a full summary of the event including details of the attack and the steps PBI has taken to date.

As discussed above, on or around May 31, 2023, a MOVEit Transfer vulnerability was first publicly disclosed.[1] As soon as Progress Software made patches available on June 2, 2023, we immediately completed Progress's recommended patching and remediation steps.

To assist with PBI's comprehensive incident response, we promptly retained Mullen Coughlin as external privacy counsel who, in turn, engaged leading cybersecurity and digital forensics specialists, Kroll, to conduct a legally privileged forensic investigation into the event to determine the nature and scope of the vulnerability's impact on our systems. We also notified federal law enforcement on June 3, 2023.

Kroll reviewed available logs and artifacts to determine the event's nature and scope and assessed whether data was subject to unauthorized access or acquisition. Through our investigation, we determined the following:

- The attack appears to have been perpetrated by the CLOP threat group;
- The threat actor exploited a zero-day SQL injection vulnerability (CVE-2023-34362) and accessed one of our MOVEit Transfer servers between May 29, 2023 and May 30, 2023;
- There were indicators of data exfiltration during the window of compromise;
- There was no evidence of lateral movement;
- As of this writing, the threat actor has not posted any PBI data to their leak site;
- There was no evidence of activity prior to or after the stated attack window; and
- A list of identified indicators of compromise is attached as ***Exhibit A.***

As noted above, the event occurred as a direct result of the May 2023 MOVEit Transfer vulnerability. PBI applied all appropriate patches and remediation steps as they became available

[1] https://www.kroll.com/en/insights/publications/cyber/responding-critical-moveit-transfer-vulnerability-cve-2023-34362

and continues to promptly implement software updates provided by MOVEit. In addition to regular patching of the MOVEit software, PBI has undertaken the following security enhancements in response to the event:

- Impacted MOVEit server replaced with new instance, which was patched and hardened;
- Added a Web Application Firewall including filters on known bad inputs, geo-location, and IP Reputation;
- Additional logging, security monitoring, and alerts implemented; and
- File Import retention on SFT server reduced to 1 day post processing.

As part of our incident response efforts, we promptly reviewed the potentially impacted data and began issuing preliminary notice to our clients on June 3, 2023. If you did not receive a letter or email, your company's data has not been identified as impacted.

If you have questions regarding this correspondence, please contact us by email at moveitsecurity@pbinfo.com.

Regards,

John Bikus
President
PBI Research Services

Exhibit A

Indicators of Compromise ("IOCs")

Specific IOCs

Malicious IP Addresses

5.252.191.103
5.252.191.103
5.252.190.93
5.252.190.249
5.252.190.84
5.252.189.252
178.33.21.153|Noisy-le-Sec|Île-de-France|FR|93130|16276|OVH SAS|ip-178-33-21.eu|OVH SAS|OVH SAS|True|False|False|False|False|True

- Database userID is 0cx50a40hc6wty6x

Webshell

human2.aspx

Public IOCs

A listing of the publicly known IOCs can be found at in the Cybersecurity Infrastructure Security Agency's (CISA) Advisory *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability.* Available at the following web page, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

Exhibit B

September 6, 2023

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_3(Notice of Data Breach)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Pension Benefit Information, LLC ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations, including <<b2b_text_1(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: <<b2b_text_2(name, 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 twenty-four (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 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 (866) 676-3191, 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,

The PBI Team

Steps You Can Take To Help Protect Personal Information

Enroll in Kroll's Identity Monitoring Services

To help relieve concerns and restore confidence following this event, we have secured the services of Kroll to provide Identity Monitoring services 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.[1]

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your Identity Monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your Identity Monitoring services.

Membership Number: **<<Membership Number s_n>>**

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. 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;

[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.

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. <<vtext 4(There are approximately [Number] Rhode Island residents that may be impacted by this event.)>>