

September 14, 2023

Dominik Cvitanovic
(504)-702-1710
Dominik.Cvitanovic@WilsonElser.com

Via Electronic Mail:

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

Re: Our Client : The J. David Gladstone Institutes
Wilson Elser File # : 16516.02152

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents The J. David Gladstone Institutes (“Gladstone”) with respect to a recent data privacy incident (hereinafter, the “Incident”). Gladstone takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that Gladstone has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals.

1. Nature of Security Incident

On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software, publicly disclosed a vulnerability in their software that had been exploited by an unauthorized third party. Many vendors across the world utilized MOVEit in the regular course of business operations to securely transfer files, and unfortunately, this Incident also impacted Pension Benefit Information, LLC (“PBI”), a vendor of TIAA, Gladstone’s retirement plans recordkeeper. PBI became aware of this vulnerability on June 1, 2023 and installed all available patches upon their release on June 2, 2023. TIAA notified Gladstone that TIAA and PBI promptly launched an investigation to understand the impact of the Incident.

That investigation determined that an unauthorized third party obtained certain files transferred by PBI through the MOVEit Transfer software between May 29 and May 30, 2023, prior to public disclosure of the vulnerability or security patches being available. TIAA then notified Gladstone of the Incident and PBI's investigation and that PBI would be providing affected persons two years of credit monitoring, fraud consultation, and identity theft protection at no cost.

As of this writing, Gladstone has not received any reports of related identity theft since the date of the Incident.

2. Number of Maryland Residents Affected

A total of three (3) Maryland residents have been potentially affected by this incident. Notification letters to individuals were mailed to potentially impacted individuals beginning on July 25, 2023, by first class mail. A sample copy of the notification letter is included with this letter under *Exhibit A*. To ensure the individuals were aware of the direct connection with Gladstone and that the credit monitoring services were legitimate, Gladstone also notified the individuals by email.

3. Steps taken in response to the Incident

Data security is one of Gladstone's highest priorities. Upon detecting this Incident, Gladstone moved quickly to determine the appropriateness of TIAA and PBI's response. PBI has replaced the impacted MOVEit server with a new instance with patches applied in a timely fashion; has added a web application firewall with filters for known bad inputs, geo-location, and IP reputation; has implemented additional logging, monitoring, and alerting for their environment; has reduced the file retention timeframe on PBI's MOVEit server to 1 day post-processing; and has worked with a forensic specialist to remediate the incident.

4. Contact information

Gladstone remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Dominik.Cvitanovic@WilsonElser.com or 504.372-6698.

Sincerely,

Wilson Elser Moskowitz Edelman & Dicker LLP

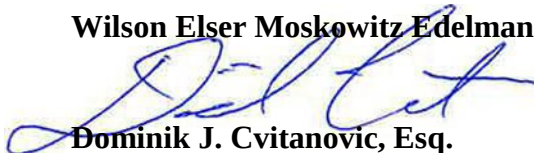

Dominik J. Cvitanovic, Esq.

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<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 Teachers Insurance and Annuity Association of America (“TIAA”). 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, Social Security number, date of birth, address, and gender.

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 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. 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 (866) 373-7560 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 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

- **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 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:

- Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- Addresses for the prior two to five years;

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.

- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
- 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 Kentucky residents, the Kentucky Attorney General – Office of Consumer Protection may be contacted at: 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601; 1-800-804-7556; and <https://www.ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Identity-Theft.aspx>.

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.