



Tawana B. Johnson
Direct: 404.476.2089
Tawana.Johnson@lewisbrisbois.com

July 24, 2023

Via electronic-mail: ldtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Re:	Our Client	:	Teachers' Retirement System of the City of New York
	Matter	:	Data Security Incident on May 29, 2023
	LBBS File #	:	16516.2089

Dear Attorney General Brown:

We represent Teachers' Retirement System of the City of New York ("TRS NYC") with a principal place of business in New York, New York with respect to a potential data security incident described in more detail below. TRS NYC takes the security and privacy of the information in its control 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 security breach, the number of Maryland residents that were potentially affected, what information has been compromised, and the steps that TRS NYC is taking in response to this incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

TRS NYC uses a third-party vendor, PBI Research Services ("PBI") to conduct audit services. In turn, PBI uses the MOVEit Transfer software for secure file transfers, including data from TRS NYC regarding its plan participants. On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software had been exploited by an unauthorized third party. According to PBI, it promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on its systems. Through the investigation, PBI learned that the third party accessed one of its MOVEit Transfer servers on May 29 and May 30, 2023 and downloaded data. On June 6, 2023, PBI notified TRS NYC that its data was impacted during the attack.

2. Maryland Residents Notified

A total of five hundred and fifteen (515) residents of Maryland were potentially affected by this security incident. A notification letter to these individuals were mailed on July 18, 2023, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

This data security incident occurred entirely within PBI's network environment, and there were no other remedial actions available to TRS NYC. However, according to PBI, it has taken the following actions in response to this incident:

- Rebuilt an entirely new server from a hardened image;
- Patched all MOVEit Transfer servers;
- Removed the malicious web shell;
- Blocked malicious IP addresses;
- Enabled ransomware detection and prevention configuration options for antivirus/antimalware software;
- Reviewed and ensured that no database user accounts were created by the threat actor(s); and
- Terminated indefinite sessions to ensure any threat actor(s) sessions would be removed from the database server post patch/reboot of the server.

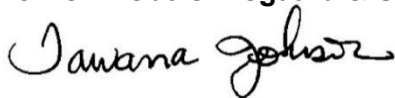
PBI has also extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through Kroll. This service will include 24 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise. The notification letter and offer of free credit monitoring were mailed on July 18, 2023.

4. Contact Information

TRS NYC 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 Tawana.Johnson@lewisbrisbois.com or 404.470.2089.

Very truly yours,

Lewis Brisbois Bisgaard & Smith, LLC



Tawana Johnson, Esq.

cc: Robert Walker, Esq.
(Lewis Brisbois LLC)

Enclosures: *Sample notification letter*



July 18, 2023



NOTICE OF DATA BREACH

[REDACTED],

The Teachers' Retirement System of the City of New York (TRS) was recently notified that TRS payees' personal information was involved in a data security incident affecting PBI Research Services, one of our third-party vendors. This incident occurred outside of TRS, and TRS' systems were not compromised. However, your personal information was exposed in this global data security incident.

TRS uses PBI's services to identify deceased retirees and other payees in order to ensure that pension benefits are paid to the rightful members or beneficiaries, and to help prevent any erroneous payment of benefits.

What Happened? PBI recently confirmed with TRS that a previously unknown vulnerability in the MOVEit Transfer application, which is used by thousands of organizations worldwide, allowed TRS data to be downloaded by an unauthorized third party. PBI's investigation revealed that the third party accessed one of PBI's MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. After a comprehensive manual review of its records, PBI recently confirmed that TRS data was impacted.

PBI has reported the matter to federal law enforcement and has told TRS that it resolved the vulnerability, while also enhancing its information security measures.

What Information Was Involved? PBI's 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, current city, state, and zip code, and prior city of residence. The information could also have included the names of former or current employers, or designated beneficiaries.

In general, anyone who was receiving an ongoing monthly benefit from TRS as of March 2023 was affected by this data security incident.

What Is TRS Doing to Protect Its Members? Although our own systems were not affected by the data security incident, TRS is reviewing additional safeguards for our website and monitoring for suspicious activity. In addition, PBI has agreed to offer you access to 24 months of free 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: TRS encourages 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. TRS also encourages you to enroll in the credit monitoring and identity protection services that PBI is offering.

For More Information: If you have additional questions, you may call the toll-free assistance line at (866) 373-9057 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. Please do not contact TRS directly, as our Member Services Representatives do not have further information about this data security incident.

TRS values our members' data security, and we deeply regret that this external data security incident affected our members.

Sincerely,

TRS Member Services

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Kroll's Monitoring Services

To help relieve concerns and restore confidence following this event, PBI has 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 **October 12, 2023** to activate your identity monitoring services.*

Kroll "Member Number": **DZCF43946-P**

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;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and

¹Kroll'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.

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 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 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 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 59 Rhode Island residents that may be impacted by this event.