STATE RETIREMENT AGENCY
120 East Baltimore Street
Baltimore, MD 21202-6700

MARYLAND
STATE RETIREMENT
and PENSION SYSTEM

410-625-5555 • 1-800-492-5909
TTY Users: call via Maryland Relay
sra.maryland.gov

MSRPS Member Data is Secure

In light of the recent data breaches at a number of large institutional investors, the Maryland State Retirement Agency (SRA) wants to assure our members that membership data maintained by the Agency is secure. None of our member data was compromised by the recent MOVEit data breach.

SRA was made aware in early June of a data breach involving MOVEit transfer software. MOVEit is a file transfer software utilized by SRA to ensure integrity of confidential data transferred to outside entities for specific business purposes. SRA has confirmed that member data maintained by SRA was not affected in the data security incident. To ensure that future submissions would not be exposed to potential vulnerabilities, the SRA Cybersecurity group has established an alternative, highly secure process for transferring the data.

TIAA Member Data May Have Been Compromised

Unfortunately, some eligible faculty members and exempt employees of the University System of Maryland and other public higher education institutions in Maryland who opted to participate in the Optional Retirement Program ("ORP"), and selected investments offered by TIAA, may have been impacted in the third-party data breach. TIAA has advised that while the MOVEit security vulnerability did not affect TIAA systems, it has affected its third-party vendor, Pension Benefit Information, LLC ("PBI"). PBI receives personal data of individual participants from TIAA to assist TIAA in death claim and beneficiary processes. TIAA has determined that personal information of individual ORP participants enrolled with TIAA was involved in the data security incident.

TIAA has advised that impacted members will receive a letter in the mail from PBI in the coming weeks offering free credit monitoring for two years at no cost to them. In the meantime, TIAA urges everyone to continually be on guard for fraud and identity theft and offers these recommendations:

- Enabling multifactor authentication everywhere it is available and not automatically provided. At TIAA, we provide it automatically.
- Creating a unique password with 12 or more characters for each of their online accounts.
- Being wary of oversharing personal information online.
- Being vigilant in spotting email and text phishing attacks, which urgently request personal information for claimed emergencies.
- Keeping personal contact information current with financial institutions and reporting unusual balance activity immediately.
- Regularly monitoring credit score and online accounts.
- Using antivirus software for all devices and updating software, hardware and applications.
- Securing home networks with unique passwords and setting up a unique PIN for mobile phone SIM cards.
- Knowing how to report identity theft and cybersecurity incidents.

You are encouraged to reach out to your assigned TIAA contact with any additional questions. You can also access additional information online from the Federal Trade Commission on how to protect your identity at consumer.gov/idtheft.