



COMMONWEALTH OF MASSACHUSETTS | PUBLIC EMPLOYEE RETIREMENT ADMINISTRATION COMMISSION

PHILIP Y. BROWN, ESQ., Chair

WILLIAM T. KEEFE, Executive Director

Auditor DIANA DIZOGLIO | KATHLEEN M. FALLON | KATE FITZPATRICK | JAMES J. GUIDO | RICHARD MACKINNON, JR. | JENNIFER F. SULLIVAN, ESQ.

MEMORANDUM

TO: All Retirement Boards

FROM: Bill Keefe, Executive Director

RE: Fraud Alert

DATE: July 16, 2025

Please be aware of a different approach in the changing-the-direct-deposit-information scam. In this instance, the fraudster imitated a retirement board employee and worked to have a colleague switch the actual employee's direct deposit information. This resulted in the interception of the employee's paycheck.

The board did not have direct deposit forms on its website; they had to be requested. The colleague sent a direct deposit form to what was represented to be the actual employee's personal email address, but which was instead the fraudster's. The form was returned with a copy of a voided check from Green Dot Bank. For retirees, the board requires notarization as well as verbal confirmation. For employees, verbal confirmation is normally confirmed, but it didn't happen in this case.

When it was discovered that the staffer was not paid, the board acted quickly. It reviewed payroll records and spoke with both employees involved. The board contacted its counsel, insurer, IT provider, bank, law enforcement, the Executive Office of Technology Services and Security (EOTSS) and PERAC. An email was sent to all staff with a follow-up meeting to review procedures for verifying financial information and confirming identities. The board will change its direct deposit forms and review and reconfirm any direct deposit changes submitted since the last retiree payroll was run.

Please review your procedures for verifying financial information and personal identification and evaluate your policies for retirees compared to staff. Stress the importance of verbal confirmation on sensitive matters such as direct deposit changes. Be incredibly skeptical about matters involving Green Dot Bank, which has been used by multiple bad actors.

In between this incident and the ransomware attack we informed you about in Memo 18/2025, there was another attack of a municipality that affected multiple departments, including the retirement board. Further support for the IT professionals' statement that it is not a matter of if an organization will get attacked, it's a matter of when. Thank you for your continued vigilance in preventing attacks, conducting proper planning in case of an attack, and acting quickly and decisively to mitigate an attack.

