OFFICE OF THE INSPECTOR GENERAL
MASSACHUSETTS

Advisory

2024 - 1

Jeffrey S. Shapiro, Esq., CIG
Inspector General

Off-Boarding and Banking Controls Protect Public Funds From Fraud

January 11, 2024

I. Introduction

The Massachusetts Office of the Inspector General (OIG) has a statutory mission under Chapter 12A of the Massachusetts General Laws to mitigate and prevent fraud, waste and abuse of public funds and assets at the state and municipal levels. Pursuant to this authority, the OIG is issuing this advisory recommending that public entities ensure that they adopt and implement strong banking controls to assist them in mitigating the risks of fraud and the misappropriation of assets.

Off-boarding and strong banking controls can mitigate the risks of fraud, misappropriation and abuse of public assets.

II. Problem

Public entities' failure to implement employee cybersecurity training, system access controls, and treasury/financial system controls allows those with fraudulent or nefarious intent to capitalize on such vulnerabilities and exploit public assets.

III. Background

There are 104 public retirement boards in Massachusetts, which include municipal, county, state and specialty group retirement boards with varying portfolios, staffs and sophistication.

In February 2021, one or more bad actors gained access to the email account of the former executive director of one of the Commonwealth's retirement boards. At the time of the executive director's departure, that retirement board did not have offboarding procedures in place to (1) notify its leadership staff and vendors of the organizational change; (2) update the signatory lists on file with its financial institutions to prevent unauthorized transactions; and (3) close the executive director's email account. Through these gaps in controls and a series of unfortunate missteps, the bad actor(s) was/were able to fraudulently transfer $3.5 million of pension fund assets to an unknown foreign bank account(s).[1] In addition, the retirement board's failure to regularly review and reconcile its account statements enabled the fraud to go undetected for eight months, making recovery of the funds more complicated and less likely to be successful.

The Cybersecurity and Infrastructure Security Agency defines cybersecurity as "the art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information."[2] While no control, procedure or safeguard can eliminate all risks, the retirement board's leadership and staff should have taken basic steps to mitigate the risk of fraud by having controls in place to detect such activity in a timely manner.

IV. Recommendations

The OIG strongly recommends that all retirement boards, state agencies and municipalities implement the controls described herein to lessen the risks of public funds being misappropriated.

1. **Training Control**

a. All employees of public entities should participate in cybersecurity training upon hire and at least annually thereafter. When practical, training should include simulated phishing attempts to test compliance with procedures. Each public entity should maintain a log to document the successful completion of required trainings by leadership and staff and appropriately follow up to ensure full compliance by all agency leadership and others with system access or account authorization.

2. **System Access Controls**

a. Public entities should develop, document and implement controls and procedures to periodically (at least annually) review user access to ensure that only authorized individuals can gain entry to operational systems and that each individual's level of access is appropriate based on their business responsibilities.

b. On the same day as an employee's termination, resignation or retirement, regardless of the role they are vacating, public entities should block the departing individual's access to business

email, web-based portal systems, (*i.e.*, banking, investing, accounting, financial, payroll, and other remote access, applications or portals), and agency paper and electronic records, including facility and computer systems. The public entity should also communicate, both internally and externally, with vendors, business partners and others, that the now-former employee is no longer authorized to transact business on the entity's behalf.

3. Treasury Controls

a. The governing body of public entities should maintain a written list of the persons authorized to act and sign on behalf of that entity with respect to its bank and investment accounts. Governing bodies should revise and communicate the list at least annually and immediately upon the departure of any authorized person.
b. Public entities should grant financial system access to only the smallest number of individuals, who should always be given the least amount of access consistent with their specific job responsibilities.
c. Only authorized individuals should initiate banking transactions, with review and approval by a second authorized employee. For audit purposes, public entities should retain evidence of each approval in accordance with the entity's records retention policy.
d. Public entities should restrict authorization to initiate wire or other electronic transfers (*i.e.*, from investment accounts to operating accounts, from operating accounts to vendors), or any other movement or transfer of funds, to the smallest number of authorized personnel possible, while also ensuring that appropriate checks and balances are in place.
e. Authorized individuals should make vendor payments only from operating accounts and should have their own usernames and passwords to access online accounts, including investment portals. Entities should configure investment portals to prohibit the same person from both initiating and approving transactions.
f. Public entities should require multi-factor authentication for all financial transactions. In addition, each entity should set a threshold amount that triggers an additional review and approval from a separate authorized individual prior to being processed.
g. One individual should prepare monthly reconciliations for all bank and investment accounts, with review and approval by another to ensure proper segregation of duties. Each public entity should ensure that variances greater than its predetermined threshold are researched, explained and resolved. For audit purposes, public entities should retain evidence of reconciliation approvals in accordance with the entity's records retention policy.

4. Regularly Scheduled Reviews and Control Updates

a. Public entities should regularly (at least annually, or upon changes in personnel, systems, vendors or risks) review and update all controls to reflect the latest technology and to mitigate always-evolving fraudulent schemes.

---

[1] Separate and apart from the OIG's investigation and review, law enforcement conducted its own investigation.

[2] The Cybersecurity and Infrastructure Security Agency, established in 2018 as part of the U.S. Department of Homeland Security, leads efforts to manage and reduce risks to the nation's cyber and physical infrastructure.

Resources

OIG Fraud Hotline
1-800-322-1323
IGO-FightFraud@mass.gov

Subscribe to the
OIG Bulletin

OIG Academy
MA-IGO-Training@mass.gov