



The City of New York
Department of Investigation

JOCELYN E. STRAUER
COMMISSIONER

180 MAIDEN LANE
NEW YORK, NY 10038
212-825-5900

Release #36-2025
nyc.gov/doi

**FOR IMMEDIATE RELEASE
WEDNESDAY, SEPTEMBER 17, 2025**

**CONTACT: DIANE STRUZZI
CLODAGH MCGOWAN
(212) 825-5931**

DOI ISSUES REPORT AND RECOMMENDATIONS TO REMEDY GAPS IN CITY RETIREMENT SYSTEM'S INTERNAL CONTROLS BASED ON CRIMINAL INVESTIGATION OF PENSION THEFT BY FORMER NYCERS EMPLOYEE

Jocelyn E. Strauber, Commissioner of the New York City Department of Investigation ("DOI"), issued a Report today on the theft of pension funds managed by the New York City Retirement System ("NYCERS"), finding critical vulnerabilities in NYCERS' internal controls, including system access controls, verification procedures, and the failure to properly segregate sensitive tasks related to pensioners' payments among different units and employees. This Report was prompted by a criminal investigation that resulted in the arrest and conviction of a now former NYCERS Associate Retirement Benefits Examiner who exploited internal control weaknesses and stole \$624,000 from the accounts of two pensioners. That former employee was sentenced today to up to three years in prison. As part of this Report, DOI made 11 recommendations to strengthen NYCERS internal controls. A copy of the Report is attached to this release and can also be found here: <https://www.nyc.gov/site/doi/newsroom/public-reports-current.page>

DOI Commissioner Jocelyn E. Strauber said, "This Report details DOI's investigation into pension fraud by a NYCERS' employee who was sentenced to prison today for stealing \$624,000 from two pensioners' accounts. The investigation revealed that NYCERS needs to strengthen its internal controls, including its review of suspended accounts and employee training, and to implement additional security practices to detect and prevent fraud. I urge NYCERS to accept and implement the 11 recommendations DOI has made to protect the pension system, and I thank NYCERS for its cooperation with this investigation."

Between February 2021 and January 2024, Gregory Mathieu, an Associate Retirement Benefits Examiner at NYCERS, exploited internal control weaknesses to fraudulently divert approximately \$624,000 in pension funds from two retirees' accounts. The fraudulent scheme involved forged Electronic Fund Transfer ("EFT") Authorizations, manipulated member profiles, and unauthorized reactivation of suspended pension accounts. DOI investigated this case with the Kings County District Attorney's Office, which handled the prosecution. In April 2025, Mathieu pled guilty to Corrupting the Government in the First Degree, a class B felony, and agreed to a sentence of one to three years in prison, and to pay \$511,115.61 in restitution. In addition, NYCERS was able to recover approximately \$113,000 of the \$624,000 in stolen funds from an account controlled by the defendant. Today, September 17, 2025, Mathieu was sentenced to up to three years in prison. The press release on Mathieu's sentencing can be found here: <https://www.nyc.gov/site/doi/newsroom/press/2025/september.page>

This Report describes DOI's findings with respect to Mathieu's fraudulent diversion of pension funds and NYCERS' internal control failures that arguably facilitated this conduct and allowed it to continue undetected, and makes recommendations for policy and procedural change to address these failures. This Report also describes findings from several DOI investigations regarding unauthorized pension account takeover, fraudulent NYCERS loan applications, and NYCERS' remedial action in response to DOI's prior recommendations intended to protect the pension system from theft and fraud.

While NYCERS has implemented significant security enhancements following Mathieu's criminal conduct, continued vigilance and improvement of internal controls remain essential to prevent future fraudulent activities and to protect the pension assets of City employees. DOI recommends the following:

more

1. Internal Control Improvement
 - a. Regular review of reactivated suspended accounts, especially those with monthly pension payments of \$3,000 or higher.
 - b. Periodic audit of retroactive payments and enhanced monitoring of returned payment patterns.
 - c. Regular assessment of access control effectiveness.
2. Conduct periodic reviews of all accounts suspended for a period of 3 years to determine if members are still alive. This review should include contact with family members and review of local obituaries and probate court records.
3. Bank account verification processes should be expanded to include EFT requests received via mail.
4. Provide enhanced training for NYCERS employees including regular ethics training emphasizing personal responsibility in fraud prevention.
5. Develop internal fraud algorithms based on risk indicators to:
 - a. Alert staff to duplicate bank accounts or shared contact information across profiles.
 - b. Alert staff to EFT requests to high-risk banks identified in previous fraud schemes.
6. Maintain electronic audit logs for all account access and account changes, including who effectuates such changes.
7. Require two-factor authentication ("2FA") when members contact NYCERS to request account information changes.
8. Notify member via email/SMS immediately upon a login to their account. Include details such as device type, browser, and IP location to help users recognize suspicious access.
9. IP Monitoring: Review or block activity when a login occurs from a geographic region that is inconsistent with prior use (e.g., NYC login followed by overseas access; multiple logins from distant locations in short time).
10. Secure Document Submission Portal
 - a. Replace mail/email/fax submission of sensitive documents (e.g., EFT forms) with a secure upload portal with 2FA authentication.
 - b. Use time-locked session links. By restricting the time a session is active, the risk of unauthorized access is reduced. After a time-out, users need to re-enter credentials, adding an extra layer of security.
11. Require identity confirmation by the relevant US Consulate followed by a NYCERS video call interview for all reactivation requests submitted by members residing overseas.

Commissioner Strauber thanked NYCERS Acting Executive Director Elizabeth Reyes for her and her staff's cooperation, in particular General Counsel Maya Khodos and Associate General Counsel & Privacy Officer Pamela Zable.

The investigation was conducted by Confidential Investigator Farhana Begum with DOI's Office of the Inspector General for NYCERS and was supervised by Assistant Inspector General Shakina Griffith, Deputy Inspector General Aleksandro Tilka, Inspector General Ann Petterson, Deputy Commissioner of Strategic Initiatives Christopher Ryan, and Deputy Commissioner/Chief of Investigations Dominick Zarrella.

DOI is one of the oldest law-enforcement agencies in the country and New York City's corruption watchdog. Investigations may involve any agency, officer, elected official or employee of the City, as well as those who do business with or receive benefits from the City. DOI's strategy attacks corruption comprehensively through systemic investigations that lead to high-impact arrests, preventive internal controls and operational reforms that improve the way the City runs.

DOI's press releases can also be found at twitter.com/NYC_DOI
Know something rotten in City government? Help DOI Get the Worms Out of the Big Apple.
Call: 212-3-NYC-DOI or email: Corruption@DOI.nyc.gov

New York City
Department of Investigation



DOI Investigation of Theft
Involving Pension Funds Managed by the
NYC Employees' Retirement System
(NYCERS) and Related Recommendations

Jocelyn E. Strauber
Commissioner

Ann Petterson
Inspector General for New York City Employees' Retirement
System

September 2025

Content

I.	Executive Summary	3
II.	Investigative Findings	4
	A. NYCERS Employee Gregory Mathieu’s Pension Fund Theft	4
	B. Platform Conversion/Fraudulent Loans/Account Takeover	8
III.	Conclusions and Recommendations	9

I. Executive Summary

The New York City Employees' Retirement System ("NYCERS") was established in 1920 and is the largest municipal public employee retirement system in the United States, with more than 430,000 active members and retirees including civilian and uniformed employees. NYCERS is governed by a Board of Trustees and is responsible for investing the assets of the retirement system, establishing the system's administrative budget and promulgating related rules and regulations. The NYCERS Board of Trustees consists of eleven members: a representative of the Mayor, the City Comptroller, the Public Advocate, the heads of the three unions with the largest number of participating employees, and the five Borough Presidents.¹

The Department of Investigation's ("DOI") Office of the Inspector General for NYCERS, recently concluded an investigation of pension theft by a NYCERS employee. Between February 2021 and January 2024, Gregory Mathieu, an Associate Retirement Benefits Examiner² assigned to NYCERS' Pension Verification and Recovery Unit ("PVARU"), exploited internal control weaknesses to fraudulently divert approximately \$624,000 in pension funds from two retirees' accounts. The fraudulent scheme involved forged Electronic Fund Transfer ("EFT") Authorizations, manipulated member profiles, and unauthorized reactivation of suspended pension accounts. DOI investigated this case with the Kings County District Attorney's Office ("KCDA"), which handled the prosecution. Mathieu pled guilty to first-degree Corrupting The Government (NYS Penal Law §496.05) and agreed to a sentence of one to three years in prison, and to pay \$511,115.61 in restitution. In addition, NYCERS was able to recover approximately \$113,000 of the \$624,000 in stolen funds from an account controlled by the defendant. On September 17, 2025, Mathieu was sentenced to up to three years in prison.

This case revealed critical vulnerabilities in NYCERS' internal controls, particularly regarding segregation of duties, system access controls, and verification procedures. Following the investigation, NYCERS implemented comprehensive reforms to address these vulnerabilities.

This report describes DOI's findings with respect to Mathieu's fraudulent diversion of pension funds and NYCERS's internal control failures that arguably facilitated this conduct and allowed it to continue undetected, and makes recommendations for policy and procedural change to address these failures. This report also describes findings from several DOI investigations regarding unauthorized pension account takeover, fraudulent NYCERS loan applications, and NYCERS' remedial action in response to DOI's recommendations.

¹ <https://www.nycers.org/about>.

² Associate Retirement Benefits Examiner responsibilities include reviewing and calculating years of service, determining membership eligibility, and obtaining and updating beneficiary or pensioner information in the NYCERS system.

II. Investigative Findings

A. NYCERS Employee Gregory Mathieu’s Pension Fund Theft

DOI’s recent investigation of pension fund theft by Mathieu demonstrates the critical need for improved internal control mechanisms at NYCERS, including segregation of duties to reduce the risk of theft by NYCERS’ employees. As described in detail below, Mathieu, an employee of NYCERS since 2009, used his familiarity with and access to NYCERS’ data and systems to divert two retirees’ pension funds to a bank account which he controlled. Mathieu stole approximately \$624,000 in pension funds between February 8, 2021, and January 2, 2024.

Mathieu’s scheme exploited the NYCERS’ pension suspension and reactivation process. NYCERS suspends pension payments when pension checks are returned to NYCERS (by the bank, US Postal Service, etc.) or when a pensioner fails to respond to a NYCERS’ inquiry to determine whether the pensioner is still alive and eligible for benefits. That inquiry is conducted by the PVARU, which is responsible for determining whether the pensioner is still eligible for payments, and, if so, reactivating the pension account. Among other things, the pensioner must complete a Payroll Verification Affidavit³ (“PVA”) to reactivate the account. The suspension process, and the reactivation mechanism, are sound controls intended to avoid payment of pension checks to deceased pensioners. In 2012, DOI issued a report concerning fraud by third parties involving deceased beneficiaries and issued a number of recommendations to ensure that deceased pensioners were removed from the pension payroll.⁴

NYCERS identifies a pension recipient as deceased or potentially-deceased through the following ways: a) notification from the decedent’s family, friends, unions, or banks; b) death match reports; and c) non-responsiveness to a PVA request.

Each month, NYCERS compares suspended pension payment files with data from the Social Security Death Master File to determine if any pension members have passed away. All members of PVARU have access to the death match report. If the holder of a suspended pension account has not been reported deceased, and the account holder fails to respond to NYCERS’ PVA inquiry, the account can remain suspended indefinitely. If the account is subsequently reactivated, the account holder will receive retroactive benefits that were due during the suspension period.

DOI’s review of NYCERS records identified systemic vulnerabilities that enabled Mathieu to manipulate NYCERS’ processes without detection. Mathieu first reactivated the pension of a deceased Department of Sanitation supervisor (“Pensioner A”), who died on January 8, 2018. Pensioner A’s death was not reported to NYCERS and Pensioner A did not appear in the death match reports. After several of Pensioner A’s checks were returned to NYCERS, and Pensioner A did not respond to a PVA request in May 2018, NYCERS suspended Pensioner A’s account.

³ If NYCERS suspects that a pensioner is deceased, or once the pensioner reaches 85 years of age, the PVA is sent to the pensioner for them to complete, notarize, and return to NYCERS.

⁴ <https://www.nyc.gov/assets/doi/reports/pdf/2012/2012-05-09-Pr12pension.pdf>

Mathieu reactivated Pensioner A’s account in February 2021, stole retroactive payments of approximately \$242,000, and continued to receive Pensioner A’s reinstated monthly pension payments of approximately \$5,700 until January 2024, when the scheme was detected. Mathieu also reactivated the suspended account of a retired Associated Railroad Signal Specialist employed by the MTA/NYC Transit Authority (“Pensioner B”). Pensioner B’s account was suspended in December 2019 because he failed to cash three of his pension checks and did not respond to a request to complete a PVA in August 2019. Mathieu reactivated Pensioner B’s account in October 2023 and stole approximately \$199,000.

The scheme was revealed only when Pensioner B visited NYCERS in January 2024, seeking to reactivate his pension account and claiming he had not received payments since 2019. When NYCERS informed Pensioner B that his pension payments were electronically deposited, Pensioner B stated that he had no account at the specified bank. Petitioner B then filed a stolen identity report with the New York City Police Department (“NYPD”).

NYPD identified Mathieu as the sole authorized user of a rented BMW that was captured on ATM machine surveillance footage during multiple cash withdrawals between October 2023 and December 2023, from the account into which Pensioner B’s payments had been electronically deposited. In January 2024, NYPD referred the case to DOI and shortly thereafter, NYCERS advised DOI of the alleged fraud and suspended Mathieu.

DOI’s investigation of Mathieu revealed the fraud involving Pensioner A. In February 2021, NYCERS received a handwritten Form 380, Authorization for an EFT, purportedly from Pensioner A, including an address change. As a result of the EFT request, Pensioner A’s NYCERS account was reactivated. NYCERS calculated that Pensioner A was entitled to retroactive payments of \$225,432.80, to be paid in installments, beginning with a \$99,999.99 payment in February 2021.⁵

On March 3, 2021, NYCERS Accounting and Banking Services (“ABS”) unit received notification that the \$99,999.99 payment to Pensioner A was rejected due to a closed bank account. On that day, Mathieu created an online bank account at a different financial institution in the name of Pensioner A. The following day, an online MyNYCERS⁶ account was created under Pensioner A’s name, followed by a new EFT request through this account. NYCERS automated bank account verification validated the account as active and matching the pensioner’s name. After several failed attempts to deliver the replacement check, which was issued by the Comptroller’s Office on July 21, 2021, Mathieu sent an email to NYCERS ABS directing that the check be cancelled and claiming Pensioner A requested an EFT.

⁵ Due to NYC Comptroller limitations, each individual payment may not exceed \$100,000.

⁶ MyNYCERS is an account management program which provides information and forms for employees and members to apply for membership, take out loans, sign up for direct deposit, change an address, and designate beneficiaries, among other actions.

While this \$99,999.99 payment was returned several times⁷, a potential risk factor for fraud, NYCERS did not flag the account or otherwise subject it to additional scrutiny. DOI raised this issue with NYCERS, and banking operations have been modified to address this oversight. NYCERS now analyzes returned checks for potential fraud and requires pensioners to verify in-person or via live video that the account should be reactivated before NYCERS will produce a benefit check, especially for long-term suspensions.

Regarding Pensioner B's pension account, DOI learned that an EFT form for Pensioner B was date-stamped by the NYCERS mail room on October 11, 2023. Pensioner B did not request an EFT change and never mailed this form to NYCERS. DOI's review of NYCERS mailroom surveillance footage shows Mathieu in the mailroom at the approximate time the form was received. DOI believes that Mathieu delivered the form to the mailroom and caused it to be date-stamped so it would appear that it came from an outside source. In addition, the EFT form listed a Connecticut address, not the address listed in Pensioner B's NYCERS profile, and bank account information that was the same as Pensioner A's bank account information. These discrepancies, and the fact that same bank account was used for payments to two non-related pensioners, should have been detected by NYCERS as potential warning signs.

NYCERS protocols also do not require account verifications for EFTs received by mail. NYCERS explained that the automated bank verification step is performed for EFT changes and online loan applications filed via MyNYCERS. Therefore, Pensioner's B bank account was updated without validity of the bank account. As outlined in the conclusion section, DOI is recommending that NYCERS verify all bank accounts, including EFTs received by mail.

A review of Mathieu's work emails revealed that on October 17, 2023, Mathieu received an email from his personal email address, attaching a falsified bank statement in the name of Pensioner B. Subsequently, Mathieu sent an email to a NYCERS' Pension Payroll employee with that bank statement and requested that Pensioner B's EFT be processed for the October 2023 pension payroll. The ABS unit, without conducting independent verifications, relied on Mathieu's instruction and processed the request, updating Pensioner B's payment method to direct the electronic deposit of funds into an account Mathieu controlled.

During the course of this investigation, DOI conducted a forensic analysis of all NYCERS electronic devices assigned to Mathieu. DOI was informed that NYCERS did not maintain an audit trail of account access that would have shown when Mathieu accessed various NYCERS systems relating to the pension benefits.

DOI's investigation included a review of transaction records and internal communications to understand how Mathieu was able to circumvent the safeguards NYCERS had in place. In April and May 2025, DOI met with NYCERS executives to discuss the findings of the Mathieu investigation and strategies to limit the risk of fraud on member accounts. As indicated above, Pensioner A and B's accounts had been suspended for over three years and each had relatively

⁷ The USPS noted on the returned check that the address was "vacant." The check was reissued to the same address.

high monthly pension payments of \$5,663 and \$6,344, respectively. By targeting these particular accounts, Mathieu was able to generate and steal significant retroactive payments, over \$640,000 in total, including payments that NYCERS should not have been making in the first instance because Pensioner A was deceased. As a product of these meetings and many other discussions between DOI and NYCERS in the aftermath of Mathieu's theft, NYCERS decided to restrict access to the suspended pensioner file to the PVARU supervisor, and to store the file in a locked folder. Because fraudulent EFT requests were made in connection with the reactivation of accounts of Pensioners A and B, NYCERS has changed its practices so that EFT requests no longer trigger an account reactivation automatically. Account reactivation now requires authorization from supervisors in both the PVARU and ABS units, a two-tier approval process.

The fraudulent EFT requests submitted by Mathieu included unauthorized changes to both mailing addresses and banking information. To reduce the risk of this sort of fraud, NYCERS implemented procedures to verify changes to member account profiles. These new procedures require confirmation from the account holder with respect to existing contact information as well as any changes to that information. In the case of address change requests, NYCERS will initiate correspondence to both the address of record as well as the requested updated address. As mentioned earlier, NYCERS has established criteria which will mandate in person or live video confirmation of reactivation request.

Because Mathieu may have used his access to the mailroom to facilitate his fraud, NYCERS has restricted access to the mailroom to authorized mailroom staff.

Mathieu submitted a fraudulent EFT request for Pensioner B using bank information for the account he created for Pensioner A. While NYCERS noted that married NYCERS members may legitimately receive payments to joint accounts, at DOI's recommendation NYCERS has initiated alerts that flag common accounts for more than one member.

DOI also addressed concerns regarding identity theft and NYCERS employee access to member profile information with NYCERS senior staff. To mitigate insider threats, DOI recommended that NYCERS implement an auditing function so that NYCERS can track and retain data about access to member accounts.

Lastly, DOI emphasized the importance of prompt notification by NYCERS to DOI of suspected fraud. Pensioner B reported to NYCERS in person that he had not authorized any changes to his banking information and that he had not received any pension payments. NYCERS did not report this information to DOI. Immediate notification to DOI would have prompted an investigation that could have limited the extent of the fraud.

In response, NYCERS recently implemented an Anti-Fraud and Anti-Corruption Policy to raise awareness by educating staff on the various tactics, techniques, procedures, and indicators of fraud and corruption. In addition, DOI is scheduled to present a series of anti-corruption presentations to NYCERS staff. NYCERS also has established an anonymous whistleblower hotline and reminded staff members of their obligation to report fraud to DOI.

Mathieu’s case highlights the importance of robust internal controls, comprehensive fraud prevention training, and systematic oversight in pension administration. In the aftermath of Mathieu’s breach, NYCERS initiated the following improvements:

- Imposing a two-tier level approval process for particular account activities
- Increasing outreach to confirm pensioner status
- Restricting access to suspended account data, date of death matching analysis, and the NYCERS’ mailroom
- EFT requests will no longer automatically trigger account reactivation
- Augmenting the returned check verification process
- Mandating in person/remote video conferencing confirmation for account reactivation requests

B. Platform Conversion/Fraudulent Loans/Account Takeover

In 2020, NYCERS introduced a digital account management platform called “MyNYCERS”. With the launch of MyNYCERS, members are required to re-register their account information to establish an online account in the new system. Subsequently, in investigations distinct from the above-referenced Mathieu investigation, NYCERS and DOI found an increase in attempted fraud by unauthorized individuals accessing member accounts and altering member mailing addresses, email addresses, phone numbers and designated bank account information. In some instances, fraudulent loan requests resulted in the theft of funds from member accounts. Challenges brought by COVID-19, such as undelivered mail and suspension of in-person appointments, exacerbated the risk of fraudulent account takeovers and loan applications.

Currently, NYCERS has 430,000 members; 190,017 are actively receiving City payroll, the remainder are retirees receiving pension benefits. To date, more than half of NYCERS members have not re-registered on the MyNYCERS platform. In June 2023, DOI recommended and NYCERS implemented a number of security measures to protect those individuals and reduce the risk that their accounts would be subject to theft or fraud. These measures limit access to NYCERS accounts by: a) IP addresses associated with previous fraud attempts; b) IP addresses used with five or more devices; d) multiple email addresses used by one device; and e) email addresses that are newly created and not associated with a single individual. Additionally, pursuant to DOI’s recommendation, members are now notified and asked to confirm any changes to their bank account information before such changes are made.

In response to DOI recommendations, NYCERS also has implemented several security enhancements to improve the member verification process during account registration. NYCERS’ risk management service now uses additional risk scoring metrics to mitigate unauthorized account access. To protect sensitive internal processes intended to mitigate fraud risk, specific details regarding the security enhancements NYCERS has implemented are not discussed in this public report.

DOI and NYCERS continue to collaborate on improvements to NYCERS' internal controls. Continued vigilance and improvement of internal controls remains essential to prevent future fraudulent activities and protect the pension assets of city employees.

III. Conclusions and Recommendations

Mathieu's case highlights the importance of robust internal controls, comprehensive fraud prevention training, and systematic oversight in pension administration. While NYCERS has implemented significant security enhancements following this incident, continued vigilance and improvement of internal controls remain essential to prevent future fraudulent activities and to protect the pension assets of city employees. To this end, DOI recommends the following:

1. Internal Control Improvement
 - a. Regular review of reactivated suspended accounts, especially those with monthly pension payments of \$3,000 or higher.
 - b. Periodic audit of retroactive payments and enhanced monitoring of returned payment patterns.
 - c. Regular assessment of access control effectiveness.
2. Conduct periodic reviews of all accounts suspended for a period of 3 years to determine if members are still alive. This review should include contact with family members and review of local obituaries and probate court records.
3. Bank account verification processes should be expanded to include EFT requests received via mail.
4. Provide enhanced training for NYCERS employees including regular ethics training emphasizing personal responsibility in fraud prevention.
5. Develop internal fraud algorithms based on risk indicators to:
 - a. Alert staff to duplicate bank accounts or shared contact information across profiles.
 - b. Alert staff to EFT requests to high-risk banks identified in previous fraud schemes.
6. Maintain electronic audit logs for all account access and account changes, including who effectuates such changes.
7. Require two-factor authentication ("2FA") when members contact NYCERS to request account information changes.
8. Notify member via email/SMS immediately upon a login to their account. Include details such as device type, browser, and IP location to help users recognize suspicious access.
9. IP Monitoring: Review or block activity when a login occurs from a geographic region that is inconsistent with prior use (e.g., NYC login followed by overseas access; multiple logins from distant locations in short time).
10. Secure Document Submission Portal
 - a. Replace mail/email/fax submission of sensitive documents (e.g., EFT forms) with a secure upload portal with 2FA authentication.
 - b. Use time-locked session links. By restricting the time a session is active, the risk of unauthorized access is reduced. After a time-out, users need to re-enter credentials, adding an extra layer of security.

11. Require identity confirmation by the relevant US Consulate followed by a NYCERS video call interview for all reactivation requests submitted by members residing overseas.