KPMG
cutting through complexity

The City of New York

# The City of New York

## Report on Disbursement Process and Controls Assessment

July 3, 2014

# Contents

# 1. Introduction

The City of New York Office of Management and Budget ("OMB") and the New York City Comptroller's Office ("Comptroller", and together with OMB, the "City") requested KPMG LLP (KPMG) to review the design and operation of selected manual and automated information technology (IT) controls over the pension payment disbursement process performed by the New York City Financial Information Services Agency (FISA). Specifically, the City wanted to document the cause of the erroneous payments made based on electronic instructions processed by FISA on April 30, 2014, and to identify and recommend improvements to processes and controls to prevent such future disbursement errors.

The primary objective of this assessment was to identify the events and control failures that led to the erroneous payments made to 31,015 New York City Police and Fire and Superior Officers Pensioners on April 30, 2014, for a total value of approximately $298.4 million. The secondary objective of this assessment was to identify and evaluate the sufficiency of the design of additional controls implemented by FISA and OPA to prevent similar unexpected payments.

As part of this assessment, KPMG met with FISA, the New York City Office of Payroll and Administration ("OPA"), OMB, and the Comptroller's office to interview key personnel and gather supporting documentation related to this event. KPMG shared the preliminary draft of this report and obtained feedback from FISA, OPA, OMB, and the Comptroller's office before submitting the final deliverable.

## Executive Summary:

The erroneous payments that occurred on April 30, 2014 resulted from a test of a proposed system change which led to the creation of an Electronic Funds Transfer (EFT) request that was transmitted to JP Morgan Chase Bank ("Chase" or "the Bank"). This request was processed by Chase as part of the normal business operations between the City and Chase and led to the disbursement of funds to 31,015 Pensioners. It is our understanding that the City, working with the Bank, has recovered over 99 percent of the funds and is working with a limited number of Pensioners on recoupment plans to recover the remaining amount.

The system change being tested was not planned or intended to test the EFT transmission process to the Bank. It was intended to test specific steps within the City's processing of Child Support deductions from the pension payments. The change also included sending the deducted amount using EFTs instead of check payments to the appropriate jurisdiction (i.e., counties or states) and sending the balance of the pension amount to the Pensioners as EFTs.

During our assessment we noted control weaknesses and the absence of controls in the Production environment. These control issues crossed multiple functions and processes within FISA and OPA including FISA Testing and Operations Support and OPA's confirmation process. It was noted that many controls do exist, but need to be strengthened, while other controls did not exist. These control weaknesses and absent controls included preventive, detective, manual, and automated controls.

During our assessment, FISA and OPA have shared with us the changes to the controls that they have already implemented. The mitigation measures as designed will help address the control weaknesses identified in this report.

## Organization of this Report:

The remainder of this report is organized as follows:

- **Section 2** provides the time line of events that led to the erroneous payments on April 30, 2014.

- **Section 3** provides an assessment of the production controls.
- **Section 4** documents the mitigation steps planned and taken by the FISA and OPA and KPMG's assessment of the mitigation steps.
- **Section 5** introduces additional recommendations provided by KPMG for the City's consideration.

# 2. Time Line of Events

Due to a series of events discussed below, 31,015 New York City Fire Department and Police Department Pensioners received an overpayment of approximately $298.4 million in pension funds. In an effort to fully understand the events and assess the controls in the pension payment system that may have contributed to these payments, KPMG met with teams from FISA and OPA. Based on these meetings, KPMG noted the following summary of events:

1. April 1, 2014–April 30, 2014 – FISA was working on the development and testing of a change request for the active payroll system and the pension payment system. The change request was to deduct Child Support payments from the regular pension payments. Chase was also requested to send the child support payment and the remaining pension payments through an EFT process, rather than through the issuing of paper checks.
2. April 30, 2014 (a.m.) – FISA scheduled a Production EFT payment per a planned payment schedule for the pension payment system. That morning, FISA's Operations Support reviewed the EFT payment file and sent the reports associated with the EFT payment to the OPA for approval. After the OPA confirmation, the first version of the EFT payment file was placed in a server location in order to send the file to Chase later in the afternoon. This was a standard process for all EFT payments for PPMS and PMS systems that was followed by both FISA and OPA.
3. April 30, 2014 (a.m.) – For the end-to-end PPMS payment cycle testing within the pension payment system's Test environment, FISA used the Production data set from the December 2013 pension payments. The file name of the output EFT Test file was the same name as the Production EFT file (discussed above)
4. April 30, 2014 (a.m.) – A test job was run to verify the accuracy of the Cash Concentration and Disbursement Plus (CCD+) payments for the Variable Supplements Funds (VSF) PPMS cycle for 31,015 Pensioners. The test job created a test version of the Issued Payments report. However, the output of this test job incorrectly placed the test report in the production Report Management and Distribution System (RMDS). When OPA reviewed this test report in the production RMDS region; they recognized that the report was incorrect, and the counts and amounts did not match the previous version of the report reviewed by the OPA for scheduled production payment (for only 3 Pensioners). OPA reported this issue to the FISA help desk and FISA reviewed the test Job Control Language (JCL) found the error in a test procedure. This was corrected by FISA and the test report was removed from RMDS. However, FISA did not realize that the associated EFT test file corresponding to the EFT report in the RMDS system, should also be removed. A complete root cause analysis for this defect was not performed effectively.
5. April 30, 2014 (a.m.) – Due to weak and missing controls (discussed above) in the Production environment security, the output Test EFT file, containing Production data and bearing the same production name, was written to the Production environment with the latest version number.
6. April 30, 2014 (2:44 p.m.) – The latest version of the Test EFT file, which was incorrectly named as a Production EFT file, was sent to Chase. The original, intended version of the payment file was never sent to Chase.
7. April 30, 2014 (p.m.) – Upon receipt of the payment request, Chase sent an e-mail acknowledgment to OPA (2:48 p.m.) confirming the receipt of an EFT request indicating the total number of entries and total dollar amount. At this time, OPA should have been able to respond to the Bank to cancel the disbursement; however, a confirmation from OPA to the Bank to proceed with the payment request was not required. The Chase acknowledgment e-mail to OPA was sent to two employees who were absent that afternoon, therefore, OPA did not respond to the Chase confirmation.
8. April 30, 2014 (11:50 p.m.) – As Chase did not receive notification from the OPA to cancel the disbursement, the Bank honored the payments requested by FISA and disbursed the money from the City's bank account to the Pensioners' bank accounts. The Bank account did not have funds to honor the payments, as the accounts were not funded by the City Comptroller's Office for this nonscheduled payment. However, Chase used the overdraft line of credit allocated to the City to make these payments.

9. May 1, 2014 (a.m.) – The Police Pension Fund received calls from Pensioners, inquiring about the unexpected payment received in their bank account(s). The Police Pension Fund's Facebook social media page also had posts from Pensioners regarding these unexpected payments.
10. May 1, 2014 (a.m.) – The Police Pension Fund contacted FISA about the calls received regarding unexpected payments and requested that FISA investigate. FISA contacted OPA to notify the team about the reported unexpected payments and to discuss next steps—including the reversal of the EFT payments.
11. May 1, 2014 (p.m.) – After continued investigation, the team found that a total of 31,015 unexpected payments, worth approximately $298.4 million, were made on April 30, 2014.
12. May 1, 2014 (p.m.) – FISA requested a reversal of the EFT payment executed and the Bank was able to recoup a majority of the Pensioners' payments (recoupment from 288 Pensioners was not completed).
13. May 2, 2014–May 5, 2014 – FISA continued to work with the Bank to execute secondary processes to reverse the unexpected payments.
14. May 5, 2014 (a.m.) – Chase honored the EFT reversal request from the City and issued a payment crediting the City's pension bank account for approximately $295.4 million for the unexpected/incorrect payments. Chase has undertaken an effort to recoup the remaining funds disbursed to the NYC Pensioners' bank accounts. At this time, the Bank has recouped over 99 percent of the funds.
15. Ongoing – Daily reports are issued by the Comptroller's office and FISA to track the amounts recovered from the Pensioners. OPA and FISA continue to work with the pension funds to recover the remaining funds.

# 3. Production Controls

## Assessment of Production Controls

In walking through the series of events that occurred prior to the unexpected disbursement of pension payments, KPMG assessed the controls in the PPMS system. The following control weaknesses and absent controls were noted:

1. **Use of Production PPMS Data in Testing Process without Redaction**
   FISA uses the PPMS Production environment data and copies it into the Test environment for functional PPMS payment cycle testing. While copying the data from Production to Test environment, the bank account numbers, bank routing numbers, and user identifiers are not redacted or scrambled. Per FISA, the testing partners in other City agencies such as OPA and the Pension Funds do not have adequate tools and processes to redact the data in a synchronized way so that the redacted data can still be used for end-to-end payment cycle testing. The test data used in this particular event was Production data from the December 2013 pension disbursement that included the names and information of the Pensioners, as well as their bank account numbers. The testing scenario generated an output Test EFT file meant for testing purposes. However, in conjunction with the other control deficiencies noted by FISA (see below), the output Test EFT file containing Production data was written into the Production environment. From the Production environment, the Test EFT file was sent to Chase and funds were disbursed into Pensioners' bank accounts.

2. **Operations Support Process – FISA**
   The EFT transmission program sending the EFT file to Chase does not run immediately after the FISA Operations Support team verifies the EFT file. There is a lag in time between the time the FISA Operations Support team verifies a specific EFT file version and the time the transmission program sends the latest version of the file to Chase. At the time of the unauthorized transmission, the process pushed the latest data set to the Bank. The combination of the time lag and the programming to release the latest (rather than a specifically named and time stamped) dataset, and control gaps #3 and #4 below, created an opportunity for a newer version of a file that had not been subject to the verification process performed by the FISA Operations Support team, to be transmitted to the Bank.

   After transmission of the file to the Bank, Chase sends an "echo" file to FISA to compare against the EFT file that is verified by the Operations Support team. The "echo" file is a replication of the file sent from FISA to the bank that is sent back to FISA to compare for transmission errors. FISA does not perform any additional verification of total amounts or total transactions in the "echo" file to the EFT report approved by the OPA.

3. **File Naming Standards Document**
   There was no control to ensure that the naming conventions for output EFT files were followed, such that they differentiate the Test EFT file versus a Production EFT file. Per discussion with FISA, the FISA team did not change the test job's output EFT file name from the prefix P (indicating Production) to the prefix T (indicating Test) after copying the job from the Production environment. This was a manual error on the part of the Operations Support team responsible for setting up the JCL for use in the scheduler. There was no peer review of this change performed by the FISA Operations Support team, as this change was considered very simple. If appropriate naming conventions were followed or a control had been in place to verify the naming conventions were followed, the test job would not have generated an output EFT file that could contaminate the Production environment.

4. **System Security**
   There were weaknesses in system security controls that allowed the Production Job Scheduler to run a test program and create a Production output. During the test process, the scheduler software running the automated job flow had a system/service account that had historically been configured with more authority than was necessary to run test job flows. Since this service account had enough authority, it could access the Production Logical Partition (LPAR) even though the test job ran in Test LPAR.

   The Production Job Scheduler was used to run this test program with its system/service accounts that had the authority to access production LPAR even though the test program ran in the Test LPAR. The use of one scheduler between the production and test LPAR, in addition to the lack of security control to separate the production and Test LPARs, contributed to output from the test process being written in the Production environment.

5. **Operations Support Process – OPA**
   The reconciliation/verification process has two major components. The first is a reconciliation of a report by OPA that is generated by the scheduled process which calculates/generates the EFT payment request. This report includes the process, number of payment lines, and the total amount. OPA confirms with FISA that the process is accurate and should be transmitted to Chase. The second reconciliation/verification is when Chase receives the payment request EFT file; it sends an e-mail confirmation to OPA, who confirm the line numbers and amount. The process used by the OPA, is that if there are no issues, then OPA takes no action with this email, and the EFT distribution will occur from Chase. If there are issues, then OPA is to contact Chase that day to either resolve the issue or cancel the process using the Chase Infodex phone number or calling the Chase account liaison assigned for the City.

   On April 30, 2014, OPA received multiple e-mails from the Bank during normal business hours for various EFT payments. One of those e-mail confirmations was related to the approximate $298.4 million unauthorized payment. OPA did not review that e-mail associated with the approximate $298.4 million in a timely manner, as the two OPA employees included on the e-mail confirmation from the Bank were absent—one employee has been on long-term leave since February, and one was absent that afternoon. If one of the two employees had received the e-mail that day, OPA would have had the opportunity to cancel the disbursement by contacting Chase between 2:49 p.m. and 11:50 p.m. on April 30, 2014. If this control was effectively implemented, OPA had the last opportunity to detect this issue and correct it prior to the disbursement.

# 4. Mitigating Procedures

## Mitigation steps taken by FISA and OPA

As discussed above, non-existent or insufficient production controls, including in the segregation of environments and validation / reconciliation of transaction files, contributed to the erroneous disbursement. FISA and OPA have informed KPMG that mitigation by instituting and/or strengthening procedures are already implemented or are in the process of being implemented currently. These new control procedures and their status are listed below. The design and implementation status for each item in the table below was communicated to, ***but has not been verified*** by, KPMG.

| Control Inefficiency | Mitigating Procedure | Responsible Party | Implementation Status |
|---|---|---|---|
| **Use of Production PPMS Data in Testing Process without Redaction** | FISA has instituted a manual control for the Operations Support team, when using PPMS Production data for testing, to scrub the bank routing numbers and the account numbers. All other Pensioner data will continue to be real Production data used in end-to-end cycle testing. | FISA | This procedure has been implemented for future testing. This procedure will be effective in preventing use of Production bank information in testing regions. |
| **Operations Support Process – FISA** | FISA has changed the EFT transmission job to validate if the output EFT file selected for sending to Chase matches the file name used by the FISA Operations Support team by using its payment date and a sequence number. The file will be sent to Chase only if both fields match. | FISA | The procedure identified by FISA, will be an automated control to prevent selecting a file that was not specifically verified by FISA Operations Support. This change has been implemented by FISA. |
| **File Naming Standards Document** | FISA developed a parsing test program to parse the Test JCL code to inspect if any of the EFT output file names has a prefix of "P," which would indicate it is a Production output file in a Test JCL job. If this occurs, an e-mail is sent to the FISA Test Manager and additional FISA employees to raise an alert and fix the Test JCL job. | FISA | The procedures identified by FISA, will be an automated control to detect when a Test JCL job writes an output EFT Test file with a production prefix. This change has been implemented by FISA. |
| **System Security** | FISA has removed the test flows from the configuration of the Production scheduler. Test flows are now run exclusively from a copy of the scheduler that only has access to test resources. The Test scheduler service account privileges are modified to only access test resources. Therefore, any attempt by the Test scheduler to write into the Production environment will fail. | FISA | This is a key security preventive control, having separate schedulers for the Production and Test environments, and having separate production and test service accounts with different privileges, will prevent a test job from writing into production. This change has been implemented by FISA. |

| | | | |
|---|---|---|---|
| **Operations Support Process – OPA** | OPA receives an acknowledgement e-mail from Chase on the EFT request made by the City. Only two employees in OPA are included on the e-mail distribution list. Both employees were absent on April 30, 2014. In future e-mail chains, OPA has requested that Chase include additional OPA employees as backup for absent employees and include FISA's Operations Support team. | OPA | This key preventative control is a fail-safe of last resort for OPA to review and intervene if an unexpected EFT file acknowledgment email is sent from Chase. This change has been implemented by OPA.<br><br>At this time, if there are any issues in the EFT acknowledgement, the OPA calls Chase bank's liaison appointed for the City.<br><br>The City has signed an agreement with Chase for the use of Infodex in conjunction with Pension Payroll payments. |

# 5. Additional Recommended Control Improvements

Based on discussion with FISA and OPA regarding the pension disbursements processes and a review of current controls and planned control improvements, KPMG proposes the following additional recommendations to further strengthen controls. The City should consider the following recommendations, or implement other equivalent controls that are designed to achieve the same results:

| Control Inefficiency | KPMG Recommendation |
|---|---|
| **Use of Production PPMS Data in Testing Process without Redaction** | FISA, OPA, and the Comptroller's office should discuss additional personally identifying data that can be redacted in Test data, including, but not limited to, social security numbers, dates of birth, home addresses, names, and phone numbers within all of their internal testing environments. This will take more time and coordination in each agency, but will assist in avoiding security breaches and accidental disbursements while still enabling efficient testing. |
| **Operations Support Process – FISA** | In the monitoring and review of each job, FISA should develop a documented step-by-step checklist procedure for use of Production data in testing. This checklist will be used to proactively educate new resources for consistency in the testing process. One critical step in this procedure would be to confirm that the output file has been renamed to change all the prefixes from a "P" to a "T" in the test job script.<br><br>FISA should also consider implementing a comparison of the Chase "echo" file returned to the output EFT file version that is verified by the FISA Operations Support team. This comparison should also include comparing total EFT counts and dollar amounts with the EFT report sent to the OPA corresponding to the EFT file. |
| **File Naming Standards Document** | FISA should document the job naming conventions when copying from Production to Test environment, and document the EFT file versioning convention (using payment date and version number) so that the entire FISA Operations Support team, Testing team, and Job Controls team can understand and follow the process consistently. This documentation will serve as a proactive measure to educate new resources in each team supporting the EFT process and testing. |
| **System Security** | The FISA team should consider updating the checklist to modify the configuration in the Test environment and confirm the authority of the test ID service account, so that test IDs used do not provide access to the Production environment. Additionally, it is a leading practice to have the access control list (ACL) reviewed to block access between the Test LPAR and the Production LPAR on a periodic basis by external reviewers. External reviewers may include FISA resources outside of the team that set up the ACL and resources outside of FISA or external security consultants with mainframe experience. |

| | |
|---|---|
| **Operations Support Process – OPA** | OPA should include a process of transition planning when one of their key staff is on long-term leave to appoint a substitute or backup staff to take over the key responsibilities. The transition process should be institutionalized within OPA. |