OFFICE OF INSPECTOR GENERAL
CITY OF ALBUQUERQUE

INVESTIGATION REPORT
CASE NO. 14-204

Department of Finance and Administration
Water Authority - Fraudulent Payments
Case No. 14-204
Executive Summary

The Office of Inspector General (OIG) conducted an investigation concerning fraudulent payments made to a personal Albuquerque Bernalillo County Water Utility Authority (WA) account by a City employee. The investigation was predicated upon information received by the Internal Audit Director that was forwarded to the OIG.

The OIG was notified that System Analyst II (CE1) who had access to WA's billing software system may have gone into his personal WA account and fraudulently credited the account several times for a total of $6,288.

Upon receiving and reviewing the information, the OIG immediately began an investigation.

METHODOLOGY

- Review of Water Authority documents
- Interviews of appropriate City and WA personnel
- Work with APD on criminal portion

Our investigation was conducted in accordance with fraud investigation techniques, which include-but are not limited to examination of records, documents, interviews with appropriate personnel, and other evidence-gathering procedures as necessary under the circumstances.

OBJECTIVE

- *Is there evidence to support the allegation of fraudulent crediting of account?*

  From February 10, 2011 through February 13, 2014, CE1 credited his WA account 22 times for a total of $6,288.00.

  Additional review was done by the WA, which found another fraudulent transaction in the amount of $150.00.

- *Were other accounts credited?*

  The OIG did a background check and found another address listing CE1 as the owner. The information was given to the WA where a search on the address was done. The WA found another account under CE1's name that was also fraudulently credited.

  From July 6, 2011 through December 12, 2013 CE1 fraudulently credited his second WA account 16 times for a total of $2,642.21.

Treasury tested their side of CE1's accounts and found an additional payment for $711.66 that was found voided on Treasury's side but was never voided in the WA system.

CE1's 2 WA accounts were fraudulently credited for a total of $9,797.87.

The City computers CE1 used were imaged by the New Mexico Regional Computer forensics Laboratory (NMRCFL). The OIG observed the City's Associate Chief Information Officer search the imaged drives at NMRCFL for any fraudulent activity. To the best of his knowledge, the Associate Chief Information Officer could not find any other fraudulent activity on the imaged hard drives.

- *Are there areas in which Department of Finance & Administrative Services (DFAS) can reduce the risk of fraud?*

RECOMMENDATIONS AND RESPONSES:

The OIG makes the following recommendations for consideration by the Department of Finance & Administrative Services.

- No personal accounts should be used to test any Point of Sale system.

  DFAS RESPONSE:

  "DFAS agrees with the finding. DFAS has ceased using personal accounts for testing Point of Sales systems.

  Timeline: This change has been implemented."

- That the logbook into the Treasury offices be signed by non-Treasury personnel to keep track of who is entering the secure area.

  "DFAS agrees with the finding and requires that the logbook into the Treasury offices be signed by non-Treasury personnel.

  Timeline: This requirement has been implemented."

CONCLUSION:

On Sunday, February 23, 2014, CE1 admitted to the detective assigned to the case that he had posted fraudulent payments to his accounts to keep his water service from being turned off.

CE1 was charged with NMSA 30-16-6E Fraud; *Whoever commits fraud when the value of the property misappropriated or taken is over two thousand five hundred dollars ($2,500) but not more than twenty thousand dollars ($20,000) is guilty of a third degree felony.* The case has been turned over to the District Attorney's office for review and possible prosecution.

Effective March 11, 2014, CE1 resigned his position from the City.

CE1 utilized his position with the City of Albuquerque to fraudulently credit his two WA accounts 38 times in a three-year span.

CE1 has made a payment plan with the WA to pay back a total of $10,703.87 which includes past due amounts, which must be paid by a certain time. If a payment is missed, CE1's water will be shut off until full payment is received.

CITY OF ALBUQUERQUE

Office of Inspector General

P.O. BOX 1293, ALBUQUERQUE, NM 87103

June 25, 2014

Accountability in Government Oversight Committee
City of Albuquerque
Albuquerque, New Mexico

Investigation: Water Authority
Department of Finance and Administration Services
14-204

FINAL

INVESTIGATIVE REPORT

ALLEGATION:

On February 18, 2014, the Office of Inspector General (OIG) was notified that a City employee who had access to the Albuquerque Bernalillo County Water Utility Authority (WA) billing software system may have gone into his personal account and fraudulently credited his account several times for a total of $6,288

The Office of Inspector General immediately began an investigation.

BACKGROUND and EVENTS

Prior to July 1 of 2013, the City's Treasury department collected payments on behalf of the WA. During this time, the City's System Analyst II (CE1), assigned to Treasury, also dealt with the software used to collect payments for the WA. Effective July 1, 2013, the City and the WA created a memorandum of Understanding (MOU) that the financial services the City was providing were now the responsibility of the WA.

On February 18, 2014, the Director for Internal Audit (IA) was contacted by the Chief Financial Officer (CFO) for the WA stating that a City employee may have fraudulently credited his WA account. After speaking with the CFO, the IA came to the OIG's office and reported what she had been told.

After speaking with the IA, the OIG went to speak with the CFO to get additional information. The CFO was not certain CE1 was the person crediting the account, but he was the main person of interest.

After reviewing the information, the OIG ran a comprehensive report on CE1 and found a second address in CE1's name. The address was given to the CFO to see if the account had also been fraudulently credited. The following day the CFO informed the OIG that the account for the second address had also been fraudulently credited.

By confirming that two WA accounts in CE1's name had been fraudulently credited, this made CE1 the main suspect in the fraudulent activity. He had the expertise and password to get into the WA system.

The OIG also did research to find addresses of CE1's family members that had accounts with the WA to check for possible fraudulent activity. No fraudulent activity was found for the names and addresses given to the WA by the OIG. All payments came in through normal channels.

On February 20, 2014, the OIG met with APD personnel to discuss the investigation. During this time, the OIG handed over copies of all the documentation that had been gathered. A detective from APD's White Collar Crimes Unit took over the criminal side of the investigation with assistance from the OIG.

Immediately following the meeting, the OIG and detectives from APD went to the Treasury Division and the office of CE1 to secure the computers used by CE1 for computer imaging by the New Mexico Regional Computer Forensics Laboratory.

On Sunday, February 23, 2014, the Detective assigned to the case interviewed CE1. CE1 admitted to posting payments to his accounts to keep his water services from being turned off. CE1 stated that he would only post enough money on the accounts to keep his water from being turned off. CE1 knew after a certain amount of time or dollar amount that the water would get turned off until payment was current.

CE1 explained to the detective that he helped put the current WA system in place. While CE1 was working on the system, he was provided an administrative password that allowed access to everything. When the new software had been implemented and the job was done, the password was never changed or taken back.

The detective stated that he forwarded the case to the District Attorney's office for review.

Interviews with ABCWUA Employees

On March 5, 2014, the OIG met with the WA Customer Service Assistant Manager (CSAM) and the Customer Information Systems Administrator (CIS).

Per statements from CSAM and CIS, CE1was not an employee of the WA, the reason CE1 interacted with the WA is because he was IT support for City Treasury, which prior to July 1, 2013 processed payments for the WA. CSAM stated that City Treasury was involved in all processes to include payments, reconciliation and banking relationships. The City would take payments via their Point of Sale (POS) system and reconcile all banking transactions. The City provided all treasury services for WA.

CSAM stated that effective July 1, 2013, the City and the WA created a memorandum of Understanding (MOU) that the financial services that the City was providing were now the responsibility of the WA.

CSAM stated that CE1 maintained the software for City Treasury and their systems. During the time Treasury was collecting payments for the WA, CE1 had access to the WA's system. When the WA converted billing systems, CE1 was on the transition team. He had access to all the training and had intimate knowledge of the billing system. This was necessary to understand how payments came in to the WA system from City Treasury.

The OIG asked how the WA found the fraudulent transactions CE1 had made to his account. CSAM stated that a staff member was going through a list of transactions in an adjustment account looking for something not related to CE1's account and stumbled on to a single transaction for CE1's account. The staff member forwarded the information to the CIS stating that something looked funny and may need to be looked into further. The CIS looked into the system and did a comprehensive review of the data. What made this transaction unusual was the use of "system user"; this is an IT user id that has access to everything. Everyone in the WA, to include CE1 has a unique id to identify the user. CE1 had a user id, but instead used the "system user" id. That is what really stood out about this transaction. CE1 was using an adjustment account to credit his accounts instead of one of the normal channels of receiving payments.

Upon the completion of her initial review, the CIS found several transactions that had fraudulently credited CE1's account for a total of $6,288.00. Additional review was done by the WA, which found another fraudulent transaction in the amount of $150.00. This brought the total amount to $6438.00 in fraudulent transactions.

CSAM stated that she received information from the CFO on a second address belonging to CE1 to look into, and in fact, CE1 had also fraudulently credited that account for $2,642.21.

CSAM stated that when Treasury completed doing its test work into CE1's fraudulent transactions, a payment for $711.66 was found voided on Treasury's side, but it was never voided in the WA system. Treasury stated that during the time of the transaction, the system was the older version and payment voids had to be inputted manually. The $711.66 was added to CE1's second account bringing the total to $3,353.87.

CSAM stated that a total of $9,791.87 was reversed from CE1's accounts. (See Exhibit 1)

Interviews with City Treasury Personnel

On Wednesday, March 5, 2014, the OIG interviewed the City's Treasury Supervisor (TS).

The OIG asked what was Treasury's role regarding the WA. The TS stated that Treasury is the bank for the City. The WA used to be part of the City, Treasury accepts all payments and water was one of them. Treasury essentially worked as their bank, accepted payments and reconciled the bank statements. TS stated that the WA did separate about three years ago, but the City still collected payments on its behalf up until July 1, 2013 when the WA started taking its own payments.

OIG asked what CE1 did for Treasury. The TS stated the CE1was the Information Technology Services Division (ITSD) contact assigned to Treasury to help with any technical issues. CE1would come if there were any issues with the POS system, troubleshooting it, making sure Treasury was up and running to assist customers. Treasury was also updating its POS system.

The OIG asked if any of Treasury employees interacted with CE1 during his testing of the WA system. The TS stated that if a system would go down, that CE1 would come down and fix the problem. To ensure everything was up and running before he left, CE1would give the cashier his WA account number and pay one dollar with his credit card. Sometimes they would post and other times he would ask that the transaction be voided. The TS stated there are 70 different payment types and that was the easiest way to make sure the system was up and running. The question was asked if this was a standard procedure. The TS stated that after these events, things have changed.

The OIG asked if CE1 had access the WA system other than in Treasury. The TS stated she assumed so; CE1 had assisted with the implementation of one of the WA systems.

The OIG asked if CE1 had access to Treasury accounts where CE1 could commit fraudulent activity. The TS stated no, that there is a lot security within treasury and separation of duties.

Entrance to Treasury is secure; the OIG asked if Treasury kept a sign in log that would indicate when people, especially CE1, would enter Treasury. The TS stated that they do not have a sign in log at that time.

The OIG asked if Treasury had done any review to see if any other accounts had been accessed by CE1. The TS stated that they looked into the two addresses provided and verified that the payments shown on the POS had documentation and a payment coupon. The TS stated they were able to verify and match all payments in the POS system except for one payment of $711.66. The $711.66 payment was made by credit card, which was then voided on the Treasury side by the cashier. A second void was supposed to have been done in the WA system by a Treasury Accountant II, but never was. TS stated that during the time of the transaction, the system was the older version and payment void had to be inputted manually. TS contacted the WA's, CSAM

and informed her that CE1's account was credited for $711.67 but that it should have been voided on the WA's system. TS's understanding is that the CSAM is going to add $711.67 to the total CE1 owes.

On Thursday, March 6, and Friday, March 7 2014, the OIG interviewed two Finance Technicians from Treasury.

The OIG interviewed Finance Technicians, FT1 and FT2, to see if they had any contact with CE1 during his time at Treasury. FT1 stated that generally CE1 was there daily. FT1 would aid in testing the scan lines on the bills to make sure they read properly. FT1 stated that CE1 would do testing of the computer systems on the computer behind the main office cashier.

FT2 was asked if she had any dealing with CE1. FT2 stated that CE1 was the "go to" person for any computer issues. FT2 also did testing for the WA. FT2 stated that CE1 would use his own account number, test the system using his debit card, and make a payment, like a dollar. They would process that type of payment. FT2 stated she would enter the information into CE1's water account, not CE1. FT2 said CE1 would just pay a dollar. FT2 stated there was a test computer that CE1 would use. FT2 stated she would see CE1 on that computer at least 3 times a week. FT2 stated that the one account belonging to CE1 was only used.

Update

Since the investigation, CE1 has met with the WA and has agreed to pay back $9,791.87 along with penalty fees and past due amounts. The total is $10,703.87. According to the WA agreement, CE1 paid 25% and will pay the remaining amount due in monthly installments. If CE1 misses a payment, his water services will be shut off.

Effective March 11, 2014, CE1 resigned his position from the City.

EXHIBIT 1

UNAUTHORIZED FRAUDULENT PAYMENTS

Account 1			Account 2		
2/13/2014	$	250.00	12/12/2013	$	175.00
12/11/2013	$	225.00	9/25/2013	$	300.00
10/16/2013	$	350.00	7/17/2013	$	100.00
9/25/2013	$	275.00	5/16/2013	$	150.00
5/15/2013	$	200.00	2/27/2013	$	195.00
4/8/2013	$	175.00	1/14/2013	$	60.00
3/14/2013	$	250.00	12/31/2012	$	150.00
1/11/2013	$	140.00	11/14/2012	$	125.00
12/20/2012	$	225.00	9/27/2012	$	190.00
11/13/2012	$	310.00	8/15/2012	$	72.00
10/1/2012	$	200.00	6/15/2012	$	150.00
8/7/2012	$	145.00	4/19/2012	$	232.21
6/15/2012	$	140.00	1/30/2012	$	125.00
5/16/2012	$	150.00	12/6/2011	$	120.00
4/19/2012	$	244.00	11/10/2011	$	293.00
3/15/2012	$	325.00	7/6/2011	$	205.00
12/15/2011	$	160.00			
11/9/2011	$	493.00			
9/29/2011	$	425.00			
5/26/2011	$	456.00			
4/20/2011	$	350.00			
2/10/2011	$	800.00			
	$	**6,288.00**		**$**	**2,642.21**

ADDITIONAL FRAUDULENT TRANSACTIONS

7/5/2013	**$**	**150.00**	11/29/2010	**$**	**711.66**
Total per Account	**$**	**6,438.00**		**$**	**3,353.87**
TOTAL				**$**	**9,791.87**

REVIEWED BY:

_____	_____
Acting IG	IG Investigator
APPROVED:	APPROVED FOR PUBLICATION**:**
_____	_____
Peter J. Pacheco, CFE, CIGI Acting IG, Office of Inspector General	Chairperson, Accountability in Government Government Oversight