INTERNAL AUDIT
IAS
ADVISORY SERVICES

Internal Audit Report

ANALYTICAL FRAUD REVIEW

Report No. SC-13-12
September 2012

David Lane
Assistant Director
Principal Auditor

Approved
Barry Long, Director
Internal Audit & Advisory Services

UC SANTA CRUZ

Table of Contents

I. EXECUTIVE SUMMARY

Internal Audit & Advisory Services (IAS) has completed an Analytical Fraud Review audit to determine if data from the campus payroll system (PPS), Financial Information System (FIS) and eProcurement system (CruzBuy) included significant errors, irregularities, or common indicators of fraud, which would warrant further review.

Overall, we noted some interrelated data sets between campus financial systems requiring further review and management resolution, but we did not detect any instances indicating fraud or misappropriation. Controls over the payroll and accounts payable processes we tested, which would help prevent fraud from occurring, appear to be effective.

It should be noted that most cases, fraud is detected as the result of a whistleblower type complaint or referral. While a pro-active data review, as performed, cannot possibly detect all inappropriate transactions, it can be a deterrent to those that might consider committing fraud and it was useful to identify the data set inconsistencies for management resolution as outlined in Appendix A, and below.

The following issues requiring management corrective action were identified during the review:

A. Duplicate Vendor Accounts in FIS
Controls to prevent or detect duplicate vendor accounts in the Financial Information System (FIS) did not always prevent duplicate accounts from being created. We identified 23 duplicate accounts in FIS and 370 accounts that appear to be duplicates but require further review.

B. Outdated Bank Accounts in PPS
The bank account numbers for 406 employees, expected to be the same in PPS and FIS, did not match. These account numbers in PPS were outdated because the employees did not update their account information when the credit union announced in 2006 that account numbers were changing.

In addition, one local credit union reported that a student organization had established a bank account using the university's taxpayer identification number, which is not allowed under UC policy. We informed the campus Financial Accounting and Reporting (FAR) office, who indicated they would be working with that student organization to close this account.

Management agreed to or is already implementing corrective actions to address risks identified in these areas. Observations and related management corrective actions are described in greater detail in section III of this report.

II. INTRODUCTION

Purpose

To determine if data from the campus payroll system (PPS), Financial Information System (FIS) and eProcurement system (CruzBuy) included significant errors, irregularities, or common indicators of fraud which would warrant further review.

Background

The university employs a fraud prevention and detection strategy that relies on prevention through design and implementation of effective internal controls, reviews and advice from Internal Audit, and reporting through the whistleblower program and hotline. The Institute of Internal Auditors (IIA) defines fraud as:

> *Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.*

The Campus Controllers' Office develops, implements, and maintains a comprehensive and cost-effective system of internal control for the UCSC campus. These controls are designed to prevent and/or detect fraudulent activities.

The university has implemented a Whistleblower Policy on reporting and investigating allegations of suspected improper governmental activities. This policy governs the reporting and investigating of allegations of suspected improper governmental activities.

The chancellor delegates to the local designated official (LDO) the authority for coordinating and implementing the Whistleblower Policy. The chancellor has also appointed an Investigations Workgroup (I-group) to provide advice to the LDO regarding oversight and coordination of investigative activities. The LDO acts as the chair of the I-group and when they suspect improper governmental activities have occurred; they may direct the appropriate office to conduct an investigation.

This review was undertaken in an effort to pro-actively identify fraud or situations that could lead to fraud when no specific allegations of improper government activities have been made.

Scope

Key relationships between financial data sets and associated campus financial systems where the data resided was identified and data was selected and analyzed from fiscal year 2012, and in some cases, fiscal years all the way back to 1996.

The review included, but was not limited to the following areas:

- Financial Information System (FIS) vendor addresses were reviewed to determine if more than one vendor was using the same mailing address. If payments were found, further steps were taken to determine disposition.
- Employee addresses from the Payroll system were compared with vendor addresses in FIS. For all matches with business accounts in FIS, payments were reviewed to determine disposition.
- Payments to any FIS vendor using a mail box as their business address were reviewed.
- Automated clearing house (ACH) bank accounts for all FIS vendors were reviewed to determine if more than one vendor used the same bank account. For vendor bank account matches, payments were reviewed to determine disposition.
- Payroll system direct deposit bank accounts were compared to FIS ACH payment bank accounts to determine if any FIS vendor payments were deposited into employee bank accounts. Matches were reviewed to determine disposition.
- FIS vendor accounts were reviewed to determine if vendors have multiple accounts. Matched payments were reviewed to determine disposition.
- Purchases with non-UCSC ship-to addresses were reviewed to determine if goods were subject to conversion for personal use.
- Local banks were surveyed to determine the existence of unapproved bank accounts using the University name or tax ID number.
- Deposits to non-revenue (expense) accounts were reviewed to determine the existence of unknown and/or misclassified revenue streams.

Due to the extensive range of financial activities and the vast volume of financial data, not all identifiable activities were reviewed. Accordingly, audit procedures were not designed and could not be expected to detect all errors and irregularities, especially minor or isolated incidents.

III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

A.	Duplicate Vendor Accounts in FIS	
Controls to prevent or detect duplicate vendor accounts in the Financial Information System (FIS) did not always prevent duplicate accounts from being created. We identified 23 duplicate accounts in FIS and 370 accounts that appeared to be duplicates but that require further review.		
Risk Statement/Effect		
When duplicate vendor accounts exist, those vendors have an inaccurate and incomplete payment history; the likelihood of duplicate payments increases and taxable payments may be reported to the employee and IRS inaccurately.		
Agreements		
A.1	Financial Accounting and Reporting will review a list of existing vendor accounts where duplicates and potential duplicates have been identified, and will eliminate the actual duplicates.	Implementation Date 12/21/2012 Responsible Manager General Accounting Manager
A.2	Financial Accounting and Reporting will assure all staff who modify or create vendor accounts are following documented procedures to check for existing vendor accounts before creating new ones and are using the word "void" consistently when deactivating vendor accounts.	Implementation Date 12/21/2012 Responsible Manager General Accounting Manager
A.3	Financial Accounting and Reporting will check for and eliminate duplicate FIS vendor accounts on a periodic basis.	Implementation Date 4/1/2013 Responsible Manager General Accounting Manager

A. Duplicate Vendor Accounts in FIS - Detailed Discussions

We electronically scanned and analytically reviewed 42,575 vendors that had been set up in the FIS Banner database since the system was implemented in 1995. At least 23 vendors had more than one account in FIS, and potentially up to 370 additional vendors had between two and four accounts. We provided the list of potential duplicate vendor accounts to the FAR for their review for duplicate

vendor accounts. Since social security numbers are not entered for all FIS vendors, we were not able to efficiently determine the number of duplicate accounts. FAR staff has experience with the vendor data set and are in a better position to determine which vendors were duplicates, and required closing.

Also, some business vendors have an agency account created by the Extra Mural Funds Accounting Office to track grant activity in addition to their normal vendor account used to make payments. However, the agency accounts are a small percentage of the overall duplicate accounts and require no corrective action.

We also noted that at least 17 vendors were voided in ways that were inconsistent with campus procedures. When FIS vendors need to be voided, the procedure calls for the word "VOID" to be typed in the beginning of the last name data field as a marker to alert FIS users not to make payments to that vendor. As a rule, vendor accounts cannot be deactivated because the vendor history would be lost. In these 17 instances, the word "VOID" was typed in one of the address fields instead, which makes it more difficult to recognize voided vendors and run reports listing them

The procedures to create new vendor accounts in FIS included steps that should have been sufficient to prevent duplicate accounts from being created; however, over the past 17 years (since FIS Banner was implemented in 1995) these duplicate accounts have been created. One reason cited by FAR is the lack of consistent use of social security numbers that provide positive identification. The director of Financial Administrative Services and Transactions noted that the inconsistent placement of the word "VOID" had started since the person who was historically responsible for vendor database maintenance retired in December 2011. Additional training and oversight may be required for the staff who has taken over these duties.

We reviewed all payments to the vendors who we were sure had multiple accounts and did not identify any payments that appeared questionable. When vendors have multiple accounts, a potential problem exists in that tax reportable payments requiring 1099 reporting may not be accurately tracked and IRS tax reporting may be inaccurate. We did not observe the "splitting" of payments that could be done that would violate IRS tax reporting requirements.

B.	Outdated Bank Accounts in PPS

The bank account numbers for 406 employees, expected to be the same in PPS and FIS, did not match. These account numbers in PPS were outdated because the employees did not update their account information when the credit union announced in 2006 that account numbers were changing.

Risk Statement/Effect

If account numbers are outdated in PPS, automated deposits could be made to an employee's saving account instead of their checking account. While not a direct risk to the University, the inconvenience and disruption that would be caused to employees could impact the workload of payroll staff who would be responding to an inflow of complaints.

Agreements

B.1	The Payroll Office will work with the credit union and/or employees to update direct deposit bank account information determined to be outdated.	Implementation Date 6/30/2013 Responsible Manager Payroll Operations Manager

B. Outdated Bank Accounts in PPS - Detailed Discussion

In our comparison of bank account numbers between PPS and FIS, we noted that a number of employee accounts were different in these two systems. This did not make sense as the accounts all had the same routing number indicating the employees banked at the same local credit union. We contacted the credit union and were told that the account numbers starting with a specific numeric sequence were old account numbers that had been in use prior to 2006.

Fortunately, the account numbers included the employees' member ID with this credit union, so deposits were being properly routed into one of their accounts, but the credit union could not assure that the deposits would go into the checking accounts vs. the savings, or into other accounts that the employee might have with the credit union.

As none of these employees had reported problems with their deposits, it is likely that someone at the credit union has been manually or otherwise assuring the deposits went to the proper accounts. Although no problems have been identified to date, there is no guarantee that these deposits would not become problematic over time. We notified the Payroll Office of this condition and they began working with the credit union and/or the employees to get the account information updated.

***

APPENDIX A – Summary of Work Performed and Results

Work Performed	Results
1. FIS vendor addresses were reviewed to determine if more than one vendor was using the same mailing address. If found, payments were reviewed to determine disposition.	We identified a large number of address matches, but most were individuals who appeared to be couples or roommates. We selected a judgment sample of vendors that appeared to be companies who had the same addresses and reviewed all payments made to them in FY2012. We did not find any payments that appeared questionable, duplicate, or that warranted further review.
2. Employee addresses from payroll system were compared with vendor addresses in FIS. For all matches with business accounts in FIS payments were reviewed to determine disposition.	A large percentage of employees also have FIS vendor accounts in their name to receive travel and other reimbursements. We specifically looked for vendors that appeared to be businesses that had the same addresses as employees. We did not find any matches in this search.
3. Payments to any FIS vendors using a mail box as their business address were reviewed.	We compiled a list of the addresses of all mail box providers from the AT&T Yellow Pages and ran a query to identify FIS vendors who were using these addresses as their business address. We produced and reviewed a report of all payments in FY2012 to these vendors. No unusual or suspicious payments were identified.
4. ACH bank accounts for all FIS vendors were reviewed to determine if more than one vendor uses the same bank account. For matches payments were reviewed to determine disposition.	We identified a substantial number of vendors with shared bank accounts, but most appeared to be couples or other individuals who used the same bank account. We focused on vendors that appeared to be businesses that had the same back accounts. Using a judgment sample and by reviewing the websites of these businesses, we found that many were subsidiaries or had other business relationships to explain the shared bank account. We performed a detailed review of all payments to the sample of businesses in FY2012 and did not find any duplicate or otherwise unusual payments.
5. Payroll system direct deposit bank accounts were compared to FIS ACH payment bank accounts to determine if any FIS vendor payments were deposited into employee bank accounts. Matches were reviewed to determine their disposition.	We again found that many employees had FIS accounts for reimbursement purposes. In this review we noted that 406 employees' bank accounts did not match when they were expected to do so. Refer to Observation Section III. B – Outdated Bank Accounts in PPS. We did not find any vendors who appear to be businesses using employee back accounts.

Work Performed	Results
6. FIS vendor accounts were reviewed to determine if vendors have multiple accounts. For matches payments were reviewed to determine disposition.	We identified 23 instances where the vendor had more than one FIS account with the same name and social security number. We also found 370 instances where there were between two and four vendor accounts with the same first, middle and last names but with social security numbers missing from one or more of the accounts. This issue is discussed in detail in Observation Section III. A – Duplicate Vendor Accounts in PPS.
7. Purchases with non-UCSC ship to addresses were reviewed to determine is goods were subject to conversion.	We reviewed all FY2012 CruzBuy purchase order transactions with special instructions - instructing the supplier to ship goods to a non-standard address. Most of these purchase orders indicated shipment was to other universities or to properties, such as UARC who is affiliated with the campus but not on site at the UCSC campus. We focused our review on orders shipped to residential addresses. None the items shipped to these addresses could be easily converted to cash or personal use. For example one order was for a set of thermocouples valued at $400 each. We reviewed these purchases with the research accountants in the divisions where the purchase orders originated and received assurance that the special shipping instructions made sense and were not out of the ordinary. Detailed testing to verify receipt of thermocouples and other items was not performed.
8. Local banks were surveyed to determine if unapproved bank accounts using the name or tax ID of the university exist.	We worked with the Controllers' Office to survey 19 local banks to determine if they had accounts in name of the UC Regents, UCSC or using the universities tax ID number. In addition, one local credit union reported that a student organization had established a bank account using the university's taxpayer identification number, which is not allowed under UC policy. We informed the campus Financial Accounting and Reporting (FAR) office, who indicated they would be working with that student organization to close this account.
9. Deposits to non-revenue (expense) accounts were reviewed to determine if unknown and misclassified revenue streams exist.	We ran a report of all deposits made to expense accounts (contra expense transactions) for FY2012 that included 2,275 transactions. The vast majority was to clearing accounts (AIS transactions), agency accounts (Conference Services), or was to record direct cost recovery (housing billing for utilities). Of the transactions that we could not explain, we selected 11 over $10,000 for detailed review. Three of the 11 should have been recorded as revenue. Since the dollar amounts involved did not justify reopening the books for a closed fiscal year we educated the departments and divisions how the deposits should have been made and General Accounting agreed to follow-up to assure future deposits related to these events were recorded to revenue.