AUDIT REPORT

Department of Financial Institutions

March 2009

STATE OF TENNESSEE

COMPTROLLER OF THE TREASURY

Department of Audit

Division of State Audit

TENNESSEE COMPTROLLER OF THE TREASURY

Arthur A. Hayes, Jr., CPA, JD, CFE
Director

Kandi B. Thomas, CPA, CFE
Assistant Director

Ronald E. Anderson, CPA, CFE
Aaron Jewell, CPA, CFE
Audit Manager

Herb Kraycirik, CPA
In-Charge Auditor

Valeria Stadelman
Tiffany Tanner
Staff Auditors

Amy Brack
Editor

Comptroller of the Treasury, Division of State Audit
1500 James K. Polk Building, Nashville, TN 37243-1402
(615) 401-7897

Financial/compliance audits of state departments and agencies are available on-line at www.comptroller1.state.tn.us/RA_SA/.
For more information about the Comptroller of the Treasury, please visit our website at www.tn.gov/comptroller/.

STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY
DEPARTMENT OF AUDIT
DIVISION OF STATE AUDIT
SUITE 1500
JAMES K. POLK STATE OFFICE BUILDING
NASHVILLE, TENNESSEE 37243-1402
PHONE (615) 401-7897
FAX (615) 532-2765

March 5, 2009

The Honorable Phil Bredesen, Governor
and
Members of the General Assembly
State Capitol
Nashville, Tennessee 37243
and
The Honorable Greg Gonzales, Commissioner
Department of Financial Institutions
10th Floor, Bank of America Building
414 Union Street
Nashville, Tennessee 37243

Ladies and Gentlemen:

We have conducted a financial and compliance audit of selected programs and activities of the Department of Financial Institutions for the period March 1, 2005, through July 31, 2008.

We conducted our audit in accordance with generally accepted government auditing standards. These standards require that we obtain an understanding of internal control significant to the audit objectives and that we design the audit to provide reasonable assurance of the Department of Financial Institutions' compliance with laws and regulations significant to the audit objectives. Management of the Department of Financial Institutions is responsible for establishing and maintaining effective internal control and for complying with applicable laws and regulations.

Our audit disclosed a finding which is detailed in the Objectives, Methodologies, and Conclusions section of this report. The department's management has responded to the audit finding; we have included the response following the finding. We will follow up the audit to examine the application of the procedures instituted because of the audit finding.

We have reported other less significant matters involving the department's internal control and instances of noncompliance to the Department of Financial Institution's management in a separate letter.

Sincerely,

Arthur A. Hayes, Jr., CPA
Director

AAH/cj
08/070

State of Tennessee

Audit Highlights

Comptroller of the Treasury Division of State Audit

Financial and Compliance Audit
Department of Financial Institutions
March 2009

———

AUDIT SCOPE

We have audited the Department of Financial Institutions for the period March 1, 2005, through July 31, 2008. Our audit scope included a review of internal control and compliance with laws and regulations in the areas of travel, cash receipts and receivables, Regulatory Business System security, payroll supplementals and differentials, mortgage lender exam reviews, and the Financial Integrity Act. The audit was conducted in accordance with generally accepted government auditing standards.

AUDIT FINDING

The IT Director Did Not Adequately Restrict Regulatory Business System Access to Effectively Mitigate Risks of Improper Access and Fraud

Seventy of 74 employees with access (95%) either did not need access or had more access than required for their respective job duties.

Financial and Compliance Audit
Department of Financial Institutions

TABLE OF CONTENTS

Financial and Compliance Audit
Department of Financial Institutions

INTRODUCTION

POST-AUDIT AUTHORITY

This is the report on the financial and compliance audit of the Department of Financial Institutions. The audit was conducted pursuant to Section 4-3-304, *Tennessee Code Annotated*, which requires the Department of Audit to "perform currently a post-audit of all accounts and other financial records of the state government, and of any department, institution, office, or agency thereof in accordance with generally accepted auditing standards and in accordance with such procedures as may be established by the comptroller."

Section 8-4-109, *Tennessee Code Annotated*, authorizes the Comptroller of the Treasury to audit any books and records of any governmental entity that handles public funds when the Comptroller considers an audit to be necessary or appropriate.

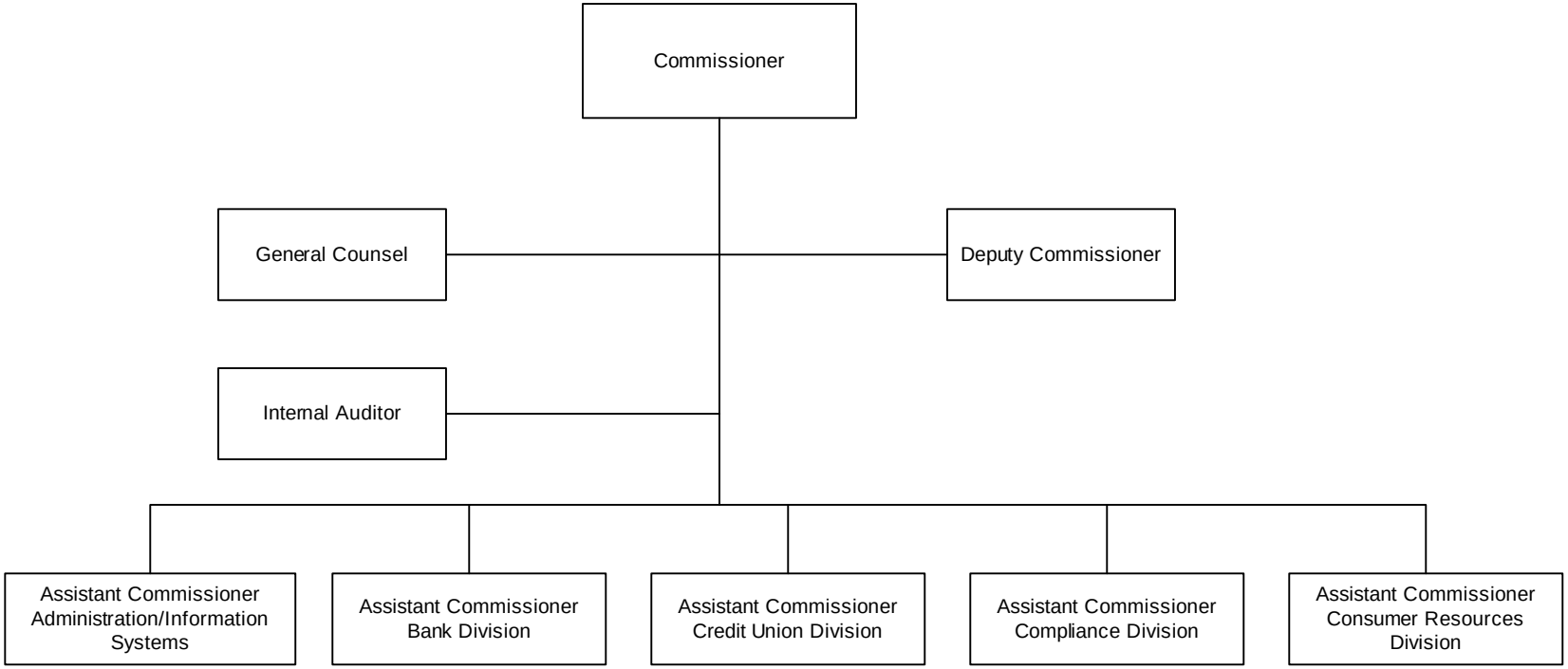
BACKGROUND

The primary mission of the Department of Financial Institutions is to provide the citizens of Tennessee with a sound system of state-chartered and licensed financial institutions. The Bank Division is responsible for the regulation and supervision of state-chartered financial institutions such as state-chartered banks, savings banks, saving and loan associations, credit card banks, nondepository trust companies, money transmitters, and business and industrial development corporations (BIDCOs). The Credit Union Division is responsible for the regulation and supervision of state-chartered credit unions. The Compliance Division is responsible for regulatory oversight of industrial loan and thrift companies; insurance premium finance companies; residential mortgage servicing, lending, and brokering; car title pledge lending; check cashing; and deferred presentment companies. The Consumer Resources Division is responsible for tracking and resolving consumer complaints, helping to inform citizens of their financial rights, and increasing the effectiveness of existing financial literacy programs.

The Department of Financial Institutions encourages the development of depository financial institutions while restricting their activities to the extent necessary to safeguard the interests of depositors. The department also works to ensure that both depository and nondepository financial institutions comply with governing laws and regulations.

An organization chart of the department is on the following page.

Department of Financial Institutions
Organizational Chart



AUDIT SCOPE

We have audited the Department of Financial Institutions for the period March 1, 2005, through July 31, 2008. Our audit scope included a review of internal control and compliance with laws and regulations in the areas of travel, cash receipts and receivables, Regulatory Business System security, payroll supplementals and differentials, mortgage lender exam reviews, and the Financial Integrity Act. The audit was conducted in accordance with generally accepted government auditing standards.

PRIOR AUDIT FINDINGS

There were no findings in the prior audit report.

OBJECTIVES, METHODOLOGIES, AND CONCLUSIONS

TRAVEL

Our objectives in reviewing travel were to determine if

- travel related expenditures were in compliance with the state's comprehensive travel policies, and
- travel advances complied with the state's comprehensive travel policies.

We interviewed key department personnel and reviewed applicable policies and regulations to gain an understanding of the procedures used to ensure that the department complied with the state's travel policies. We obtained a listing of all of the department's expenditures charged to travel in the State of Tennessee Accounting and Reporting System (STARS) during the period March 1, 2005, through February 29, 2008. We tested a total of 26 travel claims, consisting of the following: the two largest corporate travel card billings, the largest air travel card billing, the largest direct billing, the largest travel claims from the current and former commissioners, the largest travel claim from the employee with the most travel, the largest travel claims in 2007 from 13 Bank Division employees, and 6 additional claims at random.

In addition to testing each item for compliance with the state's comprehensive travel policies, we also determined if the employee was on leave during the claim period. For employees traveling with other employees, we reviewed the other employees' travel claims to

determine if mileage was claimed by two or more employees who rode together. We examined the supporting documentation for all travel advances to determine compliance with the state's travel policy criteria for awarding travel advances, and that the amounts of the advances were in compliance with state policy.

As a result of the above testwork, we concluded that

- travel related expenditures were in compliance with the state's comprehensive travel policies, and
- travel advances complied with the state's comprehensive travel policies.

CASH RECEIPTS AND RECEIVABLES

Our objectives in reviewing cash receipts and receivables were to determine if

- transactions made to the Regulatory Business System (RBS) reconciled to the daily deposits,
- outstanding receivables were properly calculated and the efforts made to collect them were in compliance with the department's procedures,
- management has a process to reconcile licenses issued to fees received,
- refunds were properly documented and calculated, and
- bank fee and credit union fee receipts not recorded in RBS could be reconciled with daily deposits.

We interviewed management to gain an understanding of the controls in place which ensure that established procedures were followed. Management gave us view-only access to RBS and an electronic file containing all RBS activity from July 1, 2006, through April 30, 2008. We randomly selected a sample of 25 transactions in proportion to the RBS activity of each profession. We reconciled these transactions to their respective daily deposits. We also haphazardly selected 17 receivables as of March 31, 2008, from RBS. We determined if the receivables were properly calculated and if collection efforts were in compliance with the department's procedures. To determine if management has a process to reconcile licenses issued to fees received, we interviewed key staff and reviewed documentation to gain an understanding of management's process to reconcile licenses issued to fees received.

We also tested the 25 largest refunds recorded in the State of Tennessee Accounting and Reporting System plus one selected at random with an effective date from March 1, 2005, through February 28, 2008, to determine if the refunds were properly documented and calculated. For the receipts not recorded in RBS, we randomly selected a sample of 25 bank fee receipts from April 24, 2006, through April 30, 2008; and 25 credit union fee receipts from July 1, 2007, through April 30, 2008, to determine if the receipts reconciled to the daily deposits.

As a result of the above testwork, we concluded that

- transactions made to RBS reconciled to the daily deposits,
- outstanding receivables were properly calculated and the efforts made to collect them were in compliance with the department's procedures,
- management has a process to reconcile licenses issued to fees received,
- refunds were properly documented and calculated, and
- bank fee and credit union fee receipts not recorded in RBS could be reconciled with daily deposits.

REGULATORY BUSINESS SYSTEM (RBS) SECURITY

Our objectives in reviewing RBS security were to determine if

- sensitive information within RBS was adequately protected from unauthorized access, and
- access to RBS was limited to only those persons whose job duties require it.

We interviewed management to gain an understanding of the controls in place to determine if sensitive information within RBS was adequately protected from unauthorized access. We obtained from management a list of persons with access to RBS at May 16, 2008, and determined if the level of access for each person on the list was appropriate, considering the person's job duties. As a result of this, we concluded that

- sensitive information within RBS was not adequately protected from unauthorized access, and
- access to RBS was not limited to only those persons whose job duties require it.

This is discussed further in the finding below.

The IT Director did not adequately restrict Regulatory Business System access to effectively mitigate risks of improper access and fraud

Finding

The IT Director for the Department of Financial Institutions did not adequately restrict Regulatory Business System (RBS) access to effectively mitigate risks of improper access and fraud. The department's Compliance Division uses RBS to store key information about the businesses it regulates, to record fees received from these businesses, and to issue licenses.

Based on our review and discussions with the Assistant Commissioner of the Compliance Division, the IT Director, the Fiscal Director, the Information Systems Consultant, and the Loan Examiner Directors, we found policy and procedural weaknesses within the department that increased the risks associated with improper system access and unauthorized system activity. Specifically, we found the following:

- The IT Director did not have written policies related to revoking, changing, reviewing, or granting access levels for RBS users and as a result did not know which users had what access. Consequently, during fieldwork and in response to the auditors' request, the Information Systems Consultant developed a report to identify current users and current access levels.

- The department's Human Resource Director had not designed the separation checklist to include a list of all computer application access that an employee has. Such a list would help ensure that access is revoked as of the last day at work.

We specifically reviewed all employees' access and found that, of the 74 employees with system access and edit capabilities, 63 had more access than required for their respective job duties, and another 7 employees did not need any access. Two of the 63 employees had unlimited access. The failure to adequately control system access increases the risk of accidental or intentional improper license issuance as well as the risk of unauthorized changes to business information stored in RBS.

In addition, we found weaknesses in the IT Director's process to assign usernames. Although all departmental employees that function in regulatory roles have unique usernames and passwords, the System Administrator and his staff all utilize the same username and password for administration and maintenance of the RBS system. The system is designed so that the audit trail only identifies data changes by username. Therefore, unless the usernames are also unique, it is not possible to identify the employee who makes a change. Furthermore, the system does not automatically generate a report or otherwise alert the administrator when data changes occur. Without automatic reports or alerts of changes, unauthorized changes or other errors could occur and go undetected.

As a result of our inquiries about access to RBS, the Director of Information Technology immediately requested that the Information Systems Consultant begin a comprehensive reevaluation of each employee's access to the system. By the end of June 2008, management had completed its evaluation and reduced employee access to levels appropriate for each employee. However, the System Administrator and his staff continue to utilize the same username and password for access to the RBS system. In spite of these improvements, management still believes that RBS needs to be replaced.

Recommendation

In order to ensure that the department continues to limit employee access to the system based on each individual's job duties and responsibilities, the System Administrator should develop written policies for revoking and changing access levels. Supervisory staff should limit requests for employee system access and edit capabilities to the minimum required for each employee's individual job duties. The System Administrator should review and approve each request to ensure that access and edit capabilities do not exceed the employee's needs. When employees' job duties change, system access and edit capabilities should be reviewed and modified accordingly. As an additional control, the System Administrator should periodically prepare a list of each employee's RBS access capabilities and review the list with the rest of management.

In order to ensure accountability for changes, the System Administrator should require that each employee accessing RBS have a unique username and password. Furthermore, since the system does not automatically report changes and edits, the System Administrator should periodically extract reports of changes and other edits and determine if the changes were appropriate. Any unusual or unapproved changes should be brought to the internal auditor's and management's attention immediately.

Management's Comment

We concur with the audit finding and have made changes to correct the noted areas where issues have been identified. Those changes are summarized below. Before noting the corrective actions taken the Department would like to state that the current Director of Information Technology began his employment with the Department in late 2007 and had only been in the position for a few months when this audit commenced. In addition, the Regulatory Board System (RBS) is an application that the Department has been working with OIR to replace for several years. The project to replace this technology (the Multi-Agency Regulatory System or better known as MARS) has since ended unsuccessfully. Therefore the Department has purchased an application from the State of North Carolina which will be modified and implemented as a replacement for the RBS system. The Department plans to implement this change in late 2009 or early 2010.

The audit finding is broken into two categories, Systems Access and Unique Usernames. Therefore, we will respond with regard to each category.

Systems Access

The Department has adopted a Computer Security Access Policy that addresses all computer related security needs (including RBS). In accordance with the Policy, a "Security Request Form" must be completed in full and signed by the Division head and the IT Director any time an employee is hired or changes positions or responsibilities. The System Administrator reviews and signs the RBS section of the form prior to setting up the access and checks for anything that may be requested but not needed for that individual's job responsibilities. These forms are kept on file to ensure that the Department maintains a complete inventory of all systems access related to each employee. This inventory is maintained by the IT Group. The Human Resources Director has implemented a separation checklist which includes an action to notify Information Systems to have all employee security access terminated. The only exception is in regard to Edison access which is tracked separately on the separation checklist.

The Computer Security Access Policy also states, "The Department's IT Director will initiate a review on an annual basis that will require each division to validate or adjust the level of security each of their employees has based on their current job responsibilities."

Unique Usernames

The RBS System Administrator has set up unique usernames and passwords for all users including technical administrative users. There is however an exception to this due to the design of the system. There are some features that can only be changed using a generic "VMS" username. This is part of the system design. With the noted plans to retire RBS in the near future, it is not practical to undertake the application re-design which would be needed to fully eliminate the generic support username. However, unique usernames and passwords for all users will be accomplished as we migrate to the new system.

PAYROLL SUPPLEMENTALS AND DIFFERENTIALS

Payroll supplementals are salary payments made to employees that could not be incorporated into the regular salary payment made at the end of each pay period. The types of supplementals include longevity pay, payments for accrued leave after a person has left employment with the state, the first salary payment after a person is hired, and salary adjustments for retroactive raises. Differentials are additional amounts added to an employee's normal salary because the requirements of the job are greater than what is normally required of a particular job classification.

Our objectives in reviewing payroll supplementals and differentials were to determine if

- payroll supplementals were approved by someone other than the preparer of the request and complied with applicable rules and regulations, and
- payroll differentials were approved by someone other than the preparer of the request and the circumstances which required the differential still exist.

We interviewed management to gain an understanding of the controls over payroll supplementals and differentials. We obtained from the State Audit Information Systems Section a listing of all payroll supplementals with an effective date from March 1, 2005, through March 15, 2008. We tested a total of 25 payroll supplementals, consisting of the following items: one from the former Commissioner, one from the current Commissioner, one from the Fiscal Director, the largest payment from each of the five types of payroll supplementals, and 17 additional supplementals at random. We determined if each payroll supplemental was approved by someone other than the preparer and was in compliance with applicable rules and regulations.

We obtained from management a current list of all employees who were receiving a payroll differential and the amount of the differential. We then determined if each was properly approved and the circumstances which required the differential still existed. As a result of our testing, we concluded that

- payroll supplementals were properly approved and were in compliance with applicable rules and regulations, and
- payroll differentials were properly approved and the circumstances which required the differential still exist.

MORTGAGE LENDER EXAM REVIEWS

Our objectives in reviewing mortgage lender exam reviews were to determine if

- exam reviews were performed in compliance with written procedures,
- management reviews of the exams were documented,
- lenders with complaints filed against them were scheduled for an exam review timely, and
- the information in the Regulatory Business System (RBS) on each exam review agreed to the information in the examination files.

We interviewed management to gain an understanding of the controls in place which ensure that established procedures are followed. We obtained a list from management of all active mortgage lenders at May 1, 2008; a list of the examination date for each mortgage lender examined; and a list of complaints received about mortgage lenders. We selected a random sample of 25 mortgage lenders that had received an examination and determined if the

examination was performed in compliance with written procedures and the management review was documented. We then accessed RBS and determined if the information about the exam reviews agreed to the information in the examination files. We obtained from management a list of complaints filed against mortgage lenders since March 1, 2005, and compared that list to the list of lenders that had been examined through June 30, 2008, to determine if lenders with complaints filed against them were scheduled for an exam review timely. As a result of our work, we concluded that

- exam reviews were performed in compliance with written procedures,
- management reviews of the exam reviews were documented,
- lenders with complaints filed against them were scheduled for an exam review timely, and
- the information in RBS on each exam review agreed to the information in the examination files.

FINANCIAL INTEGRITY ACT

Section 9-18-104, *Tennessee Code Annotated,* requires the head of each executive agency to submit a letter acknowledging responsibility for maintaining the internal control system of the agency to the Commissioner of Finance and Administration and the Comptroller of the Treasury by June 30 each year. In addition, the head of each executive agency is required to conduct an evaluation of the agency's internal accounting and administrative control and submit a report by December 31, 1999, and December 31 of every fourth year thereafter.

Our objective was to determine whether the department's June 30, 2007; June 30, 2006; and June 30, 2005, responsibility letters and December 31, 2007, internal accounting and administrative control report were filed in compliance with Section 9-18-104, *Tennessee Code Annotated.*

We reviewed the June 30, 2007; June 30, 2006; and June 30, 2005, responsibility letters and the December 31, 2007, internal accounting and administrative control report to determine whether they had been properly submitted to the Comptroller of the Treasury and the Department of Finance and Administration.

We determined that the Financial Integrity Act responsibility letters and internal accounting and administrative control report were submitted on time in compliance with *Tennessee Code Annotated.*

OBSERVATIONS AND COMMENTS

MANAGEMENT'S RESPONSIBILITY FOR RISK ASSESSMENT

Auditors and management are required to assess the risk of fraud in the operations of the entity. The risk assessment is based on a critical review of operations considering what frauds could be perpetrated in the absence of adequate controls. The auditors' risk assessment is limited to the period during which the audit is conducted and is limited to the transactions that the auditors are able to test during that period. The risk assessment by management is the primary method by which the entity is protected from fraud, waste, and abuse. Since new programs may be established at any time by management or older programs may be discontinued, that assessment is ongoing as part of the daily operations of the entity.

Risks of fraud, waste, and abuse are mitigated by effective internal controls. It is management's responsibility to design, implement, and monitor effective controls in the entity. Although internal and external auditors may include testing of controls as part of their audit procedures, these procedures are not a substitute for the ongoing monitoring required of management. After all, the auditor testing is limited and is usually targeted to test the effectiveness of particular controls. Even if controls appear to be operating effectively during the time of the auditor testing, they may be rendered ineffective the next day by management override or by other circumventions that, if left up to the auditor to detect, will not be noted until the next audit engagement and then only if the auditor tests the same transactions and controls. Furthermore, since staff may be seeking to avoid auditor criticisms, they may comply with the controls during the period that the auditors are on site and revert to ignoring or disregarding the control after the auditors have left the field.

The risk assessments and the actions of management in designing, implementing, and monitoring the controls should be adequately documented to provide an audit trail both for auditors and for management, in the event that there is a change in management or staff, and to maintain a record of areas that are particularly problematic. The assessment and the controls should be reviewed and approved by the head of the entity.

FRAUD CONSIDERATIONS

Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit*, promulgated by the American Institute of Certified Public Accountants requires auditors to specifically assess the risk of material misstatement of an audited entity's financial statements due to fraud. The standard also restates the obvious premise that management, not the auditors, is primarily responsible for preventing and detecting fraud in its own entity. Management's responsibility is fulfilled in part when it takes appropriate steps to assess the risk of fraud within the entity and to implement adequate internal controls to address the results of those risk assessments.

During our audit, we discussed these responsibilities with management and how management might approach meeting them. We also increased the breadth and depth of our inquiries of management and others in the entity as we deemed appropriate. We obtained formal assurances from top management that management had reviewed the entity's policies and procedures to ensure that they are properly designed to prevent and detect fraud and that management had made changes to the policies and procedures where appropriate. Top management further assured us that all staff had been advised to promptly alert management of all allegations of fraud, suspected fraud, or detected fraud and to be totally candid in all communications with the auditors. All levels of management assured us there were no known instances or allegations of fraud that were not disclosed to us.

APPENDIX

ALLOTMENT CODES

336.01 Administration
336.03 Bank Division
336.04 Credit Union Division
336.05 Compliance
336.06 Indirect Cost
336.08 Consumer Resources