Department of Commerce
Consumer Finance Audit

Audit Period: January through December 2017

Results Summary:

Objective	Conclusion
Licensing Process	**Well-Controlled with Improvement Needed**

* Refer to Appendix A for classification of audit objective conclusions.

Report number: 2018-COM-01 **Issuance date: April 19, 2018**

Executive Summary

Background

The Division of Financial Institutions' (DFI) Consumer Finance Section within the Ohio Department of Commerce (COM) is responsible for regulating non-depository consumer finance companies in Ohio. The License Section of Consumer Finance focuses primarily on the issuance and renewal of 12 different license or registration types, as well as letters of exemption. The section oversees over 25,000 active licenses. Entities regulated by the Division include but are not limited to: check cashing services, short-term lenders, mortgage brokers, loan originators, pawnbrokers, and mortgage lenders. License fees are credited to the Consumer Finance Fund and approximately $5.2 million was collected for licenses and fees during 2017.

During the audit, OIA identified opportunities for COM to strengthen internal controls and improve business operations. OIA conforms with the *International Standards for the Professional Practice of Internal Auditing.* OIA would like to thank COM staff and management for their cooperation and time in support of this audit.

This report is solely intended for the information and use of agency management and the State Audit Committee. It is not intended for anyone other than these specified parties.

Scope and Objectives

OIA staff was engaged to perform an assurance audit related to the controls over the agency's Consumer Finance Licensing process for the period of January through December 2017. This work was completed December 2017 through April 2018.

The objective of the review was to evaluate the design and effectiveness of controls over the Consumer Finance Licensing process.

Detailed Observations and Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. Low risk observations were discussed with individual agency management and are not part of this report. However, the low risk observations were considered as part of the audit objective conclusions.

Observation 1 – Lack of CPI Monitoring and Inappropriate System Access

As required by Ohio Revised Code 1347.15 (B), each agency shall create rules regulating access to confidential personal information (CPI). The rules shall include criteria for determining which employees need access to CPI, a list of valid reasons for which employees may access CPI, and references to the federal or state regulations that make the CPI confidential. This revised code section also requires state agencies to notify each person whose CPI has been accessed for an invalid reason by employees of the state agency. Therefore, agencies must perform periodic and timely monitoring of accesses made to CPI and maintain access controls to systems to prevent or detect unauthorized access. Policies must be kept up-to-date to reflect necessary rules or laws. Systems should be designed with robust controls to timely detect potentially unauthorized or inappropriate access to CPI.

A review of the Department of Commerce's (COM) draft Licensing Policy and Procedure Manual noted the following:

- The draft manual does not address periodic reviews of who has accessed CPI in the licensing system (CAVU) or Nationwide Mortgage Licensing System (NMLS).
- The draft manual does not address notifying the Information Technology Group (ITG) of an employee's departure to have the employee's CAVU and NMLS user access terminated.

Currently, the License Supervisor reviews NMLS and CAVU access weekly to ensure user roles and access levels are appropriate; however, evidence is not maintained to support the completion or results of these reviews. OIA reviewed 38 individuals with CAVU access and four individuals with NMLS access to determine if the individuals were current COM employees and still required system access. There were no issues noted with NMLS access; however, nine of the 38 (24%) individuals with CAVU access were no longer employed with COM. OIA worked with ITG to determine the last date these individuals accessed the system and those dates ranged from January 2009 to April 2017, which was consistent with the employees' last dates of employment.

Additionally, CAVU records an audit log of users' changes to licenses, but this data can only be accessed by reviewing each individual license in CAVU. CAVU does not provide a useable reporting method to show all accesses to license files or who accessed license data. CAVU also does not have the ability to flag users' unauthorized attempts to access CAVU.

Lack of CPI and user role access monitoring along with lack of system detection controls and reporting functionality increases the likelihood of noncompliance with statutory requirements and may result in misuse or unauthorized access to CPI without timely detection, which may negatively impact the agency's reputation. Failure to timely remove an employee's access to all systems which contain CPI once an employee is terminated or no longer requires access increases the risk of unauthorized access of CPI.

Recommendation

Promptly remove access to the nine former employees who still have active CAVU credentials. Implement a formal CPI monitoring procedure to detail procedures to complete CPI access reviews, documentation to review, review frequency, responsibilities for conducting reviews, and supporting documentation to maintain as evidence of review completion. System reports, where possible, should be utilized to determine if CPI was accessed outside of normal business hours (i.e. after hours, weekends, holidays), which may indicate inappropriate access, or if unauthorized access was attempted.

Periodically (i.e. quarterly or monthly) perform reviews of user access to ensure the users still require the access assigned to perform job duties. A policy should detail procedures to require prompt communication to ITG of an employee's separation to terminate or disable CAVU and/or NMLS access and procedures to verify the access was removed after the request. COM is transitioning to a Salesforce licensing system in the coming months to replace CAVU. During this transition, ensure there are adequate methods for monitoring access to CPI. This would include notification when an employee attempts to access data or perform activities outside of their access levels, along with routine access monitoring. Management should also closely review user roles and the level of access granted to ensure consistency with access rights needed to perform job duties.

All policies and procedures should be reviewed and approved on a routine basis to ensure they remain up-to-date and reflect current activities and rules.

Management Response

DFI will implement the following procedures and update the Consumer Finance Licensing Manual to require:

- The Licensing Manager will promptly notify COM ITG each time an employee terminates employment in order to ensure timely disabling of access to CAVU. The Licensing Manager will promptly disable NMLS access each time an employee terminates employment. To document, the Licensing Manager will notify the Superintendent or Deputy Superintendent, and the Division Counsel or Assistant Counsel, via email when these steps are completed.

- The Licensing Manager will review CAVU user access and NMLS user access on the first work day of each quarter, or as soon as practical after that but not later than one week, to determine if any data access should be disabled or limited. If any disabling or changing

of data access is needed, the Licensing Manager will email COM ITG for CAVU access and/or will change the access in NMLS as DFI's NMLS administrator. To document, the Licensing Manager will notify the Superintendent or Deputy Superintendent, and the Division Counsel or Assistant Counsel, via email when these steps are completed. • The Licensing Manager will run or request a report from ITG concerning access to CAVU outside of normal business hours on the first work day of each quarter, or as soon as practical after that but not later than one week. The Licensing Manager will review the report to determine if unusual attempts were made to access the system that may require further review or action. To document, the Licensing Manager will notify the Superintendent or Deputy Superintendent, and the Division Counsel or Assistant Counsel, via email when these steps are completed. Additionally, ITG and DFI will include logging of access to CPI and tracking of the reason for access in the requirements for a new DFI database system. COM ITG and DFI anticipate implementing a new system within the next 12-24 months. COM ITG has disabled CAVU-credential access for the former employees. DFI Management would like to emphasize that the former employees did not actually have access to the CAVU system even though the CAVU-specific credentials should be disabled as an additional security step. CAVU is only accessible from the COM network and these former employees did not have access to the network and therefore did not have access to CAVU.

Risk*	Remediation Owner	Estimated Completion Date
Moderate	Deputy Superintendent, Consumer Finance	July 2018

Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the observations and recommendations suggested above. However, these observations reflect our continuing desire to assist your department in achieving improvements in internal controls, compliance, and operational efficiencies.

* Refer to Appendix A for classification of audit observations.

Appendix A – Classification of Conclusions and Observations

Classification of Audit Objective Conclusions

Conclusion	Description of Factors
Well-Controlled	The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor.
Well-Controlled with Improvement Needed	The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.
Improvement Needed	Weaknesses are present that compromise achievement of one or more control objectives but do not prevent the process from achieving its overall purpose. While important weaknesses exist, their impact is not widespread.
Major Improvement Needed	Weaknesses are present that could potentially compromise achievement of its overall purpose. The impact of weaknesses on management of risks is widespread due to the number or nature of the weaknesses.

Classification of Audit Observations

Rating	Description of Factors	Reporting Level
Low	Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity.	Agency Management; State Audit Committee (Not reported)
Moderate	Observation has moderate impact to the agency. Exposure may be significant to unit within an agency, but not to the agency as a whole. Compensating controls may exist but are not operating as designed. Requires near-term agency attention.	Agency Management and State Audit Committee
High	Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation.	Agency Management and State Audit Committee