CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

REPORT IA 21-501

OFFICE OF INSPECTOR GENERAL

AUDIT OF THE DEPARTMENT OF FINANCIAL SERVICES' DIVISION OF REHABILITATION AND LIQUIDATION CLAIMS SECTION CONFIDENTIAL DATA ACCESS

Audit performed by the Office of Inspector General to evaluate the Department of Financial Services' Division of Rehabilitation and Liquidation Claims Section's access to confidential data

David T. Harper, Inspector General
Office of Inspector General
Department of Financial Services

August 16, 2021

CONTENTS

EXECUTIVE SUMMARY

The Department of Financial Services (DFS), Office of Inspector General (OIG) conducted an audit of the DFS Division of Rehabilitation and Liquidation (DRL) Claims section. The overall purpose of this audit was to determine if the DRL uses effective access controls to manage access to the Claims Section's application, Online Claims Processing (OLCP). The OIG used two objectives to make this determination. The first objective was to determine the effectiveness of selected IT controls in achieving management's control objectives pertaining to compliance with controlling laws, administrative rules, and other guidelines. The second objective was to determine if established Information Technology (IT) controls effectively manage user access to OLCP.

Effective IT general controls are required to maintain data confidentiality, integrity, and availability. OLCP maintains confidential information used by the Claims section to perform their job duties. The audit disclosed that there are opportunities for the DRL Claims section to strengthen access controls to OLCP. DRL can strengthen their controls by conducting quarterly access reviews to identify and remove all unauthorized users. DRL can also continue updating their process to include proof that access was terminated.

INTRODUCTION, BACKGROUND, AUDIT OBJECTIVES AND SCOPE

Introduction

The Office of Inspector General (OIG), Audit Section, conducted an audit of confidential data access controls for the Department of Financial Services' (DFS) Division of Rehabilitation and Liquidation's (DRL) Claims Section. This audit was based on OIG's Fiscal Year (FY) 2020-2021 Annual Audit Work Plan and was conducted in conformance with professional standards.

Background

The DRL follows Florida Statute (F.S.) 631, the Insurers Rehabilitation and Liquidation Act. DFS serves as the receiver of any insurer placed into receivership in Florida. The DRL plans, coordinates, and directs the receivership processes on behalf of the Department.

The DRL was divided into seven sections and had 64 fulltime positions during the period of July 1, 2018 through December 31, 2019. The DRL uses two mechanisms to aid insurance companies that are having difficulties: rehabilitation and liquidation. The rehabilitation mechanism includes preparing a plan to assist an insurer in resolving its financial and other difficulties. The goal is to return the insurer to the marketplace. When an insurer's issue cannot be resolved, the company goes through liquidation. The liquidation mechanism is responsible for identifying creditors who are to receive assets from the insurance company and distributing those assets. The Claims section of DRL is responsible for the Division's claims handling, which begins when notification of the company's liquidation is provided to those with an interest in the company's estate, including policyholders, creditors, and guaranty associations.

During FY 2018-19 DRL[1]:

- Administered 17 companies in liquidation and two companies in rehabilitation,
- Closed nine companies,
- Distributed $2.6 million in early access distributions to guaranty associations from two different estates,
- Distributed $47.9 million to claimants in four estates during the fiscal year,
- Processed 3,753 Proofs of Claim, evaluated 601 claims, processed 66 filed objections, resolved 116 objections, processed 119 requests for an assignment of claim, reopened 692 claims and set up 196 new claims,
- Managed six distribution accountings, 10 discharge accountings and processed and filed unclaimed property reports in 50 states, the District of Columbia, and one US Territory for unclaimed amounts totaling $2,986.439 from seven discharged receiverships,
- Recovered assets totaling $20 million, excluding litigation recoveries, and
- Recovered assets totaling approximately $6 million through litigation.

[1] DRL 2019 Annual Report

Audit Objective and Scope

The audit's objectives were the following:

- To determine the effectiveness of selected Information Technology (IT) controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; and ensuring the confidentiality, integrity, availability, and the safeguarding of IT resources.

- To determine if established IT controls effectively manage user access.

The scope of the audit was from July 1, 2018 through December 31, 2019.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Access Reviews

Florida Administrative Code[2] (FAC) requires each agency to ensure access to IT resources is limited to authorized users and processes based on least privilege. FAC[3] also states that "each agency shall manage identities and credentials for authorized devices and facilitate periodic review of access rights with information owners." Additionally, the Department's Application Access Control Policy[4] requires that access privileges are assigned based on an employee's role and access is reviewed quarterly. The audit disclosed DRL Claims section did not conduct the Online Claims Processing (OLCP) quarterly access reviews.

- Two of the six required application access reviews were not completed
- The 2018 third and fourth quarterly application access reviews were completed

The Division explained the employee who oversaw the application audits left the Division and a new employee had not been appointed the duty. Absent an effective review of user access to the OLCP, the risk is increased that the Department may fail to identify users that no longer need access. This unauthorized access to confidential data may result in the exposure of confidential data to unauthorized parties.

Recommendation

The OIG recommends DRL follow their internal policies and procedures (IP&Ps) which require quarterly access reviews to identify and remove all unauthorized user permissions and obsolete accounts.

[2] FAC 60GG-2.003 (1)(d)2 and 3. Information Technology Security
[3] FAC 60GG-2.003(1)(a)6. Information Technology Security
[4] DFS AP&P 4-05 Application Access Control

Finding 2: Application Access Deactivation

The FAC[5] requires organizations to identify a timeframe for removing inactive accounts. Additionally, the DRL's IP&Ps[6] state that the Division is to follow Agency Policies and Procedures (AP&Ps) 4-03 Information Technology Security (Security Policy), which requires accounts be deactivated at the time of employee separation.

The Division explained that access to the OLCP is established through the active directory access established by the Department when an individual is hired and therefore, access to the OLCP is removed when a terminating individual's access is terminated in active directory. To ensure access is terminated appropriately in Active Directory, Human Resources emails a Notice of Separation, which includes an employee's last day, to the Division's IT section. Once the notice of separation is received in the IT section, the date of termination is entered into active directory, which will automatically disable the account at the end of that day and records the date of the action on the Employee Separation Checklist. The Division's IT section keeps employee separation spreadsheets to document the date of employee separation and the date the employee's account was deactivated; however, the IT section could not provide any documentation to support that access was disabled on the date of separation. The Division explained that the Office of Information Technology requires that, after 60 days, any disabled account be deleted from active directory and therefore, they are not able to provide proof that the access was terminated. The audit indicated the following in the deactivation of application access:

- Seven accounts were deactivated within three days, and
- Six accounts were deactivated five to thirteen days after the employee separated

Absent an effective process for the documentation of the deactivation of individuals, that no longer need access to the application, the risk is increased that a former employee will retain unauthorized access to OLCP, and that unauthorized access to confidential data may result in the exposure of confidential data to unauthorized parties.

The Division stated that they will update their process for access control to ensure they document those individuals with access to OLCP. Additionally, the Division has begun updating their process to ensure that they have proof that access to OLCP was terminated when an employee separates from the Division.

Recommendation

The OIG recommends the DRL continue updating their process to include proof that access was terminated.

[5] FAC 60GG-2.003 (1)(a)7. Information Technology Security
[6] R8-03 Information Technology Security

METHODOLOGY

This IT operational audit conforms with *The International Professional Practices Framework* (IPPF), published by The Institute of Internal Auditors. The IPPF requires the OIG to consider risk when planning to perform the audit and obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions that align with audit objectives. Additionally, the IPPF requires the auditors to meet objectivity requirements and possess necessary collective knowledge, skills and experience. The audit evidence obtained provides a reasonable basis for the OIG findings and conclusions.

To accomplish audit objectives, the OIG performed the following audit procedures:

- Reviewed specific Florida Statutes, Florida Administrative Code, DFS AP&Ps and DRL IP&Ps,
- Reviewed policies and procedures that are used to establish access to determine whether the policies and procedures are following Florida Statutes, Administrative Code and Federal Regulations, and
- Conducted testing of general IT controls, including the following:
  - Test of activation requests to determine that access was provided after authorization by supervisor staff,
  - Test of deactivation of access when an employee separates from the Division,
  - Test of periodic reviews to determine that the security staff are performing periodic reviews of user access to determine that user access remains appropriate and necessary, and
  - Test of appropriateness of access to determine that the user access is appropriate for assigned job duties.

ACKNOWLEDGEMENTS

The OIG would like to thank DRL and Claims Section leadership along with Rehab Suppport and OIT leadership for their input, cooperation and assistance throughout the performance of this engagement.

The Office of Inspector General performs audits, consulting activities, and reviews of Department of Financial Services' programs, activities, and functions to promote accountability, integrity, and efficiency in state government.

This engagement was conducted in conformance with The *International Standards for the Professional Practice of Internal Auditing*, published by The Institute of Internal Auditors, Inc., pursuant to Section 20.055, Florida Statutes, and *Principles and Standards for Offices of Inspectors General,* published by the Association of Inspectors General. This engagement was conducted by Jasmine London, CIGA, FCCM, Auditor, under the supervision of Debbie Clark, CPA, CISA, CIGA, CGAP, Director of Audit.

Please address inquiries regarding this report to the DFS Office of Inspector General at 850-413-3112.

DISTRIBUTION LIST

Jimmy Patronis, Chief Financial Officer
Peter Penrod, Chief of Staff
Scott Fennell, Deputy Chief Financial Officer
Toma Wilkerson, Director of Rehabilitation and Liquidation
Allyson Puckett, Director of Claims

ATTACHMENT

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding 1: Application Access Reviews

The audit disclosed DRL Claims section did not conduct the Online Claims Processing (OLCP) quarterly access reviews.

- Two of the six required application access reviews were not completed,
- The 2018 third and fourth quarterly application access reviews were completed, and
- No access reviews were completed in 2019

The Division explained the employee who oversaw the application audits left the Division and a new employee had not been appointed the duty. Absent an effective review of user access to the OLCP, the risk is increased that the Department may fail to identify users that no longer need access. This unauthorized access to confidential data may result in the exposure of confidential data to unauthorized parties.

Recommendation:
The OIG recommends DRL follow their internal policies and procedures (IP&Ps) which require quarterly access reviews to identify and remove all unauthorized user permissions and obsolete accounts.

Response:
The Division is committed to improving all aspects of access control for its systems. The Division has appointed an ASO for the Claims Section and implemented a tracking process that is initiated from the Director's office on a quarterly basis to confirm that quarterly access control audits for all systems are completed. The sections receive a reminder that quarterly audits are due and follow up continues until receipt of all section audits.

Expected Completion Date for Corrective Action:
The corrective action has been completed. The tracking process has been implemented and a copy of the tracking spreadsheet and OLCP access review for quarter ending June 30, 2021, will be provided in a separate document.

Finding 2: Application Access Deactivation

The audit indicated the following in the deactivation of application access:

- Seven accounts were deactivated within three days, and
- Six accounts were deactivated five to thirteen days after the employee separated

The Division explained that access to the OLCP is established through the active directory access established by the Department when an individual is hired and therefore, access to the OLCP is removed when a terminating individual's access is terminated in active directory. To ensure access is terminated appropriately in Active Directory Human Resources emails a Notice of Separation, which includes an employee's last day, to the Division's IT section. Once the notice of separation is received in the IT section, the date of termination is entered into active directory, which will automatically disable the account at the end of that day and records the date of the action on the Employee Separation Checklist. The Division's IT section keeps employee separation spreadsheets to document the date of employee separation and the date the employee's account was deactivated, however the IT section could not provide any documentation to support that access was disabled on the date of separation. The Division explained that the Office of Information Technology requires that, after 60 days, any disabled account be deleted from active directory and therefore, they are not able to provide proof that the access was terminated.

Recommendation:
The OIG recommends the DRL continue updating their process to include proof that access was terminated.

Response
Currently, our HR office sends an e-mail notifying the IT section of an employee separation. IT updates the OIT Active Directory Network so the employee's access will expire on the date of separation and documents the date in an Employee Separation Checklist. Most separation notices include a two-week projected separation date which allows IT to change Active Directory to expire far in advance of the actual separation date. Termination of Active Directory deactivates an employee's access to all Division systems. This allows the IT staff to disable Division systems later because the access was previously removed through the deactivation of Active Directory. The Division does not have the ability to run a report that confirms the date the Active Directory was terminated.

A new separation procedure is being implemented that requires IT to perform a screen shot of the field that is set to expire in Active Directory and will be imbedded in the Employee Separation Checklist. Once IT completes the final exit spreadsheet which includes terminating both Active Directory and OLCP access, it will send confirmation to HR verifying that all systems have been deactivated. HR will not close out the employee separation process until it receives this confirmation from IT which will be included in each employee's separation checklist and file. We believe this process meets the recommendation of updating DRL's process to include proof that access was terminated.

Expected Completion Date for Corrective Action:
The Division expects to complete the corrective action within 30 days of this response or by Thursday, September 30, 2021. The IT Employee Separation Checklist instructions will be

updated to require a screen shot of the Active Directory deactivation and the HR Employment Termination Checklist will be updated to require a copy of the final IT Employee Separation Checklist. Copies of the updated checklists will be provided to OIG by the above deadline.

The Division of Rehabilitation and Liquidation maintains its own Human Resource and Information Technology sections for administration of receivership estates. Responses referenced herein refer to the Division sections as Human Resources ("HR") and Information Technology ("IT").