Exhibit 1

Follow-up Review of the Audit of Driver's License and Motor Vehicle Record Data Exchange Usage by the Risk Management Division

Office of the County Auditor

Robert Melton, CPA, CIA, CFE, CIG
County Auditor

Review Conducted by:
Gerard Boucaud, CIA, CISA, Audit Manager
Muhammad Ramjohn, CISA, Information Technology Auditor

Report No. 19-21
September 26, 2019

BROWARD COUNTY
FLORIDA
OFFICE OF THE COUNTY AUDITOR
115 S. Andrews Avenue, Room 520 • Fort Lauderdale, Florida 33301 • 954-357-7590 • FAX 954-357-7592

September 26, 2019

Honorable Mayor and Board of County Commissioners:

We have conducted a follow-up review of the Audit of Driver's License and Motor Vehicle Record Data Exchange Usage by the Risk Management Division. The objective of our review was to determine the implementation status of our previous recommendations.

We conclude that four previous recommendations were implemented, and one previous recommendation was partially implemented.

We conducted this review in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

We appreciate the cooperation and assistance provided by the Enterprise Technology Services Division throughout the course of our review.

Respectfully submitted,

Bob Melton
County Auditor

cc: Bertha Henry, County Administrator
Andrew Meyers, County Attorney
Monica Cepero, Deputy County Administrator
George Tablack, Chief Financial Officer
John Bruno, Chief Information Officer
Wayne Fletcher, Director Risk Management

TABLE OF CONTENT

INTRODUCTION

Scope and Methodology

The County Auditor's Office conducts audits of Broward County's entities, programs, activities, and contractors to provide the Board of County Commissioners, Broward County's residents, County management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted a follow-up review of the Audit of Driver's License and Motor Vehicle Record Data Exchange Usage by the Risk Management Division (Report No. 18-27). The purpose of our follow-up was to determine the status of previous recommendations for improvement.

The objectives of the original audit were to determine whether:

1. The use of DAVE complies with the terms of the Memorandum of Understanding with the Department of Highway Safety and Motor Vehicles (DHSMV) along with the adequacy of internal control to ensure compliance.
2. Any opportunities for improvement exist.

We conducted this review in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

Our follow-up review included such tests of records and other review procedures, as we considered necessary in the circumstances. The follow-up testing was performed for the period June 1, 2019 to August 31, 2019. However, transactions, processes, and situations reviewed were not limited by the review period.

Overall Conclusion

We conclude that four previous recommendations were implemented, and one previous recommendation was partially implemented.

Background

In December 2014, the Risk Management Division (RMD) entered into a Memorandum of Understanding (MOU) with Department of Highway Safety and Motor Vehicles (DHSMV) to obtain access to the Driver's License and Motor Vehicle Record Data Exchange (DAVE), which provides remote electronic access to driver license and motor vehicle information. This agreement was renewed in February 2018 giving the RMD continued access for an additional three years.

As the information provided through the data exchange is confidential, the MOU has requirements to ensure the physical and logical security of the information. These requirements include, but are not limited to, inactivation of terminated users, acknowledgements of information confidentiality as well as criminal sanctions for confidentiality violations, professional use of the information, annual user training, and periodic reviews and audits of user activity.

Risk Management Division's Data Exchange Usage

Pursuant to Section 119.0712(2), Florida Statutes, as outlined in 18 United States Code, section 2721, personal information in motor vehicle and driver license records can be released:

> *For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.*

RMD, a division of the Finance and Administrative Services Department (FASD), used DAVE to verify the driver's license status of current County employees.

County employees do not have direct access to the DAVE application. The County has created a data interface that automatically downloads drivers' license data for current County employees using a secure file transfer protocol (SFTP). Once downloaded, this information is transferred to the Safety and Health Investigative and Liability Database (SHIELD) application, which is used to manage employee personal information, and generate and distribute reports of suspended licenses to County management.

As of May 2019, the Risk Management Division restructured their operations and moved the function of investigative services to the Human Resources Division. This move transferred all the access, rights, and responsibilities of DAVE to the Human Resources Division. However, Enterprise Technology Services (ETS) still manages the security of the SHIELD application where DAVE data is stored.

OPPORTUNITIES FOR IMPROVEMENT

This section report actions taken by management on the findings in our previous review. The issues and recommendations herein are those of the original review, followed by the current status of the recommendations.

1. Access to Drivers' License Data Should be Restricted Based on Job Responsibilities and Segregation of Duties to Prevent Unauthorized Activity.

During our review of access to DAVE data within the SHIELD application, we noted the following concerns:

A. Management has a process for authorizing logical access to SHIELD using a user access request form. However, this process is not formally documented and is not consistently followed. We noted that one employee hired during the audit period was granted access to SHIELD without an authorized user access form. Providing user access without an appropriately authorized user access request form increases the risk of unauthorized or inappropriate access. Established user administration procedures should be followed to document the level of access an employee is authorized to have as well as management's approval of that access.

B. Privileged access to the SHIELD application is not appropriate in some instances. During our review, we noted the following concerns:

   i. Three of 27 (11%) SHIELD administrators are also operational users performing day to day transactions. This combination of access allows these users to bypass application controls and represents a segregation of duties conflict. As a result, inappropriate activities could occur without timely detection. Application administration functions should be performed by information technology personnel using established user administration procedures rather than operational user staff.

   ii. Two employees had the ability to perform application development activities as well as application administration. This combination of access allows these employees to bypass established change management procedures and represents a segregation of duties conflict. As a result, inappropriate changes could be made to the application without timely detection. Application development functions should be segregated from application administration functions to ensure established change management procedures are followed.

C. Annual reviews of user access to the SHIELD application are not performed to ensure that access to confidential information is restricted based on job responsibilities. Chapter 5, Section H of the MOU requires that all access to the information must be monitored on an ongoing basis. Failure to periodically review access to County systems may allow employees to retain inappropriate access after a change in

job function, termination from Broward County, functional or security changes to applications, and organization structural changes.

We recommended management:

A. Ensure formal procedures for requesting, removing, and modifying user access to SHIELD using access request forms are consistently followed.

B. Restrict business users from performing application administration for the SHIELD application. In addition, application development and administration functions should be segregated.

C. Review user access to SHIELD at least annually. The review should be documented to demonstrate management's due diligence.

Status:

A. **Implemented.**

B. **Implemented.**

C. **Implemented.**

2. Individuals with Access to DAVE Data Stored on County Systems Should Acknowledge the Confidentiality of the Information and Criminal Sanctions for Unauthorized Use.

During our review of employee confidentiality acknowledgements, we noted 24 of 24 (100%) employees with access to DAVE information stored on County systems have not formally acknowledged their understanding of the confidential nature of the information and criminal sanctions for unauthorized use. The MOU requires the County to protect and maintain the confidentiality and security of the data received from the DHSMV. Formal acknowledgement of the confidentiality of the information and criminal sanctions for unauthorized use assists management in demonstrating its due diligence and responding to violations of confidentiality by employees.

We recommended management ensure all users with access to DAVE information stored on County systems formally acknowledge their understanding of the confidential nature of the information and the criminal sanctions for unauthorized use.

Status:

Partially implemented. We noted one of seven ETS employees with access to the data exchanged under the terms of the MOU and did not acknowledge their understanding of the confidentiality of the information and the criminal sanctions for unauthorized use. Management stated that that employee refuses to sign the certification until the Office the County Attorney approves the certification language. Management should ensure all users with access to DAVE information stored on County systems formally acknowledge their understanding of the confidential nature of the information and the criminal sanctions for unauthorized use. Access to DAVE data should be removed for any user refusing to acknowledge the confidential nature of the information and the criminal sanctions for unauthorized use.

3. Application Logs Should be Periodically Reviewed to Identify Unusual Activity.

Management does not perform a periodic review of application logs to identify and follow-up on any unusual activity identified. The SHIELD application has logging enabled; however, management has not implemented a process to periodically review the logs in order to obtain timely notification of inappropriate or unauthorized activity. Without a periodic review of application logs, inappropriate or unauthorized activity may remain undetected.

We recommended management implement procedures to periodically review activity logs for the SHIELD application. In addition, we recommended that management document the review.

Status:

Implemented. Management performed a review of application log activity to identify unusual procedures in July 2019; however, we encourage management to formally approve procedures governing this activity.