Exhibit 1

Follow-up Review of the Audit of Driver and Vehicle Information Database Usage by the Risk Management Division

Office of the County Auditor

Audit Report

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

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

Report No. 19-17
August 22, 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

August 22, 2019

Honorable Mayor and Board of County Commissioners

We have conducted a follow-up review of the Audit of Driver and Vehicle Information Database Usage by the Risk Management Division. The objective of our review was to determine the implementation status of our previous recommendations.

We conclude that all eight previous recommendations are no longer applicable as management has transferred the access, rights, and responsibilities of the Driver and Vehicle Information Database to the Human Resources Division.

We appreciate the cooperation and assistance provided by the staff of the Risk Management Division throughout our review process.

Respectfully submitted,

Bob Melton
County Auditor

cc: Bertha Henry, County Administrator
Andrew Meyers, County Attorney
Wayne Fletcher, Director of Risk Management

TABLE OF CONTENTS

INTRODUCTION

Scope and Methodology

The Office of the County Auditor conduct 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 and Vehicle Information Database Usage by the Risk Management Division (Report No. 18-28). The purpose of our follow-up was to determine the status of previous recommendations for improvement.

The objectives of the original review were:

1. The use of the DAVID system 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 controls to ensure compliance. To determine whether performance measure numbers are accurate.
2. Any opportunities for improvement exist.

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

Overall Conclusion

We concluded all eight previous recommendations are no longer applicable as management has transferred the access, rights, and responsibilities of the Driver and Vehicle Information Database to the Human Resources Division.

Background

In December 2014, the Risk Management Division (RMD) entered into a Memorandum of Understanding (MOU) with the DHSMV to obtain access to the Driver and Vehicle Information Database (DAVID), which provides information relating to driver records and motor vehicle information and history. This agreement was renewed in February 2018 giving the RMD continued access to DAVID for an additional six years.

As the information provided in DAVID is confidential, the MOU includes requirements to ensure the 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 DAVID 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 DAVID to perform the following:

- Verify candidate employee information.
- Verify current and candidate employee driver license status.
- Verify vehicle insurance requirements.
- Perform Vehicle Identification Number (VIN) searches.

RMD had a total of nine active users in the DAVID system during the audit period; two of these users were reclassified as inactive during the period. Active users can request, view, and print drivers' license and vehicle information. Each request submitted through DAVID is logged and stored by the system indefinitely. One user was registered as the Point of Contact (POC) with the DHSMV for RMD. The POC can approve access to the system, assign user roles, deactivate terminated employees, and perform reviews of user activity.

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 DAVID to the Human Resources Division.

OPPORTUNITIES FOR IMPROVEMENT

This section reports 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. Information Obtained from DAVID Should be Used for Legitimate Business Purposes Only.

During our review of personal information requests in DAVID, we noted the following concerns:

A. On two separate occasions within the audit period, one user utilized their DAVID access to perform searches for a relative and close friend for personal reasons in violation of the MOU, which states:

> *"Information exchanged will not be used for any purpose not specially authorized by this MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, business use, personal use, or the dissemation, sharing, copying or passing of this information to unauthorized persons."*

Although these situations appear to be isolated instances, misuse of the DAVID database increases the County's legal risk and may lead to the revocation of access to DAVID and unilateral termination of the MOU by the DHSMV.

B. For eight of 60 (13%) searches reviewed, evidence supporting the business justification for the search was not retained. Upon further inquiry with management, we noted that these searches pertained to validating employee driver's license status based on a report from the SHIELD application; however, these reports are not retained to provide justification for the search performed. Without the maintenance of appropriate evidence to support the business justification for searches, management is unable to demonstrate compliance with MOU requirements and inappropriate searches may remain undetected.

We recommended management:

A. Implement appropriate procedures to ensure the DAVID database is used for legitimate business purposes related to RMD's objectives.

B. Ensure that appropriate documentation is maintained and retained to support the business justification for DAVID searches.

Status:

A. **Not Applicable.** This service has been transferred to the Human Resources Division; this recommendation is no longer applicable to this agency.

B. **Not Applicable.** This service has been transferred to the Human Resources Division; this recommendation is no longer applicable to this agency.

2. Quarterly Quality Control Reviews Should be Performed, Documented and Retained in Accordance With DHSMV's Audit Guidelines.

During our evaluation of the Quarterly Quality Control Review process, we noted the following concerns:

A. Appropriate segregation of duties are not enforced to ensure the integrity of the review. We noted quality control reviews are performed by the Program Manager, who is a frequent user of DAVID. This combination of responsibilities creates a conflict as this individual is potentially reviewing his or her own activity. Segregation of duties is a preventive control designed to preclude improper activity and is essential to ensure that errors or irregularities are detected timely during the normal course of business. Failure to implement appropriate segregation of duties increase the risk of error and inappropriate activity.

B. Adequate documentation of the quality control reviews is not created or maintained by management in order to demonstrate management's due diligence activities. The MOU requires that, effective February 2018, the quality control review report must be documented within 10 days after the end of each quarter and maintained for two years. Without adequate documentation of quarterly control reviews, management is unable to demonstrate compliance with specific requirements of the MOU increasing the County's legal risk.

C. Employees have the ability to access DAVID over the internet from computers outside of the County's network; however, the quality control review does not include procedures to monitor this activity. Employees should only access DAVID information from outside of the County's network when authorized by management. Failure to periodically monitor the location (IP Address) from which DAVID is accessed increases the risk that inappropriate activity may remain undetected.

We recommended management:

A. Ensure job duties are adequately segregated to help ensure errors and irregularities are prevented or detected on a timely basis.

B. Document the results of quarterly quality control reviews in accordance with the requirements of the MOU.

C. Enhance quality control review procedures to include a review of the location from which DAVID is accessed. Management should investigate any such occurrences and document the outcome.

Status:

A. **Not Applicable.** This service has been transferred to the Human Resources Division; this recommendation is no longer applicable to this agency.

B. **Not Applicable.** This service has been transferred to the Human Resources Division; this recommendation is no longer applicable to this agency.

C. **Not Applicable.** This service has been transferred to the Human Resources Division; this recommendation is no longer applicable to this agency.

3. Individuals With Access to DAVID and DAVID 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 the following concerns:

A. Two of 7 (29%) active DAVID users have not formally acknowledged their understanding of the confidential nature of the information and criminal sanctions for unauthorized use.

B. Two of 6 (33%) users with access to DAVID data transferred to 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 DAVID and DAVID data stored on County systems formally acknowledge their understanding of the confidential nature of the information and the criminal sanctions for unauthorized use.

Status: Not Applicable. This service has been transferred to the Human Resources Division; this recommendation is no longer applicable to this agency.

4. Physical Security Controls Should be Enhanced to Adequately Protect Confidential Information.

Risk Management uses combination door locks to restrict access to workstation areas; however, we noted procedures have not been implemented to periodically change the combination lock. As a result, management has not changed the combination lock in the past four years. Broward County IT Administration Policy Volume 7: Chapter 3, Section 4.2 requires access rights to secure areas be revoked immediately for personnel terminated or who no longer require access. Combinations to locks must be changed. Failure to periodically change combination locks increase the risk of inappropriate access to confidential data.

We recommended management implement a process to periodically change combination locks. Management should maintain a log of these changes.

Status: Not Applicable. This service has been transferred to the Human Resources Division; this recommendation is no longer applicable to this agency.

5. Terminated Employee Access Should be Revoked Immediately Upon Termination.

One employee retained access to DAVID for 30 days after their termination from the County. The MOU requires that employee access be immediately deactivated following termination. Terminated employee access to DAVID may result in a breach of confidential information and violate the terms of the MOU. Upon further review, we noted the employee did not access DAVID after the termination date.

We recommended management ensure appropriate procedures are in place to immediately disable terminated employee access.

Status: Not Applicable. While this service has been transferred to the Human Resources Division making this recommendation no longer applicable to this agency. We noted four Risk Management Division users retained access after the transfer. Management should ensure access is restricted to only those employees who require access for the performance of their job responsibilities.