Red Flags Rule

Audit Report # 18-110
March 8, 2018

The University of Texas at El Paso

Office of Auditing and Consulting Services

"Committed to Service, Independence and Quality"

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU

March 8, 2018

Dr. Diana Natalicio
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited- scope audit of Red Flags Rule. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by Office of the Comptroller and Student Business Services staff during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:

Mr. Richard Adauto III, Executive Vice President

Mr. Carlos Martinez, Comptroller

Mr. Juan Gonzalez, Director, Student Business Services

Ms. Sandra Vasquez, Assistant Vice President for Equal Opportunity (EO) and Compliance

University of Texas System (UT System):

System Audit Office

External:

Governor's Office of Budget, Planning and Policy

Legislative Budget Board

Internal Audit Coordinator, State Auditor's Office

Sunset Advisory Commission

Audit Committee Members:

Mr. David Lindau

Mr. Steele Jones

Mr. Fernando Ortega

Dr. Carol Parker

Mr. Benjamin Gonzalez

Dr. Gary Edens

Dr. Roberto Osegueda

Dr. Stephen Riter

Auditors Assigned to the Audit:

Courtney Rios

Monica Escandon

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of the Red Flags Rule Program at the University of Texas at El Paso. The objective of this audit was to determine if the University has created and implemented a written Identity Theft Program that meets the Federal Trade Commission's (FTC) *Identity Theft Rules* (16 CFR 681), commonly referred to as the Red Flags Rule.

The following procedures were performed to accomplish this objective:

- Determine whether the University developed and implemented a written program designed to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account" in compliance with 16 CFR 681 *Identity Theft Rules*.
- Verify that the University manages Red Flags Rule activities that include an annual risk assessment of all areas subject to identify theft, the periodic updating of covered accounts, employee training, and monitoring.
- Confirm that all Red Flags Rule reporting requirements were met in calendar year 2016.

During the audit, we noted the following:

- The University has well documented policies and procedures that address the requirements of the Red Flags Rule.
- The Annual Program Meeting and review was not conducted in December 2016 to report on the 2016 calendar year results.
- Subprogram reports, with the exception of the Information Security Office Report, were not submitted for calendar year 2016.
- An Annual Report was not sent to the President in 2017 for calendar year 2016.

Program monitoring needs to improve to ensure that all activities in the Identity Theft Program are performed consistently and timely to ensure compliance in calendar year 2017.

BACKGROUND

The University of Texas at El Paso is required to develop and maintain an Identity Theft Program to detect, prevent and mitigate identity theft in accordance with the 16 CFR 681, the Federal Trade Commission's (FTC) Red Flags Rule.

The Rule applies to financial institutions and creditors that offer or maintain "covered" accounts. The FTC provides a definition of a covered account in 16 CFR 681.1(b) (3):

(3) Covered account means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

The University of Texas at El Paso is considered a "creditor" under the Red Flags Rule because the University is:

- participating in the Federal Perkins Loan program,
- participating as a school lender in the Federal Family Education Loan Program,
- offering institutional loans to students, faculty or staff, or
- offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

The University is required to develop procedures for the following items:

1.	**Identification of Red Flags:**	Policies and procedures to identify which Red Flags, singly or in combination, are relevant to detecting the possible risk of identity theft to customers using a risk evaluation method appropriate to the organization.
2.	**Detection of Red Flags:**	Policies and procedures designed to prevent or mitigate identity theft in connection with any new account or existing account.
3.	**Responding to Red Flags:**	Policies and procedures to assess whether the Red Flags detected evidence of a risk of identity theft. There must also be a reasonable basis for concluding that a Red Flag does not detect the risk of identity theft.
4.	**Program Updates:**	Policies and procedures in place to ensure the program is updated periodically which reflects changes in risks to the customer and institution.
5.	**Administration of the Program:**	Should involve senior management in development, implementation and oversight. Additionally, ongoing staff training is required as well as oversight of service provider arrangements to ensure they are in compliance.

AUDIT OBJECTIVES

The objective of this audit was to determine if the University has created and implemented a written Identity Theft Program that meets the Federal Trade Commission's (FTC) Identity Theft Rules (16 CFR 681), commonly referred to as the Red Flags Rule. The following procedures were performed to accomplish this objective:

- Determine whether University developed and implemented a written program designed to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account" in compliance with 16 CFR 681 Identity Theft Rules.

- Verify that the University manages Red Flags Rule activities that include an annual risk assessment of all areas subject to identify theft, periodic updating of covered accounts, employee training, and monitoring.

- Confirm that all Red Flags Rule reporting requirements were met in calendar year (CY) 2016

SCOPE AND METHODOLOGY

The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing and the authoritative guidelines of the International Professional Practice Framework issued by the Institute of Internal Auditors.

The audit scope was determined by performing a Risk Analysis to identify high-risk areas for review and testing. Audit methodology included interviews with key personnel and the review of current processes in Student Business Services and the Information Security Office.

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority - an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

AUDIT RESULTS

A. Written Red Flags Rule Program

The university is required to develop and maintain a Written Red Flags Rule Program:

16 CFR 681(d) *Establishment of an Identity Theft Prevention Program*—(1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

A.1. University Policies and Procedures

HOP 8.1 Policy Overview

> *The University of Texas at El Paso ("University") will develop, maintain and update an Identity Theft Prevention, Detection and Mitigation Program ("Program") to detect, prevent and mitigate identity theft in accordance with 16 CFR 681.2, the Federal Trade Commission's "Red Flags Rule."*

The University has a documented policy," *Identity Theft Prevention, Detection and Mitigation Policy* "in Section VII, Chapter 8, of the Handbook of Operating Procedures (HOP). The policy was updated in 2015 and is in compliance with the Red Flags Rule.

HOP 8.4.1 Responsible Party

> *8.4.1.1 The President shall appoint the Responsible Party.*

The Comptroller in the Office of the Vice President for Business Affairs (VPBA) is the appointed University official in charge of the Program. Responsibility for the risk assessment, training, and identification of subprograms is delegated to the Director of Student Business Services.

No exceptions were noted.

A.2. Information Security Policies and Procedures

In addition to the Handbook of Policies and Procedures, the Chief Information Security Officer (CISO) has developed and published a more detailed policy for the identification and response to identity theft. The policy and information security standards are published on the University's Information Security Office website.

UTEP Standard 12: *Security Incident Management* includes:

- Reporting Requirements
- Incident Management Procedures
    a) Detection or Reported Incident
    b) Response to Incident
    c) Initial Incident Assessment
    d) Forensics/Data Gathering
    e) Assigning Responsibility for Investigating Incident
    f) Escalation
    g) Time Requirements
    h) Notification
- Employee Reporting
- Reporting to Information Security Office
- Reporting Requirements to U.T. System
- Monitoring Techniques and Procedures

ISO Information Security Standard 12 is comprehensive and addresses the requirements of the Red Flags Rule. The policy was recently updated in 2017.

No exceptions were noted.

B. Risk Assessment, Training, and Monitoring not performed for all subprograms

The University should provide training and monitor all University staff as necessary to implement and enforce the Policy and Program effectively, as outlined in the UTEP HOP:

HOP 8.4.2 Risk Assessment and Program Review

8.4.2.1 An annual risk assessment shall be performed to determine if additional departments and/or areas have become responsible for opening or maintaining covered accounts. Each department must determine the following:

- *Types of covered accounts offered and maintained*
- *Existing account opening processes*
- *Methods for accessing existing accounts*
- *Previous instances where identity theft has occurred*

8.4.2.2 The program administrator shall complete an annual program and review any incidents of identity theft occurring since last review, changes in methods of identity theft and to the methods of identifying and preventing identity theft.

The Annual Program meeting and review was not conducted in December 2016 to report on the 2016 calendar year results. Subprogram reports, with the exception of the Information Security Office Report, were not submitted for calendar year 2016.

The Annual Meeting has been held in previous years and included two PowerPoint presentations developed by Student Business Services for the training. In addition to the employee training, the office identifies the departments that handle covered accounts. Each department must submit an annual subprogram report to ensure the University is complying with the Red Flags Rule. Subprogram reports from previous years were provided to auditors.

Management stated that the absence of the Annual Program Review for 2016 to be reported in 2017 was an oversight. The Annual Program Review will be completed for 2017. Training took place on December 14, 2017, and subprogram reports for calendar year 2017 will be due in February 2018. The risk assessment to identify the subprograms was conducted in November 2017. Additionally, Program information and report templates have been provided in advance to all departments required to submit subprogram reports.

Recommendation:

The risk assessment, training and monitoring should be conducted annually to ensure compliance with the Red Flags Rule.

Level: This finding is considered **MEDIUM** due to the fact to the fact the program should be updated at least annually to consider new covered accounts and new ways to detect and prevent identity theft.

Management Response:

We agree with the recommendation. The training for the 2017 reporting period has already been conducted and all subprogram reports have been turned into Student Business Services. Systems are in place to ensure training is conducted annually.

Responsible Party:

Director Student Business Services.

Implementation Date:

May 31, 2018

C. Reporting

C.1 Information Security Office Red Flags Report

The CISO prepared a Red Flag Subprogram Report and submitted it to the VPBA. The report includes the results from the following activities conducted by the ISO:

- ISO Risk Assessment
- Method of Detection of Red Flags
- Documentation of all actual or potential identity theft incidents and their resolution
- Prevention and Mitigation Responses
- Program Updates
- Training

C.2 Annual Report to the President was not prepared in 2016

The VPBA should report annually to the President to ensure compliance with the Red Flags Rule. This report should include the subprogram report submitted by the ISO and all other subprograms with covered accounts. Per the HOP,

HOP 8.4.3 Reporting

> *8.4.3.1 The VPBA shall submit an annual report to the President illustrating the program's effectiveness, any third party service provider agreements, significant incidents of identity theft, management's response, and any recommended changes to the Program.*

The report should address material matters related to the Policy and Program and evaluate issues such as:

- *the effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts;*
- *third party service provider agreements related to Covered Accounts;*
- *significant incidents involving Identity Theft and management's response;*
- *recommendations for material changes to the Program.*

An Annual Report was not sent to the President in 2017 for calendar year 2016.

Recommendation:

Prepare and submit an Annual Report to the President that summarizes the program activities, third party service provider agreements, significant incidents of identity theft, and recommended changes to the program.

Level: This finding is considered **MEDIUM** due to the fact that the Information Security Office completed a Red Flag Annual Report timely.

Management Response:

We agree with the recommendation that the program Annual Report should be submitted to the President annually.

Responsible Party:

Comptroller

Implementation Date:

May 31, 2018

CONCLUSION

Based on the results of audit procedures performed, we conclude that the University has successfully developed written policies and procedures to detect, prevent and mitigate identity theft in compliance with16 CFR 681, the Federal Trade Commission's "Red Flags Rule."

The University CISO has also created detailed policies and procedures to supplement the Handbook of Operating Procedures. The CISO prepares a Red Flags Annual Report, which discloses all potential identity theft red flags during the year. The Report outlines the methodology used to effectively identify and resolve the incidents. Although the highest risks are addressed in this report, additional support activities are not performed and reported on a consistent basis.

We wish to thank the management and staff of the Office of the Comptroller, Student Business Services, and the Information Security Office for their assistance and cooperation provided throughout the audit.