Alaska Commission on Postsecondary Education

Internal Audit Committee Meeting

July 21, 2022

Internal Audit Committee

Teleconference: Dial 1-888-788-0099
Enter conference code: 818 3398 1654 #

Thursday, July 21, 2022

1. 3:15 p.m. Convene/Roll Call

2.* Adoption of Agenda

3.* Approval of Minutes of April 8, 2021 Meeting

4. Approval of Annual Fair Credit Reporting Act (FCRA) Red Flags Fraud Prevention Plan – Quality Assurance Officer Jackie Hall

5. Audit Updates – Quality Assurance Officer Jackie Hall

7.* Establish Next Meeting Date
Staff recommendation:
April 2023 Commission meeting date

8.* 3:45 p.m. Adjourn

***Action Required**

MINUTES OF THE
ALASKA COMMISSION ON POSTSECONDARY EDUCATION
INTERNAL AUDIT COMMITTEE MEETING
April 8, 2021

A meeting of the Alaska Commission on Postsecondary Education (ACPE) Internal Audit Committee, conducted via distance delivery, originated from the office of the Commission at 3030 Vintage Blvd. Juneau, Alaska on Wednesday, May 26, 2021. Chair Joshua Bicchinella called the meeting to order at approximately 2:45 p.m.

ATTENDEES

Committee members present for all or portions of the meeting: Commission Chair Joshua Bicchinella, Corporation Chair Anna MacKinnon, Commission Member Barbara Adams and Sana Efird, Ex-Officio.

Commission staff present for all or portions of the meeting: Sana Efird, Executive Director; Kerry Thomas, Director of Program Operations; Jackie Hall, Quality Assurance Officer; and Joe Felkl, Executive Secretary.

ADOPTION OF AGENDA

Member MacKinnon moved to adopt the agenda of the May 26, 2021, Executive Committee meeting. Member Adams seconded the motion. By roll call vote, all members present voted aye. The motion carried.

APPROVAL OF MINUTES

Member MacKinnon moved to approve the minutes from the April 8, 2019, Internal Audit Committee meeting as written with an amended that the approval is contingent upon legal review. Commissioner Adams seconded the motion. By roll call vote, all members present voted aye. The motion carried.

Discussion: Member MacKinnon asked if it was appropriate for members that did not attend the meeting to motion and approve the minutes. Ms. Efird recommended moving forward with a vote, and staff would check with Assistant Attorney General Susan Sonneborn to confirm the action was appropriate. Chair Bicchinella commented the minutes appear to be an accurate reflection of the 2019 meeting.

REPORTS

Identify Theft Prevention Program Review - Ms. Hall presented her report starting on page 5 of the meeting packet on the agency's annual identify theft prevention program review as required by the Fair and Accurate Credit Transaction Act (FACTA), an amendment to the Fair Credit Reporting Act (FCRA) which includes the Red Flags Rule (16 CFR 681.1).

Discussion: Member Adams asked how the number of fraud indicators this year compare to last year. Ms. Hall explained she does not have specific numbers on the number of indicators. A discrepancy in address can be common. The Commission has not had any prior incidents where a consumer contacted the Commission and stated they did not take out a loan. The Commission sends out letters to notify consumers of potential fraud or identify theft, so they can contact the Commissioner before the loan proceeds through the process. Chair Bicchinella asked if the data on the indicators could be provided to the committee. Ms. Hall asked if members were looking for information about contacts from consumers about potential identity theft or statistics on the number of red flag indicators. Member Adams clarified the red flag indicators appear to be a process of data cleaning. She appreciate hearing numbers on how rare it is claims of fraud are received, but information on every red flag indicator might be too detailed. Chair Bicchinella agreed.

Federal Family Education Loan Compliance Review - Ms. Hall referenced her written report on page 13 of the meeting packet on several compliance reviews for the Commission's Federal Family Education Loans. Federal Guarantor, Ascendium Education Inc., conducted a program review of ACPE's servicing of its guaranteed portfolio during August 2019. This review covered the period of May 1, 2017 through April 30, 2019. On January 10, 2020, Ascendium issued an audit closure notice stating ACPE met all requirements and officially closed the review. Additionally, the US Department of Education (ED) conducted a program review of ACPE's servicing of its guaranteed portfolio during August 2019. The review covered the period of October 1, 2014 through March 31, 2019. On May 6, 2020, ED issued an audit closure notice stating ACPE met all requirements and officially closed the review.

Discussion: Member Adams about the normal timeframe of an audit. Ms. Hall replied the guarantor audits occur every two years, and she does not have a timeframe for the next US Department of Education.

2021 MEETING DATE

Member MacKinnon moved to hold the next committee meeting on the same day as the regular April Commission meeting, which is scheduled for April 6, 2022. Member Adams seconded the motion. By roll call vote, all members present voted aye. The motion carried.

ADJOURN

There being no further business to discuss, Chair Bicchinella adjourned the meeting at approximately 3:15 p.m.

Alaska Commission on
Postsecondary Education
P.O. Box 110505
Juneau, Alaska 99811-0505

Customer Service Center
Toll Free: (800) 441-2962
In Juneau: (907) 465-2962
TTY: 711 or (800) 770-8973
Fax: (907) 465-5316
acpe.alaska.gov

MEMORANDUM

To: Members, Internal Audit Committee
Through: Kerry Thomas, Director of Program Operations
Sana Efird, Executive Director
From: Jackie Hall, Quality Assurance Officer
Date: June 30, 2022
Subject: Annual Identity Theft Prevention Program Review

The Fair and Accurate Credit Transaction Act (FACTA) is an amendment to the Fair Credit Reporting Act (FCRA) and includes the Red Flags Rule (16 CFR 681.1). Under the Red Flags Rule, a qualifying creditor such as the Alaska Commission on Postsecondary Education (ACPE) must develop and oversee an Identity Theft Prevention Program.

ACPE implemented its Identity Theft Prevention Program (Program) in 2009, which includes policies and procedures designed to reasonably identify, detect and respond to identity theft. Under the Programs oversight and administration requirements, staff must annually review its Program to evaluate its effectiveness in addressing the risk of identity theft.

The Commission's Quality Assurance (QA) staff conducted a review of ACPE's Identity Theft Prevention Program to ensure all aspects of the Program are applicable to the current business environment and to determine if changes should be made to address emerging risks to customers, or the safety and soundness of the agency from identity theft. The following factors were considered:

- ACPE's past experience with identity theft;
- Changes in methods to detect, prevent and mitigate identity theft;
- Changes in the methods to open accounts;
- Changes to the methods to access accounts;
- Changes in types of accounts ACPE offers; and
- Changes in business arrangements, programs, or services.

Compliance Report
QA's annual compliance review confirmed existing Red Flags continue to be appropriate for ACPE's covered accounts. No new red flag categories were identified and no new covered accounts were implemented in 2021. ACPE's Program conforms to the provisions of FACTA and FCRA and is effective in addressing the risks of identity theft in connection with covered

accounts. Therefore, no changes were made to ACPE's Identity Theft Prevention Program in 2021. Additionally, ACPE had no incidents of identity theft in 2021.

Employee Training

The State of Alaska (SOA), Office of Information Technology (OIT) implemented its security awareness training program in 2019, in an ongoing effort to promote a culture of cybersecurity awareness, and continues to provide mandatory statewide cybersecurity training to all SOA employees, annually.

ACPE implemented its privacy and security training program in 2009, specific to identity theft detection and prevention practices. This training detailed the Red Flags Rule, ACPE's Identity Theft Prevention Program and provided guidance on how to detect, prevent and respond to potential identity theft. Over time, ACPE has expanded its training program to include other important security topics, prevention measures, and best practices to help employees understand the risks in using today's technology, how to effectively defend against potential security threats, the role employees play in safeguarding personal and confidential information.

Through annual training, staff reinforce their knowledge, commitment and effectiveness in protecting customers' personal information, which translates into a stronger security posture throughout the organization.

Staff completed the following privacy and security training in 2021:

SOA Statewide Cybersecurity Training

- Cyber Heroes Series: Don't Take the Bait – This course focused on helping employees guard against phishing attacks.
- Captain Awareness: Securely Working from Home – This course provided helpful tips and best practices to securely work from home.
- Cyber Essentials Series: This course focused on helping employees understand how to stay safe while working remotely.
- 2021 Your Role: Internet Security and You – This course provided awareness that every employee is a target of cybercrime. The course covered the types of attacks so employees can spot them and help keep the organization safe from cybercrime.

ACPE Privacy and Security Training

- ACPE's Security Measures – This course provided an overview of technical, physical, and personnel security measures to secure our systems and facilities, and to protect customer and employee information.
- Teleworking Best Practices – This course reinforced the importance of safeguarding sensitive information while teleworking.
- Safeguarding Nonpublic Personal Information (NPI) – This course covers the types of protected customer information and the importance of safeguarding NPI.
- The FACTA Red Flags Rule – This course provides an overview of the Red Flags Rule, ACPE's Identity Theft Prevention Program and guidance on detecting, preventing and mitigating identity theft.
- ACPE's Security Breach Incident Identification Protocols – This resource provides guidance on how to identify and respond to an unauthorized release of or unauthorized access to nonpublic personal information.

Servicer Oversight
A key requirement in the administration of ACPE's program is to monitor the activities of service providers to ensure they are conducting activities covered by the Rule – for example, application processing, onboarding loans, managing accounts, customer billing and correspondence, and collections – servicers must apply the same standards as ACPE in performing these activities.

ACPE requires third-party servicers who provide services directly to, and on behalf of ACPE, to maintain an Identity Theft Prevention Program and provide ACPE with documentation supporting the program. Servicers must provide ACPE with annual reports that outline any of the following:

- Red flags detected that could result in emerging risks to ACPE customers and how those red flags have been incorporated into their Identity Theft Prevention Program;
- Changes to their Identity Theft Prevention Program. If changes were made, servicers must provide current documentation; and
- Any instances of identity theft and agency responses.

ACPE outsources a portion of its origination and servicing activities to the following entities:

CampusDoor Holdings Inc.
In April 2022, ACPE outsourced the loan origination of its private education loans to CampusDoor. Loan applications will be collected, processed and disbursed by CampusDoor beginning with the 2022 academic period. All loans disbursed by CampusDoor will be transferred for servicing to Pennsylvania Higher Education Assistance Agency (PHEAA), conducting business as American Education Services (AES).

CampusDoor's Identity Theft Program (Program) focuses on four distinct points in the origination of private student loans during which Red Flags may arise.

- Loan application intake;
- Automated customer identification process;
- Obtaining a consumer credit report; and
- Obtaining supporting customer documentation.

CampusDoor's Program conforms to the provisions of FACTA and the FCRA and was approved by their internal Risk Management Committee in September 2020. No changes were made to their program in 2021.

Pennsylvania Higher Education Assistance Agency (PHEAA)
PHEAA, conducting business as AES, is ACPE's third-party servicer for the Federal Family Education Loan Program (FFELP) portfolio as well as new loans originated by CampusDoor.

PHEAA's Identity Theft Detection, Prevention and Mitigation Program (Program) consists of steps to identify, detect, and respond to patterns, practices, or specific activities that indicate the possible existence of identity theft (Red Flags). PHEAA's Program conforms to the provisions of FACTA and FCRA.

PHEAA's annual report included confirmation of their established Identity Theft Prevention Program and employee training. PHEAA concluded that no new red flag categories were identified, and no changes were made to their Program in 2021. PHEAA reported no incidents of identity theft in 2021.

Transworld Systems Inc.
Transworld Systems, Inc. (TSI), formerly Premiere Credit of North America is ACPE's third-party collection vendor for defaulted alternative education loans.

TSI's Fraud and Identity Theft Program (Program) focuses on four key elements, which create a framework to address the threat of fraud and identity theft in the loan servicing and debt collection environments.

- Identify the Red Flags of fraud and identity theft TSI is likely to encounter in loan servicing and debt collection;
- Set up processes to detect Red Flags in day-to-day operations;
- Prevent and mitigate identity theft and if a Red Flag is detected, respond appropriately to prevent and mitigate the harm done; and
- Perform an annual evaluation of the Program based on reports of current Fraud and Identity Theft practices and make corresponding updates as needed;
- Update training materials to help ensure the relevance and effectiveness of the Program.

TSI's annual report included confirmation of their established Identity Theft Prevention Program and employee training. TSI's Program conforms to the provisions of FACTA and FCRA. TSI concluded that no new red flag categories were identified, and no changes were made to their Program in 2021. TSI reported no incidents of identity theft in 2021.

ACPE Guide

● ACPE: Identity Theft Prevention Program

PURPOSE:

To establish an Identity Theft Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide continued administration of the program in compliance with 16

EFFECTIVE DATE:

3/12/2018

TO BE USED BY:

Quality Assurance, General Managers

Table of Contents

ACPE's Identity Theft Prevention Program 2
1. Program Oversight and Administration 2
2. Detection of Red Flags 2
3. Identified Red Flags 2
4. Responding to Red Flags and Address Discrepancies 3
5. Program Resources and Support 4
6. Safeguards to Protect Customer Information 4

Overview

ACPE's Identity Theft Prevention Program was developed in compliance with the Fair Credit Reporting Act (FCRA), the Fair and Accurate Transaction Act (FACTA), the Red Flag Program Clarification Act, and the Red Flags Rules to identify, detect, and respond to cases of potential identity theft. It is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide continued administration of the program in compliance with 16 CFR 681.

A covered account is 1) an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions, or 2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft. Each financial institution and creditor must periodically determine whether it offers or maintains a "covered account."

The program includes policies and procedures designed to reasonably:

1. **Identify** relevant Red Flags for the covered accounts the financial institution or creditor offers or maintains;
2. **Detect** those Red Flags that have been incorporated into the program;
3. **Respond** appropriately to any Red Flags that are detected to prevent and mitigate identity theft;
4. Ensure the **program is updated periodically** to reflect changes in risks to customers and the financial institution; and

5. **Educate** staff about Red Flags.

ACPE's Identity Theft Prevention Program

1. Program Oversight and Administration

The Internal Audit Committee of the Commission provides oversight of ACPE's Red Flags Program. Operational implementation of the program and training has been delegated to Quality Assurance (QA).

The Internal Audit Committee will:

- Review compliance reports
- Approve material changes to the program as necessary to address changing risks
- Receive annual or more frequent updates, as needed, specific to the Red Flags Program

The Quality Assurance team will:

- Review the program annually to ensure all aspects of the program are up-to-date and applicable in the current business environment
- Implement approved changes
- Provide and document annual staff training (training provided as part of new employee training and annually thereafter)

2. Detection of Red Flags

The program detects red flags in connection with the opening of covered accounts and servicing of existing covered accounts as set forth in the Customer Identification Program rules, 31 CFR 103.121, by:

A. Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and

B. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

3. Identified Red Flags

ACPE has identified the following relevant red flags:

A. **Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, including**:

- A fraud or active duty alert included with a consumer report
- A notice of credit freeze from a consumer reporting agency, in response to a request for a consumer report
- A notice of address discrepancy from a consumer reporting agency

B. **An application or other customer document appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.**

C. **The presentation of suspicious personal identifying information, including:**

- Personal identifying information provided is inconsistent when compared against external information sources used by ACPE
- ACPE is notified by an internal or external source (ACPE staff, credit bureau, collection vendor, school, etc.) that the personal identifying information provided is associated with known fraudulent activity.
- The Social Security Number provided is the same as that submitted by other persons opening an account or other customers
- The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete
- Personal identifying information provided is not consistent with personal identifying information on file with ACPE

D. **The unusual use of, or other suspicious activity related to, a covered account, such as:**

- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account
- ACPE is notified the customer is not receiving account statements as expected
- ACPE is notified of unauthorized transactions in connection with a customer's covered account
- ACPE receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by ACPE
- ACPE is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person of a fraudulent account for a person engaged in identity theft

4. Responding to Red Flags and Address Discrepancies

The program provides appropriate responses to detect and mitigate identity theft. The response is commensurate with the degree of risk posed. Appropriate responses to the detection of red flags include:

- Determine no response is needed under the particular circumstances
- Monitor a covered account for evidence of identity theft
- Contact the customer
- Change any passwords, security codes or other security devices that permit access to an account or lock an account
- Refuse to open a new account
- Invalidate a Promissory Note
- Close an account
- Notify law enforcement

Address Discrepancies

The program includes procedures to notify an applicant of discrepancies between the address provided on the loan application and the address contained in the consumer’s credit report, as set forth in the Address Discrepancy Rules, section 114 of the FACT Act, 15 U.S.C 1681m. ACPE will furnish the consumer's address to the consumer reporting agency from which it received the notice of address discrepancy if:

A. ACPE establishes a continuing relationship with the consumer; and

B. ACPE regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.

5. Program Resources and Support

ACPE has developed policies, procedures, training resources, and internal controls to assist in identifying red flags, including subscribing to alerts from the national terrorist watch list administered by the Office of Foreign Assets Control (OFAC), and responding to potential identity theft. Credit bureaus and agencies have measures in place to ensure compliance with OFAC regulations. The credit bureau will match a credit applicant's name and other information to the OFAC list, and a red flag or alert is placed on the report when a potential match exists.

The following resources support ACPE's Identity Theft Prevention Program:

A. **Program Information**
- Guide providing an overview of ACPE's Identity Theft Prevention Program, ACPE's Red Flags, and staff responsibilities under the program.

B. **Incident Identification**
- Procedure for responding to OFAC/Red Flag reports regarding the SDN list, an identity discrepancy, high risk address, fraud, and military active duty alerts.

C. **Incident Response and Borrower Notification**
- Customer notice of identity discrepancy
- Customer notice of address discrepancy
- Customer notice of high risk address
- Notice of address change to the borrower
- Notice of address change to the cosigner
- Process flow for identity theft based on FFELP false certification
- Procedure when handling customer reports of potential identity theft
- Procedure for processing forgery and fraud claim forms
- Procedure to processing FFELP claims of identity theft
- Guide on identity theft under the FFELP program
- Guide on handling allegations of loan forgery and fraud
- Guide on ACPE's Red Flags and staff responsibilities

6. Safeguards to Protect Customer Information

ACPE's Information Security Program contains administrative, technical, and physical safeguards to protect customer information and prevent identity theft. This program includes agency policies, procedures, and informational resources for the following:

A. **Employee Management and Training**
- Recruitment and Background Checks

- Data System Administration
- Training and Awareness

B. **Computer and Network Information Security**

- Secure System Access and User Authentication
- Passwords
- Securing Mobile Devices
- Electronic Transmittal of Nonpublic Personal Information (NPI)
- IT Infrastructure Security Monitoring

C. **Facility Security**

- Access to Confidential Information
- Records Retention and Data Disposal

D. **Incident Response and Reporting**

E. **Business Continuity Planning**

Alaska Commission on
Postsecondary Education
P.O. Box 110505
Juneau, Alaska 99811-0505

Customer Service Center
Toll Free: (800) 441-2962
In Juneau: (907) 465-2962
TTY: 711 or (800) 770-8973
Fax: (907) 465-5316
acpe.alaska.gov

MEMORANDUM

To: Members, Internal Audit Committee
Through: Kerry Thomas, Director of Program Operations
Sana Efird, Executive Director
From: Jackie Hall, Quality Assurance Officer
Date: June 30, 2022
Subject: Federal Family Education Loan Program Reviews

Federal Family Education Loan Program Reviews

No activity in this area since the last report.

Upcoming Program Reviews

Federal guarantors typically conduct biennial reviews of FFEL lenders. Ascendium has not contacted ACPE to schedule our next program review.