Alaska Commission on Postsecondary Education

Internal Audit Committee Meeting

April 8, 2021

ALASKA COMMISSION ON POSTSECONDARY EDUCATION
INTERNAL AUDIT COMMITTEE

Teleconference: 1 (800) 315-6338; **Code:** 67401#

Thursday, April 8, 2021

1.	2:45 p.m.	Convene/Roll Call
2.*		Adoption of Agenda
3.*		Approval of Minutes of April 10, 2019 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
6.*		Establish Next Meeting Date Staff recommendation: • April 2022 Commission meeting date
7.*	3:15 p.m.	Adjourn

***Action Required**

ALASKA COMMISSION ON POSTSECONDARY EDUCATION
MINUTES OF THE
INTERNAL AUDIT COMMITTEE

April 10, 2019

A meeting of the Internal Audit Committee was held on Wednesday, April 10, 2019 in the ACPE office conference room at 3030 Vintage Boulevard in Juneau, Alaska. The meeting convened at 3:04 p.m.

ATTENDEES

Members participating: Josh Bicchinella, Randy Weaver, Patricia Jacobson, and Stephanie Butler (ex-officio). Staff participating: Michelle Norman, Quality Assurance Officer; and Patricia Nickell-Zimmerman, Executive Secretary.

ADOPTION OF AGENDA

Commissioner Bicchinella moved to adopt the agenda as written. Commissioner Weaver seconded the motion. Members unanimously adopted the agenda without change.

MINUTES FOR APPROVAL

Commissioner Weaver moved to adopt the March 20, 2018 minutes as written. Commissioner Bicchinella seconded the motion. The minutes were unanimously approved without change.

REPORTS

Internal Auditor Recruitment - Executive Director Butler noted that due to the State's hiring freeze, there will not be ongoing recruitment for the Internal Auditor position. The Quality Assurance staff has absorbed those duties.

Identify Theft Prevention Program Review - Ms. Norman presented a report on the agency's annual identify theft prevention program review.

Federal Family Education Loan Compliance Review - Ms. Norman provided a written report on the compliance review of the Federal Family Education Loans, as it relates to the Service members Civil Relief Act program. She reported that in August of 2018 the US Department of Education issued a Final Program Review Determination and identified a population of loans that needed corrections. These corrections have been made and they were reported to the auditor on January 25, 2019. The final audit closeout is expected after the end of the first quarter.

Premiere Credit of North America Contract Review – Ms. Norman provided a written report on the 2018 PCNA contract review. The review identified seven findings that resulted in 11 recommendations. The vendor is addressing them.

2020 Meeting Date

Commissioner Bicchinella moved to hold the next committee meeting on the same day as the regular April Commission meeting, which is scheduled for April 8, 2020. Commissioner Weaver seconded the motion. The members unanimously agreed.

Adjourn

Commissioner Weaver moved to adjourn. Commissioner Bicchinella seconded the motion. The members unanimously agreed. The meeting adjourned at 3:45 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: March 15, 2021
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, implement, and administer an identity theft prevention program.

ACPE implemented its Identity Theft Prevention Program in 2009. Under the programs oversight and administration requirements, staff must annually review its identity theft prevention 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.

Review of Covered Accounts
QA reviewed existing state and federal programs and red flag categories, as outlined in ACPE's Identity Theft Prevention Program, to determine if there were changes in the type of accounts that ACPE maintains, or changes in the business processes for these covered accounts that would pose potential risk of identity theft. It was determined the existing red flags continue to be

appropriate for ACPE's covered accounts. In addition, no new covered accounts were implemented in 2020.

Indicators of Fraudulent Activity
In 2020, ACPE received two reports of potential identity theft related to the opening of a new account. Both incidents were identified based on a notice of address discrepancy from the consumer reporting agency. Procedures dictate the applicant be notified of a discrepancy between the address provided on the loan application and the address contained in the consumer's credit file.

Notices were mailed to each applicant at the address shown on their credit report, requesting the consumer contact ACPE regarding a recent application for an education loan. Both consumers contacted ACPE to report the potential fraudulent activity. ACPE took immediate steps to cancel the pending applications and unauthorized the online accounts associated with each transaction. Staff provided each consumer with additional steps to take if they believe they are a victim of identity theft.

Staff reviewed the program's detection and response methods for authenticating customers, monitoring transactions, and verifying the validity of change of address requests for the opening and servicing of covered accounts. Staff assessed the effectiveness of the programs detection and response methods against the potential fraudulent activity that occurred during the review period.

Staffs review of ACPE's Identity Theft Prevention Program and assessment of the identity theft reports, reaffirmed ACPE's existing controls and red flag indicators are appropriate in detecting and mitigating potential identity theft in today's environment. Based on this assessment, no changes were made to the program in 2020.

Employee Training
All employees must annually participate in ACPE's privacy and security training, which includes identity theft detection and prevention. The goal of this training is to help employees understand the risks in using today's technology, how to effectively defend against potential security threats, and 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.

ACPE's privacy and security training covers the following topics:

- Safeguarding Nonpublic Personal Information
- The FACTA Red Flags Rule
- ACPE's Identity Theft Prevention Program and Red Flags
- ACPE's Technology Policy
- ACPE's Security Breach Incident Identification Procedure

In July 2019, the State of Alaska (SOA), Office of Information Technology (OIT) launched a new training platform to help improve online security practices and raise cybersecurity awareness. OIT annually assigns one or more online cybersecurity training modules, hosted by KnowBe4.

In addition to ACPE's annual privacy and security training, staff completed the following OIT training modules in 2020:

- **2020 Common Threats** – This course provided strategies for staying safe on computers, mobile devices, and in modern office environments.
- **Internet Security When You Work From Home** – This course focused on the challenges of working remotely and how to stay safe and secure online while working from home.

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, managing accounts, billing customers, providing customer service, and collections – they 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. In addition, servicers must provide ACPE with annual reports that outline any:

- Red flags detected that could result in emerging risks to ACPE customers and if necessary how those red flags have been incorporated into their Identity Theft Prevention Program;
- Changes to their Identity Theft Prevention Program and staff training materials. If changes were made, provide current documentation;
- Any instances of identity theft that have not been reported to ACPE and their responses to those reports.

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

Premiere Credit of North America, LLC ("Premiere Credit")
Premiere Credit is ACPE's third-party collection vendor for defaulted alternative education loans.

Premiere Credit's annual report included confirmation of their established Identity Theft Prevention Program in 2020. No new red flag categories were identified, and no changes were made to their existing program. However, with the acquisition of Premiere Credit by Performant Recovery, they gained an Information Security Officer and team to provide more education and staff straining in areas like phishing and red flags.

Premiere Credit reported no incidents of identity theft in 2020.

Pennsylvania Higher Education Assistance Agency (PHEAA)
Pennsylvania Higher Education Assistance Agency (PHEAA), conducting business as American Education Services (AES), is ACPE's third-party servicer for the Federal Family Education Loan Program (FFELP) portfolio. ACPE outsourced the FFELP portfolio to PHEAA in April 2020.

PHEAA's annual report included confirmation of their established Identity Theft Prevention Program and employee training. No new red flag categories were identified, and no changes were made to their program 2020.

PHEAA reported no incidents of identity theft in 2020.

ACPE Guide
● ACPE: Identity Theft Prevention Program

PURPOSE:
Documents ACPE's Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with a covered account and to provide continued administration of the program in compliance with 16 CFR 681 and the FACTA.

EFFECTIVE DATE:
3/12/2018

TO BE USED BY:
Quality Assurance, General Managers

Table of Contents

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: March 20, 2021
Subject: 2019 FFELP Program Review

Ascendium Federal Family Education Loan (FFEL) Program Review

Federal Guarantor, Ascendium Education Inc., conducted a program review of ACPE's servicing of its guaranteed portfolio during August 2019. Guarantors are charged under FFEL Program regulations, 34 CFR 682, with the responsibility to ensure institutional compliance by conducting comprehensive biennial reviews of lenders. This review covered the period of May 1, 2017 through April 30, 2019.

The focus of the review was to determine ACPE's compliance with the Higher Education Act (HEA) and applicable federal regulations and requirements in administering the FFEL program. The review focused on the process for conversion to repayment, Income Based Repayment (IBR), deferment, forbearance, claims, Lender's Interest and Special Allowance Request and Report (LaRS) submittals and adjustments, and Servicemembers Civil Relief Act (SCRA).

On December 11, 2019, Ascendium Education Inc. issued a Program Review Report, which identified two findings. This report was provided to the US Dept. of Education.

1. **Ineligible Period of Deferment.** During the review, it was identified one borrower's unemployment deferment request was processed for an incorrect period. ACPE incorrectly applied the deferment to the borrower's account with a start date of 2/6/19 rather than 2/2/19. The deferment start date was corrected from 2/6/19 to 2/2/19. Documents containing the screen shot reflecting the updated start date and the Government Billing Screen from our servicing system reflecting the 12/31/2019 LaRS adjustments to the account were provided.

2. **Failure in Loan Servicing.** The review identified a period of delinquency, 11/5/09 – 6/7/10 that was not covered by a forbearance as should have occurred, resulting in a gap

in due diligence of more than 45 days. The period in question was outside the Period under Review (PUR) 5/1/2017 – 4/30/2019. Consequently, the due diligence activity screen shots initially provided for the review did not cover the period of 11/5/09 – 6/7/10. Screen shots covering this period were provided, reflecting no gap in due diligence.

On January 10, 2020, Ascendium issued an audit closure notice stating ACPE met all requirements and officially closed the review.

US Department of Education Federal Family Education Loan (FFEL) Program Review

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. The focus of the review was to determine ACPE's compliance with the Higher Education Act (HEA) and applicable federal regulations and requirements in administering the FFEL program. FFEL servicers follow the regulatory requirements of FFEL Program regulations, 34 CFR 682. The review focused on Income Based Repayment (IBR), Servicemembers Civil Relief Act (SCRA) and military deferment benefit processing.

On October 22, 2019, ED issued a Program Review Report, which identified two findings.

3. **Late Notification and Incomplete Disclosure of IBR Renewal Letters.** During the review, it was identified IBR renewal letters were being sent outside the required window. The system parameters for generation of the letters were updated and text edits made to the renewal letter.

4. **Military Service Deferment Incorrectly Granted.** The review identified two borrowers for whom the military deferment was granted but to which they were not entitled. Procedures related to the eligibility determination were updated and the loans for the two borrowers were adjusted.

On March 11, 2020, ED issued a Final Program Review Determination reflecting one outstanding requirement.

1. **LaRS Borrower Level Detail.** Ed requested a borrower level detail of the December 31, 2019 LaRS report for the two military borrowers' accounts, which ACPE provided on March 13, 2020.

On May 6, 2020, ED issued an audit closure notice stating ACPE met all requirements and officially closed the review.