Alaska Commission on Postsecondary Education

Internal Audit Committee Meeting

April 26, 2023

Internal Audit Committee
Zoom Link
Meeting #: 891 4828 1484
Password: 824552
Teleconference: (888) 788-0099; Code: 891 4828 1484 #

Wednesday, April 26, 2022

1.	2:35 p.m.	Convene/Roll Call
2.*		Adoption of Agenda
3.*		Approval of Minutes of July 21, 2022 Meeting
4.		Annual Identity Theft Prevention Program Review – Quality Assurance Officer Jackie Hall
5.		Audit Updates – Quality Assurance Officer Jackie Hall
7.*		Establish Next Meeting Date Staff recommendation: April 2024 Commission meeting date
8.*	2:50 p.m.	Adjourn

***Action Required**

MINUTES OF THE
ALASKA COMMISSION ON POSTSECONDARY EDUCATION
INTERNAL AUDIT COMMITTEE MEETING
July 21, 2022

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 Thursday, July 21, 2022. Chair Joshua Bicchinella called the meeting to order at approximately 3:17 p.m.

ATTENDEES

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

Commission staff present for all or portions of the meeting: Sana Efird, Executive Director; Jackie Hall, Quality Assurance Officer; and Dannielle Erickson, Executive Secretary.

ADOPTION OF AGENDA

Member Adams moved to adopt the agenda of the July 21, 2022, Internal Audit meeting. Commission Chair Bicchinella seconded the motion. By roll call vote, all members present voted aye. The motion carried.

APPROVAL OF MINUTES

Corporation Chair Adams moved to approve the minutes from the April 8, 2021, Internal Audit Committee meeting as written. Commission Chair Bicchinella seconded the motion. By roll call vote, all members present voted aye. The motion carried.

Discussion: None

REPORTS

Identify Theft Prevention Program Review - Mrs. Hall presented her report starting on page 5 of the meeting packet on the agency's annual identity 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: *Corporation Chair Adams stated she thought the report was very thorough and she appreciated the information.*

Commission Chair Bicchinella stated he also appreciated the report and thought it was very thorough. He added that he is very pleased that routine cyber security training is a priority for Commission Staff. He asked if outside services have a third party audit their work or if it is done internally. Mrs. Hall explained that under the compliance requirements for maintaining an identity theft prevention program, they have to have an internal audit committee. Each entity provides a report internally of their program status

MINUTES OF THE
ALASKA COMMISSION ON POSTSECONDARY EDUCATION
INTERNAL AUDIT COMMITTEE MEETING
July 21, 2022

and any updates or changes that were made as well as an overview of the training they provide their staff. Once their report is completed, they provide that report to us.

Federal Family Education Loan Compliance Review - Mrs. Hall referenced her written report on page 14 of the meeting packet on several compliance reviews for the Commission's Federal Family Education Loans. Federal guarantors typically conduct biennial reviews of FFEL lenders. At this time, Ascendium had not reached out to schedule the next program review.

Discussion: *Commission Chair Bicchinella asked if there was any cause for concern for not hearing from them and if we should look into it. Mrs. Hall explained that the timeframe does vary and the prior review was extensive as well as a separate review from the Department of Education. There were also some changes with the review process, so that could have affected their timeline. She stated we should proactively reach out if we do not hear from them within 6 to 8 months. She concluded that she believes we are well within the timeline, so no cause for concern.*

Corporation Chair Adams asked what all the components are to the internal audit process. Mrs. Hall stated that she is not an internal auditor with the Commission and her role is to do ongoing compliance reviews of our program. The annual review is a requirement in state law for Identity Theft Prevention Programs, which is why it is built into the program. She does not have any direct oversite that she could outline for her. Ex-Officio Efird interjected that during the process for preparing for the audit, the Senior Managers work with General Managers to ensure all financial transactions are sound and the workflows have the proper oversite. She added that in the past there was an Internal Auditor position on the Commission Staff; however, it was deleted before she took over as Executive Officer. However, staff are going through and reviewing checks and balances.

Commission Member Head joined at this point and apologized for being late to the Internal Audit Committee Meeting. She stated that she did not have any questions for Mrs. Hall.

CLOSING COMMENTS

Ex-Officio Efird wanted to voice her deep appreciation for all the hard work that Quality Assurance Officer Jackie Hall has done. She stated that the workload Mrs. Hall has been managing is extensive and complex. She wanted to take the opportunity to let the Committee know what an amazing employee Mrs. Hall is and what a benefit she is to the Commission.

2023 MEETING DATE

Commission Chair Bicchinella moved to hold the next committee meeting on the same day as the regular April Commission meeting, which is scheduled for April 5, 2023. Corporation Chair Adams seconded the motion. By roll call vote, all members present voted aye. The motion carried.

MINUTES OF THE
ALASKA COMMISSION ON POSTSECONDARY EDUCATION
INTERNAL AUDIT COMMITTEE MEETING
July 21, 2022

ADJOURN

There being no further business to discuss, Commission Chair Bicchinella adjourned the meeting at approximately 3:45 p.m.

Alaska Commission on Postsecondary Education

Internal Audit Committee Meeting

April 26, 2023

Report Highlights

1. **Report: ACPE's Identity Theft Prevention Program**
   - Annual Program Review
   - Staff Training
   - Reports from ACPE's Third-party Servicers
2. **Report: Federal Family Education Loan (FFEL) Program Reviews through American Education Services (AES)**
   - Guarantor Review under the Common Review Initiative
   - Servicer Review by the U.S. Department of Education

Identity Theft Prevention Program

Alaska Commission on Postsecondary Education

Fair and Accurate Credit Transaction Act (FACT Act)

Red Flags Rules

Identify Red flags and incorporate into a written identity theft prevention program	**Detect** Red flags that have been incorporated into your program
Respond Appropriately to red flags that are detected	**Update** Program to reflect changes to risk and protect ACPE

Identity Theft Prevention Program (ITPP)

ACPE's ITPP was implemented in 2009 to address the threat of fraud and identity theft by:

- **Monitoring** daily activities to identify red flag indicators
- **Responding** to any red flag indicators or claims of identity theft
- **Preventing** and **mitigating** identity theft through
  - Staff education
  - Oversight & monitoring of third-party servicers
  - Annual review of the program to ensure its effectiveness

ITPP Annual Program Review

Considerations

1. ACPE's Past Experience with identity theft
2. Internal processes align with the programs red flag categories
3. Any changes to our covered programs
4. Any changes in business arrangements

Assessment

1. Reviewed the programs detection and response methods
2. Assess the effectiveness of those methods against any fraudulent activity during the review period
3. Review covered programs and any changes to servicing activities

ITPP Assessment Results

- **Detection & Response:** The methods used to identify and prevent identity theft are still applicable to the activities being performed
- **Covered Programs:** No new programs introduced or changes to existing covered accounts in 2022
- **Business Arrangements:** ACPE outsourced a portion of its servicing activities last year, which does represent a change in business arrangements

Housekeeping Changes

- **Section 1. Program Oversight and Administration:** Addition of appropriate and effective oversight of service providers.
- **Section 3. Identified Red Flags, subsection C. The presentation of suspicious personal identifying information**: changes include information sources used by either ACPE or its third-party servicers.
- **Section 6. Safeguards to Protect Customer Information:** Addition of subsection D. Service Provider Oversight and Risk Management Program.

ACPE Policy
Identity Theft Prevention Program

Quality Assurance 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;
- Exercise appropriate and effective oversight of service provider arrangements; and
- Report annually to the Internal Audit Committee regarding compliance with the program.

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

- Personal identifying information provided is inconsistent when compared against external information sources used by ACPE or its service providers;
- ACPE is notified by an internal or external source (ACPE staff, credit bureau, service provider, 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 another person on file with ACPE or its service providers;
- 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; or
- Personal identifying information provided is not consistent with personal identifying information on file with ACPE or its service providers.

D. **Service Provider Oversight and Risk Management Program**

- Contract oversight;
- Ensure service providers have reasonable policies, and procedures to detect, prevent, and mitigate the risk of identity theft;
- Annual reports on red flags detected, changes to Identity Theft Prevention Program, and any instances of identity theft; and
- Regular monitoring of activities in connection with one or more covered accounts.

Identity Theft Reports

- No reports of identity theft received in 2022
- A release of nonpublic personal information (NPI) through the filing of Assertion of Liens to Alaska's Recording Office
    - Social Security Number of four individuals was recorded and available through public records
    - The information could have been collected for unauthorized use to conduct fraudulent activity

Breach of Security

Alaska Personal Information Protections Act (APIPA)

Requires notification when a breach of security containing personal information occurs

Personal information consists of a combination of an individuals first and last name and one or more information elements:

- Social Security Number;
- Driver's license number;
- Bank account number, credit card number, or debit card number
- Personal security code, identification number or passwords to access financial accounts.

- ACPE provided written notification to each borrower, including:
  - Details of the incident
  - Information to obtain a free copy of their credit report
  - Ways to identify potential signs of identity theft
- ACPE notified the Department of Law, through the Assistant Attorney General
  - No additional action is required

Annual Staff Training

Educating staff about identity theft and the important role employees play in safeguarding personal and confidential information.

ACPE Privacy & Security

- The Red Flags Rule
- Identity Theft Prevention Program
- Protecting Nonpublic Personal Information
- Password Management
- Cybersecurity
- Teleworking Best Practices

SOA Cybersecurity Training

- Internet Security When you Work from Home
- Phishing: Don't Get Reeled In
- 2022 Social Engineering Red Flags
- Classic Danger Zone

Third-Party Servicers

ACPE Partners

- CampusDoor Holdings, Inc.
- Pennsylvania Higher Education Assistance Agency (PHEAA); conducting business as American Education Servicers (AES)
- Transworld Systems, Inc.

Third-Party Oversight

ACPE's role shits to oversight, ensuring our partners have processes in place to detect, prevent, and mitigate identity theft

- ACPE's partners are also subject to the Red Flags Rule and must implement an Identity Theft Prevention Program. Each agency must administer the program by:
  - Involving a board of directors, an appropriate committee, or a designated senior manager in oversight of the program
  - Provide training to staff
  - Exercise appropriate oversight of service provider arrangements
- Contractually, ACPE requires partners provide:
  - Current versions of program materials
  - Annual reports that highlight any changes to their Program, employee training, and any instances of identity theft or release of NPI on ACPE accounts

Annual Reports-ACPE Partners

- **CampusDoor Holdings, Inc.**
  - No incidents of identity theft or unauthorized release of nonpublic personal information
  - No material changes made to their ITPP
  - Annual all staff training conducted
- **Pennsylvania Higher Education Assistance Agency (PHEAA); conducting business as American Education Services (AES)**
  - No incidents of identity theft or unauthorized release of nonpublic personal information
  - No material changes made to their ITPP
  - Annual all staff training conducted
- **Transworld Systems, Inc.**
  - No incidents of identity theft or unauthorized release of nonpublic personal information
  - No material changes made to their ITPP
  - Annual all staff training conducted

QUESTIONS?

Alaska Commission on Postsecondary Education

Federal Family Education Loan Program Reviews

Guarantor Review – Common Review Initiative
Servicer Review – U.S. Department of Education

Alaska Commission on Postsecondary Education

Higher Education Act (HEA)

Federal regulations governing the Federal Family Education Loan Program require that participating lenders and servicers maintain complete and accurate records pertaining to loans made under the program.

- ACPE is the lender for the Federal Family Education Loans owned by the Alaska Student Loan Corporation (ASLC).
- April 1, 2020, ACPE outsourced the servicing of our FFELP portfolio to American Education Services (AES).
- As a federal loan servicer, AES is subject to federal audits and program reviews to ensure their compliance with the HEA.

ACPE Program Reviews

As a federal loan lender, ACPE worked directly with auditors throughout the review process and discussed findings and recommendations upon conclusion.

- Guarantor Review – Closed in January 2020
  - Period of May 1, 2017 – April 30, 2019
- U.S. Department of Education Review – Closed in May 2020
  - Period of October 1, 2014 – March 31, 2019

AES Program Reviews

AES services Federal Family Education Loan portfolios for multiple lenders; therefore, program reviews cover the services performed across multiple lenders.

- Current program reviews include a sample of ACPE loans in the selection criteria
- Auditors work directly with AES through the process.
- ACPE will be notified of any significant findings that require corrective action.

Guarantor Audit

Education Credit Management Corporation

Period of May 1, 2020 – April 30, 2022.

Upon conclusion, ACPE will receive an official report

Common Review Initiative

The scope of this review will examine processes including:

- Rehabilitated Loans;
- Income Based Repayment (IBR);
- Deferment and Forbearances;
- Servicing and Due Diligence;
- Claims;
- Cures;
- Electronic Signatures;
- Call Recordings;
- Purchases, Sale or Transfer of Loans; and
- LaRS

Servicer Audit

U.S. Dept. of Education

Period of March 31, 2020 – December 31, 2021.

ACPE will only be notified if there is a significant finding that requires corrective action.

U.S. Dept. of Education

The scope of this review will examine processes including:

- Cancer Treatment Deferment;
- Income Driven Repayment;
- Military Service Deferments;
- Military Service Grace;
- Lender Manifest through National Student Loan Data System (NSLDS); and
- Servicemembers Civil Relief Act of 2003

QUESTIONS?

Alaska Commission on Postsecondary Education

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, 2023
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 annually review its Program to evaluate its effectiveness in addressing the risk of identity theft and to ensure all aspects of the Program are applicable to the current business environment.

With the outsourcing of ACPE's loan origination activities to CampusDoor and the servicing of newly originated loans by American Education Services (AES), ACPE's role in detection, prevention and mitigation strategies shifts to third-party oversight, ensuring service providers have processes in place to detect, prevent and mitigate identity theft, and staffs monitoring activities for compliance. As a result of this transition, housekeeping changes were made to ACPE's Program to include activities performed by either ACPE or its service providers as well as the inclusion of service provider oversight and risk management.

Identity Theft Reports
No incidents of identity theft were reported in 2022; however, staff identified the release of nonpublic personal information (NPI) to Alaska's Recorder's Office as part of ACPE's filing of Assertion of Liens.

ACPE filed four Assertion of Liens with the State of Alaska's Recorder's Office that included the Social Security Number (SSN) instead of the borrower's reference number. While the SSN was not readily identified as such, by the fact it was presented in a 10-digit format with a leading

zero, it was still presented un-redacted for public consumption. It is reasonable to assume the information could have been collected for unauthorized use during the two-months the nonpublic information was published. Upon notification, the Recorder's Office removed the notices from public view and ACPE notified each borrower impacted, providing details of the incident and instructions on how to obtain a free copy of their credit report to identify potential signs of identity theft.

ACPE takes the privacy of personal information very seriously; our process of filing an Assertion of Lien is intended to prevent incidents such as this by using a 10-digit account number in place of the SSN. However, in the event of a release of personal information, ACPE is quick to review our processes and take corrective action when warranted. As required, ACPE reported this incident to the State of Alaska, Office of the Attorney General. No further action was requested or required by law.

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 2022:

SOA Cybersecurity Training

- Internet Security When you Work from Home – This course provided helpful tips for keeping safe online when working away from the office.
- Phishing: Don't Get Reeled In – This course explores phishing and answers the questions:
    - What is phishing?
    - How do hackers do this?
    - Why it's important to avoid phishing attacks.
- 2022 Social Engineering Red Flags - This course focused on helping employees learn how to spot the red flags or signs of danger associated with social engineering, including:
    - Why hackers deploy social engineering attacks;
    - The different types of attacks hackers use; and
    - What action(s) employees should and shouldn't take to protect themselves and the organization.

- Classic Danger Zone – This informative game teaches the tactics of cybersecurity and helps employees avoid the pitfalls of cyberattacks.

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.

Third-Party Service Provider Oversight

A key component 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.

ACPE outsourced the loan origination of its education loans to CampusDoor in 2022, with the implementation of its primary loan programs in April, followed by the specialty loan programs in August. Education loan applications are collected, processed and disbursed by CampusDoor and 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 annual report included confirmation of their established Program and employee training. CampusDoor's Program conforms to the provisions of FACTA and the FCRA and was approved by their internal Risk Management Committee in December 2022, with no changes. CampusDoor reported no incidents of identity theft for ACPE accounts in 2022.

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, approved by their internal Risk Management Committee in March 2022, with no changes to the Program. Additionally, PHEAA reported no incidents of identity theft for ACPE accounts in 2022.

Transworld Systems Inc.
Transworld Systems, Inc. (TSI) 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 and conforms to the provisions of FACTA and FCRA.

- 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 approved by their internal Risk Management Committee in 2022, with no changes to the Program. TSI reported no incidents of identity theft for ACPE accounts in 2022.

ACPE Policy
● 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 CFR 681.

EFFECTIVE DATE:
10/17/2022

TO BE USED BY:
ACPE staff and Internal Audit Committee

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 5

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. The Program 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).

Internal Audit Committee will:

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

Quality Assurance 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;
- Exercise appropriate and effective oversight of service provider arrangements; and
- Report annually to the Internal Audit Committee regarding compliance with the program.

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; and
- 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 or its service providers;
- ACPE is notified by an internal or external source (ACPE staff, credit bureau, service provider, 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 another person on file with ACPE or its service providers;
- 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; or
- Personal identifying information provided is not consistent with personal identifying information on file with ACPE or its service providers.

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 or its service provider is notified the customer is not receiving account statements as expected;
- ACPE or its service provider is notified of unauthorized transactions in connection with a customer's covered account
- ACPE or its service provider 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; or
- 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:

- 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; or
- Determine no response is needed under the particular circumstances.

Address Discrepancies

The Program includes a process 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 or its service provider 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 including 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. **Service Provider Oversight and Risk Management Program**
- Contract oversight;
- Ensure service providers have reasonable policies, and procedures to detect, prevent, and mitigate the risk of identity theft;
- Annual reports on red flags detected, changes to Identity Theft Prevention Program, and any instances of identity theft; and
- Regular monitoring of activities in connection with one or more covered accounts.

E. **Incident Response and Reporting**

F. **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 15, 2023
Subject: 2022 Federal Family Education Loan Program Review

Federal regulations governing the Federal Family Education Loan Program (FFELP) require that participating lenders maintain complete and accurate records pertaining to the loans made under the program. American Education Services (AES) is ACPE's third-party servicer for the FFELP portfolio owned by the Alaska Student Loan Corporation. As a third-party servicer, AES is subject to federal audits and program reviews to ensure their compliance with the Higher Education Act (HEA) and applicable federal regulations and requirements in administering the program. These reviews are not specific to any one lender, but instead cover the services performed by AES for some or all lenders, depending on the type of audit being conducted and the scope of review requested.

Guarantor Federal Family Education Loan (FFEL) Program Review

Guarantors are charged under 34 CFR 682.410(c) with the responsibility to ensure institutional compliance by conducting comprehensive biennial reviews of lenders or servicers. Federal guarantor, Educational Credit Management Corporation (ECMI), is leading a Common Review Initiative (CRI) program review, which is performed by a group of guarantors for a designated group of lenders. The CRI is a U.S. Department of Education lender review process where participating guarantors cooperate to conduct reviews by sharing staff and costs to reduce the number of redundant reviews while simultaneously improving the overall quality of reviews.

ECMI is currently conducting a program review that includes a sample of loans owned by the Alaska Student Loan Corporation. The review covers the period of May 1, 2020, through April 30, 2022, and the scope of this review will examine the following processes:

- Rehabilitated loans;
- Income Based Repayment (IBR);
- Deferment and Forbearance;
- Servicing and due diligence;

- Claims;
- Cures;
- Electronic signatures;
- Call recordings;
- Purchases, sale or transfer of loans; and LaRS loan level detail, including adjustments.

This program review has not been closed and no audit findings have been reported to date. Because this review includes multiple lenders, CRI will discuss any findings and recommendations with AES. ACPE will be notified if there is a significant finding that requires corrective action.

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

The US Department of Education (ED) is currently conducting a program review of AES as a third-party servicer. The focus of the review is to determine AES's compliance with the Higher Education Act (HEA) and applicable federal regulations and requirements in servicing the FFEL Program. This program review covers the period of March 31, 2020, through December 31, 2021, and includes a sample of loans owned by the Alaska Student Loan Corporation. The scope of this review includes, but is not limited to the following:

- Cancer Treatment Deferment;
- Income Driven Repayment;
- Military Service Deferments;
- Military Service Grace;
- National Student Loan Data Systems (NSLDS) Lender Manifest; and
- Servicemembers Civil Relief Act of 2003.

This program review has not been closed and no audit findings have been reported to date. Because this review includes multiple lenders, ACPE will only be notified if there is a significant finding that requires corrective action.