Alaska Commission on Postsecondary Education

PROVIDING EDUCATION & CAREER FUNDING SOLUTIONS

Internal Audit Committee Meeting

April 2, 2026

ALASKA COMMISSION ON POSTSECONDARY EDUCATION

Internal Audit Committee
Zoom Link
Meeting #: 885 8261 9421
Password: ACPE
Teleconference: 1 (888) 788-0099; Code: 885 8261 9421 #

AGENDA

April 2, 2026

1.	**3:10 P.M.**	Convene/Roll Call
2.		Adoption of Agenda ➢ *Suggested motion: move to adopt the agenda of the April 2, 2026 Internal Audit Committee Meeting.*
3.		Approval of Meeting Minutes from April 8, 2025 Internal Audit Committee Meeting ➢ *Suggested Motion: move approval of the meeting minutes from the April 8, 2025 Internal Audit Committee Meeting.*
4.		Annual Identity Theft Prevention Program Review – Jackie Hall, Program Manager
5.		Audit Updates – Jackie Hall, Program Manager
6.		Establish Next Meeting Date Staff Recommendation: April 2027 Commission Meeting
7.	**3:40 P.M.**	Adjournment ➢ *Suggested Motion: Move the Commission adjourn the April 2, 2026 Internal Audit Committee Meeting.*

*Action Required

MINUTES OF THE
INTERNAL AUDIT COMMITTEE

ALASKA COMMISSION ON POSTSECONDARY EDUCATION
April 8, 2025

A meeting of the Internal Audit Committee was held on Wednesday, April 8, 2025 in the ACPE office conference room at 3030 Vintage Boulevard in Juneau, Alaska. The meeting convened at 3:00 p.m.

ATTENDEES

Members participating: Josh Bicchinella, Corporation Chair; John Brown, Commission Chair; and Brittany Williams, Commission Member.

Members absent: Kerry Thomas, Acting Executive Director (ex-officio).

Staff participating: Andrew Bocanumenth, Assistant Attorney General; Jackie Hall, Program Manager; Grace Newman, Administrative Assistant; and Katrina Skidmore, Administrative Assistant.

ADOPTION OF AGENDA

Commission Chair Brown moved to adopt the agenda as written. Commissioner Williams seconded the motion. Members unanimously adopted the agenda without change.

MINUTES FOR APPROVAL

Commission Chair Brown moved to adopt the April 26, 2023 minutes as written. Commissioner Williams seconded the motion. The minutes were unanimously approved without change.

REPORTS

Identify Theft Prevention Program Review - Jackie Hall, Program Manager, presented a two-year update on ACPE's Identity Theft Prevention Program, covering calendar years 2023 and 2024, in compliance with the federal Red Flags Rule. ACPE's program, in place since 2009, continues to focus on identifying, detecting, and mitigating identity theft through daily monitoring, staff training, annual program reviews, and oversight of third-party servicers.

Annual reviews for both years found the program to be effective and aligned with ACPE's operations, with no material changes required and no identity theft reports received from the public. Staff completed required annual privacy and cybersecurity training, coordinated with State of Alaska training, and third-party servicers confirmed compliance, training completion, and no identity theft incidents involving ACPE accounts.

While no identity theft was reported, several security incidents involving personal information were identified in 2023 and 2024. These incidents—including data shared during wage garnishment processes, a national data transfer breach affecting a small number of ACPE borrowers, a lien filing issue, misdirected mail, and an email masking error by a collection vendor—were investigated,

reported as required under state and federal law, mitigated promptly, and assessed as low risk to affected individuals. No ongoing issues or consumer complaints were reported.

Discussion: Chair Brown asked whether any comparative data exists showing how Alaska's identity theft or security breach rates compare to those of other states, given Alaska's smaller borrower population. Program Manager Hall responded that she is not aware of any comprehensive national data that allows for state-by-state comparisons of breach rates. She noted that differences in state and federal reporting laws, notification thresholds, and disclosure requirements make meaningful comparisons difficult, and that breach information is typically reported individually rather than aggregated into a national dataset.

Guarantor Federal Family Education Loan (FFEL) Program Review

Program Manager Hall presented a report on Federal Family Education Loan Program (FFELP) guarantor reviews conducted through American Education Services (AES) during the two-year reporting period. She explained that federal regulations require lenders and servicers to maintain accurate loan records and that guarantor agencies conduct biennial compliance reviews under the Common Review Initiative, a collaborative process in which guarantors share staff and resources to perform reviews collectively.

Program Manager Hall reported on a completed guarantor review covering May 1, 2020, through April 30, 2022, which included testing of 51 lenders and 307 borrower files, including a sample of ACPE loans. While the review identified findings for certain lenders, none of the findings impacted ACPE loans. After all applicable issues were addressed, the guarantor team closed the review on February 13, 2024.

She also reported on a second guarantor review that is currently in progress, covering the period from May 1, 2022, through April 30, 2024. The review team remains in the testing phase, and details regarding the loan sample and any findings are not yet available. Program Manager Hall indicated that results from this review will be included in a future update once the review is complete.

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

Program Manager Hall reported that American Education Services (AES) underwent a U.S. Department of Education program review covering the period from March 31, 2020, through December 31, 2021. ACPE loans were included in the review sample; however, no findings impacted ACPE. Any findings identified were confidential between the Department of Education and AES.

Program Manager Hall stated that AES addressed all findings identified by the Department of Education, and the review was officially closed on May 6, 2024. She noted that, unlike guarantor reviews, Department of Education program reviews do not follow a set schedule, and there is no information at this time regarding any upcoming federal reviews.

2026 Meeting Date

Commission Chair Brown moved to hold the next Internal Audit Committee meeting in conjunction with the Quarterly Commission Meeting for April 2026, dates to be determined. Corporation Chair Bicchinella seconded the motion. The members unanimously agreed.

Discussion: Chair Brown asked whether the motion needed to specify an exact date and sought clarification from legal counsel. Assistant Attorney General Andrew Bocanumenth confirmed that the motion was appropriate as stated and explained that it provides flexibility to schedule the committee meeting during the same week as the Quarterly Meeting once dates are finalized. He affirmed that no specific date was required at this time.

Adjourn

Commission Chair Brown moved to adjourn. Corporation Chair Bicchinella seconded the motion. The members unanimously agreed. The meeting adjourned at 3:36 p.m.

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

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

MEMORANDUM

To: Members, Internal Audit Committee
Through: Kerry Thomas, Executive Director
From: Jackie Hall, Program Manager
Date: February 25, 2026
Subject: Identity Theft Prevention

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 implement an Identity Theft Prevention Program designed to detect the warning signs, or red flags, of identity theft in its day-to-day operations.

ACPE implemented its Identity Theft Prevention Program (Program) in 2009, which includes policies and procedures designed to identify, detect, and respond to potential identity theft threats. Under the Program oversight and administration requirements, staff:

- Annually review the Program to evaluate its effectiveness in addressing the risk of identity theft;
- Implement approved changes to the Program;
- Provide annual training to educate staff about identity theft, Red Flags, and other important privacy and security topics;
- Exercise appropriate and effective oversight of service provider arrangements and
- Report annually regarding compliance with the Program.

The following report covers compliance activities for 2025.

Program Evaluation

When evaluating the Program, staff consider our experience with identity theft, any changes to the covered accounts under the Program, modifications in business arrangements with third-party providers, and advancements in technology that might introduce new red flags. Staff reviews the detection and response methods and assesses their effectiveness against any fraudulent activities that may have occurred during the review period. Additionally, they ensure that internal processes align with the existing red-flag categories and recommend changes to the Program as needed.

2025 Program Review

- **Detection & Response:** The methods used to identify and prevent identity theft were applied effectively throughout the activities performed in 2025.
- **Covered Programs:** No new covered accounts or changes made to existing covered accounts in 2025.
- **Business Arrangements:** There were no modifications to business arrangements in 2025.
- **Identity Theft:** ACPE received no reports of identity theft in 2025.
- **Program Changes:** Staff recommended no material changes to the Program in 2025.

Employee Training

In 2009, ACPE launched its annual all-staff training program to equip staff with vital skills in detecting and preventing identity theft. This training covers the Red Flags Rule and Identity Theft Prevention and guides staff in detecting, preventing, and responding to red flags and reports of potential identity theft. Annual privacy and security training has since expanded to include other important security topics, prevention measures, and best practices, helping employees understand their role in protecting personal and confidential information.

In 2019, the State of Alaska (SOA) Office of Information Technology (OIT) launched its security awareness training program as part of an ongoing effort to foster a culture of cybersecurity awareness.

Through this annual training, staff reinforce their knowledge and commitment to protecting personal information, thereby strengthening the organization's security posture.

2025 Privacy & Security Training

ACPE staff completed the following training in 2025.

SOA Annual Cybersecurity Training

Quarter 1:

- Acceptable Use Policy; and
- Survey to understand Cybersecurity Weaknesses.

Quarter 2:

- 2025 KnowBe4 Security Awareness Training;
- Reporting Security Incidents; and
- Security Snapshots.

Quarter 3:

- Password Trivia;
- How to Create Strong Passwords Quiz;
- Security Awareness Training; and
- Security Snapshots on Passwords.

Quarter 4:

- Security Awareness Proficiency Assessment;
- Links and Attachments; and
- Safe Web Surfing.

ACPE Annual Training Topics

- ACPE security measures;
- Working remotely and traveling best practices;
- Protecting personal information;
- The Red Flags Rule;
- ACPE's Identity Theft Prevention Program;
- Security breach protocols.

Security Incidents

ACPE ensures compliance with state and federal laws governing the protection of customer information. Protected customer information is generally any information about a person that is not publicly available and may be protected from disclosure by state and federal law. ACPE and its service providers guard against the inadvertent release of nonpublic personal information (NPI) by ensuring that NPI is properly transmitted, stored, and disposed of.

2025 Security Incidents

The following is a list of security incidents involving nonpublic personal Information for ACPE accounts.

Notice Date: 6/24/2025

- **Event Summary:** A bankruptcy notice was mailed to ACPE but delivered to the Juneau Chamber of Commerce, occupier of ACPE's previous physical location. A Chamber staff member opened the notice and, upon realizing they were not the intended recipient, delivered the notice to ACPE.
- **Investigation Results:** The bankruptcy document contained the cosigner's name but only the last four (4) of their SSN, which does not meet the definition of personal information constituting a breach under state and federal law.
- **Notice Requirements:** None.

Notice Date: 8/19/2025

- **Event Summary:** An Administrative Wage Garnishment (AWG) check from an employer was mailed to ACPE, but misrouted within the State of Alaska mail system and delivered to the Department of Environmental Conservation by mistake.
- **Investigation Results:** The check and enclosed documentation included the name and SSN of the affected borrower, which meets the definition of personal information constituting a breach under state and federal law.
- **Notice Requirements:** According to AS 45.48.010(c), ACPE notified Allison Baldock, Assistant Attorney General. No further action is required.

Notice Date: 12/30/2025

- **Event Summary:** An Administrative Wage Garnishment (AWG) termination order was emailed by ACPE to the email address of the employer's contact person listed on the Department of Labor and Workforce Development's Secure Access Manager (SAM) system. This individual subsequently notified ACPE that they are no longer the owner of or affiliated with the business in question.
- **Investigation Results:** The AWG termination order included the borrower's name but only the last four (4) of their SSN, which does not meet the definition of personal information constituting a breach under state and federal law.
- **Notice Requirements:** None.

Third-Party Service Provider Oversight

ACPE monitors its service providers' activities to ensure compliance with the Red Flags Rule. Contractually, ACPE requires third-party servicers who provide services directly to and on behalf of ACPE to maintain an Identity Theft Prevention Program and to submit annual compliance reports that include any instances of identity theft identified within the reporting period. These reports are

an essential component of ACPE's third-party risk management program and serve to ensure that service providers are actively monitoring and addressing potential threats to sensitive and confidential information.

CampusDoor Holdings Inc.

In 2022, ACPE outsourced the origination of its state education loan programs to CampusDoor. CampusDoor administers the application process, disburses funds to the school, and then transfers the loan to American Education Services (AES) for ongoing servicing.

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.

2025 Annual Report

CampusDoor's annual compliance report included the following:

- **Program materials:** Documented Program review approved by Risk Management. The Program conforms to the requirements of FACTA and FCRA. CampusDoor made updates to OFAC retention requirements, as approved by its Risk Committee, and to the language and formatting of its program in 2025.
- **Annual staff training:** CampusDoor requires all consumer-facing employees to complete annual compliance training on Identity Theft and Fraud Prevention. Staff completed training by 11/7/2025.
- **Identity Theft:** No reported cases of identity theft for ACPE accounts and no records of an identity theft or fraud complaint for ACPE.
- **Breach:** No instances of a breach occurred for ACPE accounts in 2025.

Pennsylvania Higher Education Assistance Agency (PHEAA)

PHEAA, conducting business as American Education Services, is ACPE's third-party servicer for its state and federal education loan programs. ACPE outsourced the servicing of its FFELP portfolio in 2020, followed by its state education loan programs in 2022 and 2023.

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).

2025 Annual Report

PHEAA's annual compliance report included the following:

- **Program materials:** Documented Program review approved by the PHEAA Board of Directors in April 2025. The Program conforms to the requirements of FACTA and FCRA. PHEAA made no material changes to its program in 2025.
- **Annual staff training:** PHEAA conducts annual training introducing the FCRA, Red Flags Rule requirements, and staff responsibilities related to the Identity Theft Detection, Prevention, and Mitigation Program. Staff completed training by October 31, 2025.

- **Identity Theft:** No reported cases of identity theft for ACPE accounts and no records of an identity theft or fraud complaint for ACPE.
- **Breach:** No instances of a breach occurred for ACPE accounts in 2025.

Transworld Systems Inc.

Transworld Systems, Inc. (TSI) is ACPE's third-party collection vendor for its defaulted state 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 harm to the consumer; and
- Perform an annual evaluation of the Program based on reports of current Fraud and Identity Theft practices, make corresponding updates as needed, and update training materials to help ensure the relevance and effectiveness of the Program.

2025 Annual Report

TSI's annual compliance report included the following:

- **Program materials:** Documented Program review approved by the Chief Legal and Compliance Officer in February 2025. The Program conforms to the requirements of FACTA and FCRA. TSI updated sections: State Law, Client and Company Standard for Compliance, and Non-substantive updates.
- **Annual staff training:** TSI's compliance training is an enterprise-wide learning solution that promotes awareness of and adherence to Federal, state, and Local Laws, client guidelines, company policy, and procedures.
- **Identity Theft:** No reported cases of identity theft for ACPE, and no records of an identity theft or fraud complaint for ACPE.
- **Breach:** No instances of a breach occurred for ACPE accounts in 2025.

ACPE Procedure
• 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 existing covered account and to provide continued administration of the program.

EFFECTIVE DATE:
6/11/2024

TO BE USED BY:
ACPE staff and Internal Audit Committee

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. 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 Procedure
• Identity Theft Prevention Program

Supporting Documentation

Guide

- Red Flags Guide

Procedure

- Responding to a Report of Identity Theft
- Security Breach: Incident Identification

Training

- Privacy and Security Training and Awareness

Does a third party need to receive a copy of any of the above documents? Yes

ACPE's Identity Theft Prevention Program

1. Program Oversight and Administration

The Internal Audit Committee provides oversight of ACPE's Red Flags Program. Operational implementation of the Program and training has been delegated to Program Management.

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.

Program Management 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 the 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.

ACPE Procedure
• Identity Theft Prevention Program

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 an 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**
   - Procedures for responding to red flag reports, identity discrepancy, high-risk address, fraud, and military active duty alerts.

C. **Incident Response and Borrower Notification**
   - Customer Identity Theft Letter and Affidavit
   - Procedure when handling customer reports of potential identity theft
   - Procedure for processing forgery and fraud claim forms
   - Guide on handling allegations of loan forgery and fraud
   - Guide on ACPE's Red Flags and staff responsibilities

ACPE Procedure
• Identity Theft Prevention Program

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

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

MEMORANDUM

To: Members, Internal Audit Committee
Through: Kerry Thomas, Executive Director
From: Jackie Hall, Program Manager
Date: February 12, 2026
Subject: Federal Family Education Loan Program Reviews

Federal regulations 34 C.F.R. Part 682, governing the Federal Family Education Loan Program (FFELP), require participating lenders and servicers to maintain complete and accurate records of loans made under the program.

Guarantors are charged under 34 C.F.R. 682.410(c) to ensure institutional compliance by conducting comprehensive biennial program reviews under the Common Review Initiative (CRI) guidelines. The CRI is a Department of Education-approved lender review process in which participating guaranty agencies cooperate to conduct reviews by sharing staff and costs, using CRI procedures.

The Pennsylvania Higher Education Assistance Agency, operating as American Education Services (AES), is the Commission's dedicated third-party servicer for the FFELP portfolio owned by the Alaska Student Loan Corporation (ASLC). As a federal loan servicer, AES is subject to rigorous federal audits and program reviews to ensure compliance with the Higher Education Act and relevant federal regulations. These program reviews are not limited to any specific lender; they assess the services AES provides to some or all lenders, depending on the audit's type and scope.

Program Reviews under the Common Review Initiative

CRI Program Review 2024-2025

The CRI team conducted a program review beginning in July 2024 that included a sample of ASLC-owned loans. This review covered the period of May 1, 2022, through April 30, 2024. A total of 275 borrower files were tested by the guarantor review team, and the scope of this review examined 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

The CRI reported the findings directly to AES on April 29, 2025, and ACPE was provided a copy of the report on May 20, 2025. The report included the following aggregate findings from the review; however, none of these findings included ASLC loans. AES is responsible for responding to the report and any corrective action noted within. The CRI Program Review was closed on July 17. 2025.

- Deferments
  - *29 borrower files tested. No findings*
- Forbearance and Call Monitoring
  - *29 Borrower files tested. No findings*
  - *10 borrowers tested for call monitoring. No findings*
- Collection Due Diligence, Cures, and Claim Reimbursement
  - 29 borrower files tested. No findings
- LaRS Detail
  - *70 borrower files tested. No findings*
- Purchases, Sales, and Transfers
  - *29 borrower files tested. No findings*
- Income-Based Repayment (IBR)
  - *29 borrower files tested. No findings*
- LaRS Adjustments
  - *29 borrower files tested. No findings*
- Rehabilitated Loans
  - *21 borrower files tested. One finding and one observation*

U.S. Department of Education Program Review

ED Program Review 2022-2024

The U.S. Department of Education (ED) conducts periodic program examinations to ensure lenders and servicers meet program requirements. The last program review covering the period of March 31, 2020, through December 31, 2021, was closed on May 6, 2024. As of the date of this report, AES has not been notified of an upcoming review.

Alaska Commission on Postsecondary Education

Internal Audit Committee Meeting

April 2, 2026

Identity Theft Prevention

- Annual Program Review
- Staff Training
- Annual Reports from Business Partners

Fair and Accurate Credit Transaction Act (FACTA)

Red Flags Rule

Identify Red flags and incorporate into a written identity theft prevention program	**Detect** Red flags that have been incorporated into the program
Respond Appropriately to red flags that are detected	**Update** The program based on operational changes and emerging risks

Identity Theft Prevention Program

ACPE's Identity Theft Prevention Program (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 red flag indicators or claims of identity theft
- **Preventing** and **mitigating** identity theft through
  - Staff education
  - Annual review of the program to ensure its effectiveness
  - Oversight & monitoring of third-party servicers

ITPP Annual Program Review

Considerations

1. ACPE's experience with identity theft
2. Any changes to ACPE's programs
3. Any changes in business arrangements
4. Advancements in technology

Assessment

1. Review the program's 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

Annual Assessment

2025 Program Review

- **Detection & Response:** The methods used to identify and prevent identity theft were applied effectively throughout the activities performed in 2025
- **Covered Programs:** No new covered accounts or changes made to existing covered accounts
- **Business Arrangements:** There were no modifications to business arrangements in 2025
- **Identity Theft:** ACPE received no reports of identity theft
- **Program Changes:** No material changes were made to the existing program

Annual Staff Training

In 2009, ACPE implemented mandatory all-staff training to equip staff with the knowledge and skills needed to address the threat of fraud and identity theft.

ACPE Privacy & Security Topics

- ACPE security measures
- Working remotely and traveling best practices
- Protecting personal information
- The Red Flags Rule
- ACPE's Identity Theft Prevention Program
- Security breach protocols

Annual Staff Training

SOA Cybersecurity Topics

Quarter 1:

- Acceptable Use Policy
- Survey to understand Cybersecurity Weaknesses

Quarter 2:

- 2025 KnowBe4 Security Awareness Training
- Reporting Security Incidents; and
- Security Snapshots

Quarter 3:

- Password Trivia
- How to Create Strong Passwords Quiz
- Security Awareness Training
- Security Snapshots on Passwords

Quarter 4:

- Security Awareness Proficiency Assessment
- Links and Attachments
- Safe Web Surfing.

Security Incidents

A breach of security involving personal information

Breach of Security

Alaska Personal Information Protection Act (APIPA)

The Alaska Personal Information Protection Act, AS 45.48, became law on July 1, 2009.

APIPA provides several protections for personal information including:

- Requiring entities to notify customers if there is a breach of personal information;
- Granting customers the ability to put a freeze on their credit report for security;
- Restrictions on the use of social security numbers;
- Regulations pertaining to the disposal of records containing personal information;
- Allowing victims of identity theft to petition the court for a determination of factual innocence, and
- A requirement of truncated payment card information on sales receipts.

ACPE complies with all state and federal laws governing the protection of personal information.

Breach of Security

Alaska Personal Information Protection Act (APIPA)

- "Breach of security" means the unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector.

- "Personal information" means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of
  - An individual's first name, or first initial, and last name; and
  - One or more of the following information elements:
    - The individual's social security number;
    - The individual's driver's license number or state identification card number;
    - The individual's account number, credit card number, or debit card number; and
    - Passwords, personal identification numbers, or other access codes for financial accounts.

Breach of Security

Bankruptcy Notice

Notice Date:
June 24, 2025

Investigation Results:
The information contained the full name and truncated Social Security Number (SSN).

Did a Brach Occur?
No

Notification:
Not required

Incident Summary

A bankruptcy notice was mailed to ACPE but delivered to the Juneau Chamber of Commerce, occupier of ACPE's previous physical location.

A Chamber staff member opened the notice and, upon realizing they were not the intended recipient, delivered the notice to ACPE.

Investigation Outcomes

The bankruptcy document contained the cosigner's name but no other identifiable elements. The SSN was truncated to the last four digits; therefore, this was not a breach under APIPA.

Breach of Security

Wage Garnishment

Notice Date:
August 19, 2025

Investigation Results:
The information contained the full name and Social Security Number (SSN).

Did a Brach Occur?
Yes

Notification:
Notification sent to Assistant Attorney General.

Incident Summary

An Administrative Wage Garnishment (AWG) check from an employer was mailed to ACPE, but misrouted within the State of Alaska mail system and delivered to the Department of Environmental Conservation.

Investigation Outcomes

The check and enclosed documentation included the name and SSN of the affected borrower, which meet the definition of personal information constituting a breach under APIPA and necessitate reporting requirements under AS 45.48.010(c).

Breach of Security

Wage Garnishment

Notice Date:
December 30, 2025

Investigation Results:
The information contained the full name and truncated Social Security Number (SSN).

Did a Brach Occur?
No

Notification:
Not required

Incident Summary

An Administrative Wage Garnishment (AWG) termination order was emailed by ACPE to the employer's email address listed in the Department of Labor and Workforce Development's Secure Access Manager (SAM) system. The individual subsequently notified ACPE that they are no longer the owner of or affiliated with the business in question.

Investigation Outcomes

The AWG termination order included the borrower's name but no other identifiable elements. The SSN was truncated to the last four digits; therefore, this was not a breach under APIPA.

Third-Party Service Providers

- **CampusDoor Holdings, Inc.**
  Loan Originations
- **American Education Services (AES)**
  Loan Servicing
- **Transworld Systems, Inc.**
  Default Collections

2025 Business Partner Reports

CampusDoor Holdings, Inc.

- Documented Program review approved by Risk Management. CampusDoor made a few minor updates to its program, which was approved by its Risk Management Committee
- Annual staff training conducted by all consumer-facing employees by November 7, 2025
- No reported cases of identity theft for ACPE accounts, and no records of identity theft or fraud complaints

Pennsylvania Higher Education Assistance Agency (PHEAA)

- Documented program review approved by the PHEAA Board of Directors. No material changes were made to their program
- Annual staff training for all employees completed by October 31, 2025
- No reported cases of identity theft for ACPE accounts, and no records of identity theft or fraud complaints

Transworld Systems, Inc.

- Documented program review approved by the Chief Legal and Compliance Officer. No material changes were made to their program
- Annual staff compliance training completed by the end of 2025
- No reported cases of identity theft for ACPE accounts, and no records of identity theft or fraud complaints

Oversight and Monitoring

Risk Management

Third-party oversight is a risk management practice that ensures external partners comply with applicable requirements, manage risks appropriately, and deliver services that meet established performance and quality standards. Potential outsourcing risks can include:

- Reputational risk;
- Operational risk;
- Transaction risk;
- Financial risk;
- Privacy & Security risk; and
- Regulatory compliance risk.

ACPE's third-party oversight and monitoring program provides a structured risk management framework that allows staff to assess, manage, and mitigate risks associated with our servicing partners while ensuring the services delivered on ACPE's behalf meet required operational, compliance, and quality expectations.

Oversight and Monitoring

ACPE's risk management program and oversight framework includes key topics and tasks for monitoring critical activities conducted by ACPE's third-party partners. These topics include agency security measures, contracts and servicing agreements, reporting and reconciliation, loan origination, servicing, and collection activities, and performance standards.

Contracts & Security

- Annual Audited Financial Statements
- Annual Fees
- Business Continuity and Disaster Recovery
- System and Organization Controls

Reporting & Reconciliation

- Invoices and Billing
- Monthly Transaction Reconciliation
- Interest Rate & Interest Subsidy
- Borrower Benefits

Loan Origination, Servicing, and Collection Activities

- Loan Eligibility and Disbursement Processing
- Loan Repayment Activities
- Delinquency Monitoring and Intervention
- Special Program Activities

Performance Standards

- Customer Complaints and Appeals
- Call Center Statistics
- Call Monitoring

Questions?

Federal Family Education Loan Program Reviews

- Guarantor Review
- U.S. Department of Education Review

Higher Education Act (HEA)

Federal Family Education Loan Program

Federal regulations governing the FFEL Program require participating lenders and servicers to maintain complete and accurate records of loans made under the program.

- Under the Higher Education Act, Guarantors ensure institutional compliance by conducting biennial program reviews under the Common Review Initiative (CRI) guidelines.
- The CRI is a lender review process where participating guaranty agencies conduct reviews together by sharing staff and costs.
- These reviews assess the services AES provides for a sample of loans across some or all lenders, depending on the scope of the audit conducted.

Federal Guarantor Review

Common Review Initiative (CRI) 2024-2025

Conducted by Ascendium Education Solution

Review Period:
July 20, 2024 – March 14, 2025

Program Period:
May 1, 2022 – April 30, 2024

Report Issued:
May 20, 2025

Lender Notification:
No loans identified in the list of findings were held by ASLC/ACPE

Status:
Closed July 17, 2025

The guarantor team tested 275 borrower files across 43 lenders, including a sample of ACPE loans. **ACPE was not affected by the following findings.**

1. **Deferments**
   29 borrower files tested - No finding
2. **Forbearance and Call Monitoring**
   29 borrower files tested - No findings
   10 borrowers tested for call monitoring. No findings
3. **Collection Due Diligence, Cures, and Claim Reimbursement**
   29 borrower files tested - No findings
4. **LaRS Detail**
   70 borrower files tested - No findings
5. **LaRS Adjustments**
   29 borrower files tested – No findings
6. **Purchases, Sales, and Transfers**
   29 borrower files tested - No findings
7. **Income-Based Repayment (IBR)**
   29 borrower files tested - No findings
8. **Rehabilitated Loans**
   21 borrower files tested - One finding

Federal Servicer Review

U.S. Dept. of Education 2022-2024

Review Date:
Early 2022

Program Period:
March 31, 2020 – December 31, 2021

Report Issued:
AES received a confidential report of findings.

Lender Notification:
April, 18, 2024, AES reported they were taking steps to address findings. ACPE was not affected by any findings.

Status:
Closed May 6, 2024

The scope of this review examined processes including:

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

As of the date of this report, AES has not been notified of an upcoming program review.

Federal Loan Program Reviews

Questions?

Thank You

Jackie Hall, Program Manager and Privacy Officer

Jackie.hall@alaska.gov

907-465-6692

April 2027

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Thank you for your time!

Mailing Address

PO Box 110505
Juneau, AK 99811

Email

Eed.acpe-execdirector@alaska.gov

marie.bates@alaska.gov

Phone number

(907) 465-6740