2204-PR1: Fraud Prevention and Identity Verification Procedures

Associated Policy: 2204: Student Aid Fraud Prevention and Identity Verification
Effective Date: 2026/03/20
Date of Latest Revision: 12/1/2025
Approved by: the Fraud Prevention Committee
These procedures will be reviewed annually by the Fraud Prevention Committee.

POLICY STATEMENT

The purpose of the Fraud Prevention and Identity Verification Policy is to protect the integrity of Utah State University's student financial aid, enrollment, and student account processes by preventing, detecting, and responding to fraudulent activity. This includes ensuring that all aid awarded, disbursed, and reported is made only to legitimate, eligible students whose identities have been verified in compliance with federal, state, and institutional requirements.

PURPOSE

This procedure outlines the steps to support the institutional standards for identity verification, fraud monitoring, data safeguarding, and reporting obligations outlined in Policy 2204.

DEFINITIONS

Definitions in this Procedure shall be as set forth in Policy 2204 and as outlined below.

1. Identity Verification

- **Initial Screening**: All applications are reviewed during onboarding for accuracy, consistency, and potential indicators of identity misuse.
    - Admissions screens demographic information, transcripts, prior schools, and application data for anomalies (duplicate addresses, suspicious emails, inconsistent dates, etc.). Admissions documents concerns in RHACOMM (FRAUD) and notifies the Federal Aid Team.
    - IT Security monitors IP addresses, device/browser fingerprints, and login patterns and notifies the Federal Aid Team when anomalies match fraud indicators.
    - Federal Aid Team reviews all flags received and determines whether identity verification is required. Federal Aid places the IDVREQ hold in Banner and documents the reason in RHACOMM (FRAUD).

- **Verification Methods:** Identity must be verified before the student receives any federal, state, institutional, donor-funded, or private aid.
  Acceptable methods:
    - In-person verification with original government-issued photo ID (Federal Aid verifies and records).
    - Remote secure verification through USU's approved third-party vendor.
    - V4/V5 FAFSA verification following FSA Handbook requirements, including collecting the Statement of Educational Purpose. Federal Aid updates RRAAREQ/RNAVR screens and maintains documentation.

- Registrar may verify identity when updating certain academic records and reports unusual academic activity patterns to Federal Aid.

- Admissions provides supplemental information from the original application if questions arise during identity review.

- **Academic Activity Confirmation:**
  Before Title IV disbursement, documented academic activity is required.
  - Registrar confirms activity (assignment submission, quiz, graded interaction).
  - Federal Aid reviews non-attendance reports, resolves conflicting information, and stops/pulls back aid if activity is not confirmed.
  - IT Security provides login data if activity appears suspicious or inconsistent with student location/device history.

- **Failure to Complete Identity Verification:**
  If a student does not complete required identity verification:
  - Federal Aid rejects the ISIR if applicable, suspends packaging/disbursement, or pulls back aid already disbursed.
  - Admissions may cancel admission if identity cannot be confirmed.
  - Registrar may cancel registration for students unable to verify identity or attendance.
  - IT Security disables A-number access if fraud or compromise is confirmed.
  - Cases are escalated to the Fraud Prevention Committee for institutional review and next steps.

2. Fraud Detection

Teamwork Monitoring:

These procedures operate in coordination with USU's Incident Response Plan (IRP) when a case involves possible data compromise, unauthorized access, or breach indicators.

USU uses coordinated cross-departmental monitoring to identify indicators of potential fraud or identity misuse.

- Federal Aid Team runs Argos/Banner reports that detect:
  - Shared bank account or routing numbers across multiple students
  - Duplicate or conflicting SSNs, birthdates, mailing addresses, or phone numbers
  - Suspicious FAFSA patterns, including repeated corrections, unusual parent/student swaps, or inconsistent dependency information
  - Unusual enrollment patterns such as add/drop activity timed around refund dates
- Admissions monitors application submissions for:
  - Repeated submissions from the same IP address or device
  - Temporary, unverifiable, or suspicious email domains
  - Duplicate application details used across multiple records
- IT Security reviews:
  - IP address clusters, foreign logins, and geolocation anomalies
  - Device/browser fingerprint duplication across multiple students
  - Login attempts or password resets consistent with account compromise
- Registrar monitors:
  - Students enrolled only in online courses with no academic activity
  - Drop/withdrawal patterns immediately after disbursement
  - Repeated course enrollments intended to create aid eligibility
- Controller's Office identifies:
  - Refund amounts inconsistent with student eligibility
  - Multiple refunds issued to bank accounts shared by unrelated individuals
  - Returned/bounced checks or failed payment activity that aligns with fraud indicators
- Manual Review:
  - When any red flag is identified, a manual review is initiated.

  - Federal Aid Team evaluates anomalies, compares data across Banner, Canvas, vendor systems, and federal databases (NSLDS, COD, IRS, SSA), and documents all findings in RHACOMM (FRAUD) and the Fraud Dashboard. Federal Aid is also responsible for ensuring required RHACOMM entries are completed for all Title IV–related cases.
  - Admissions verifies transcripts, external documentation, or elements of the original application when academic or identity inconsistencies arise.
  - Registrar confirms academic activity with instructors when student participation is uncertain or inconsistent with disbursement records.
  - IT Security reviews account access logs for signs of compromise or unauthorized use.
  - All relevant offices contribute documentation to the Fraud Dashboard and escalate concerning patterns to the Fraud Prevention Committee.

- Red Flag Logging:
  - All fraud indicators, whether automated or manual, must be documented.
  - Record findings in RHACOMM using the FRAUD category code.
  - Add the case to the internal Fraud Dashboard with:
    - Indicators identified
    - Offices involved
    - Actions taken
    - Next steps required
- If fraud indicators suggest unauthorized access, disclosure, or misuse of personally identifiable information, the matter must also be escalated through the University's Incident Response Plan (IRP)
- Dashboard access must be restricted to authorized staff with FERPA/GLBA training.

3. Institutional Review Process/ Responsibilities

- Admissions: Verifies transcripts, diplomas, and application authenticity.
- IT Security: Reviews IP addresses, device/browser fingerprints, and login behavior.
- Student Financial Support: Confirms FAFSA submission, reviews NSLDS history, and cross-checks IRS/DOC/NSLDS flags.
  - Federal Aid Team (Title IV Programs and Private Loan Administration)
    - Oversees Title IV fraud prevention and identity verification processes.
    - Validates student eligibility and prevents improper disbursements of federal aid.
    - Reports any credible suspicion of fraud or misuse of Title IV funds to the U.S. Department of Education's Office of Inspector General within 30 days, in coordination with Legal Affairs and Information Security.
    - Ensures all documentation related to fraud reports is retained in accordance with 34 CFR §668.24.
    - Resolves conflicting information and ensures accurate and timely reporting to COD and NSLDS in accordance with Title IV Administrative Capability requirements.
    - Administers private/alternative loan certification and monitors for indicators of fraud, identity misuse, or misrepresentation.
    - Reviews evidence for Title IV regulatory adherence and prepares documentation for OIG submission.

  - Scholarships Team (State, Institutional, and Private Programs)
    - Safeguards, monitors, and coordinates the awarding and disbursement of all state, institutional, donor-funded, and private financial aid programs.
    - Verifies eligibility criteria for institutional and donor-funded awards and ensures compliance with relevant state regulations and donor agreements.
    - Identifies and reports suspected fraud, identity misuse, or improper disbursement involving non-Title IV aid to the Fraud Prevention Committee in accordance with this policy and university procedures.

- Coordinates with the Federal Aid Team, Admissions, Registrar, Controller's Office, and Information Technology to monitor enrollment, academic activity, and financial transactions related to scholarships and non-federal aid.

Roles at a Glance – Summary

Office	Primary Responsibilities
Federal Aid	Title IV eligibility & Identity Verification, IDVREQ holds, OIG reporting, Private Loans
Scholarships	Institutional, State, Private (Non-federal aid)
Admissions	Application authenticity
Registrar	Academic activity verification
Controller's	Refund anomalies
IT Security	IP/device/access anomalies

Fraud Prevention Committee

The Fraud Prevention Committee consists of individuals from key areas such as the Office of Admissions, Student Financial Support, Office of the Registrar, Information Technology, University Ethics and Compliance Services, and the Controller's Office. The committee includes:

- Vice President for Strategic Enrollment
- Director, Federal Aid
- Associate Director of Federal Aid Operations
- Executive Director, Student Financial Support
- Executive Director, Enrollment Strategy & Innovation
- Director, Admissions
- Executive Director, Admissions Pathways & Engagement
- Assistant Registrar
- Data Privacy Officer
- Chief Information Security Officer
- Security Engineer, Enterprise Systems and Security
- Controller

This committee is responsible for receiving reports of suspected or confirmed fraud or identity theft, reviewing escalated cases involving incomplete identity verification or potential fraud, determining the status of fraud cases, reviewing applicable institutional policies and procedures as needed, and communicating with students and families.

4. Case Resolution Pathways

- Determinations regarding case status (potential misuse, confirmed fraud, or cleared) are made by the Fraud Prevention Committee, in consultation with Federal Aid, Admissions, Registrar, and IT Security.
- Confirmed Fraud or Identity Theft:
  - Cancel all pending aid disbursements.
  - Notify Cashiers to prevent collections activity on fraudulent balances.
  - Reject fraudulent documents and cease processing.
- Potential Misuse but Legitimate Student:
  - Hold all future disbursements pending OIG guidance.
  - Maintain communication logs and all supporting evidence.

- Cleared Cases:
  - Document verification steps.
  - Release holds and proceed with standard processing.
- Any fraud case that may involve compromise of institutional data or systems will be escalated to the Incident Response Plan (IRP) process immediately to ensure proper classification and compliance with applicable data breach obligations.

5. Fraud Case Tracking

- Maintain a secure Fraud Dashboard or equivalent tracking spreadsheet with:
  - Student identifiers, case status, fraud category, OIG reporting date, and resolution details.
- Quarterly reconciliation between Fraud Dashboard and Banner holds to ensure no cases remain unresolved.

6. Training and Oversight

- Annual training is required for all employees handling admissions, student accounts, financial aid, or identity verification.
- New hires must complete training within 30 days.
- Training covers:
  - Regulatory requirements (34 CFR §668.16, §668.24, §668.25).
  - Red flag identification.
  - Reporting procedures.
  - Data privacy and security protocols.
- Annual fraud prevention training will include awareness of the IRP, so that employees understand how fraud cases may intersect with information security incidents and data breach notification obligations.

REPORTING PROCEDURES

1. When to Report? Reporting Triggers

An OIG report must be initiated when there is:

- Reasonable cause to believe fraud, identity theft, or misuse of Title IV or other institutional/state funds has occurred.
- Unusual FAFSA data, admission patterns, or enrollment activity.
- Discovery of fraudulent, altered, or falsified documents.
- A request for information from the U.S. Department of Education Office of Inspector General (OIG) or other regulatory authority.
- Confirmation of fraudulent admission or identity theft affecting a USU applicant or student.
- OIG reports must be submitted within 30 days of credible suspicion, in accordance with the Federal Student Aid Handbook.

2. Authorized Reporters

Only the following positions are authorized to submit official reports to OIG and other external agencies:

- Director of Federal Aid (OIG and federal aid-related reporting)
- USU Compliance Officer (privacy, consumer protection, and regulatory reporting)
- University Legal Counsel (fraudulent admission and legal notifications)
- USU Privacy Officer (student privacy breach determinations)

- USU Police Department (law enforcement reporting)

Note: The responsible office for each reporting requirement will be confirmed and documented in internal procedures.

All confirmed or suspected incidents involving personal data must also be assessed under the University's IRP, which governs incident classification, escalation, and external notification requirements.

3. Reporting Destinations and Methods

Depending on the nature of the case, reports may be submitted to one or more of the following:

1. Internal Notification to Impacted Offices
    a. Financial Aid (to stop disbursements)
    b. Registrar (to cancel fraudulent enrollment)
    c. Admissions (to flag future applications)
    d. IT/GLBA Team
2. USU Privacy Officer
    a. Report all confirmed fraudulent admissions and suspected identity theft for documentation and privacy compliance review.
3. USU Police Department Dispatch
    a. File a report for confirmed or suspected identity theft and fraudulent admission.
4. U.S. Department of Education – Office of Inspector General (OIG)
    a. Use the OIG Hotline: https://oig.ed.gov/oig-hotline
    b. Submit only through secure institutional credentials.
- Do not transmit PII by unencrypted email, but upload in approved channels (directly to OIG fraud reporting form).
5. Other Federal or State Agencies
    a. Federal Trade Commission (FTC) at www.IdentityTheft.gov for confirmed identity theft.
    b. State law enforcement or regulatory bodies as required.

4. Required Reporting Fields

4.1 Internal Notifications to USU Offices

For Financial Aid, Registrar, and Admissions, provide:

- Student or victim name and A-number
- Summary of fraudulent activity
- Actions to take (e.g., stop disbursements, flag account, cancel registration)
- Contact person for follow-up

4.2 Required OIG Reporting Fields

This reporting is done by the Director of Federal Aid. For OIG and other applicable federal agency reports, include as much of the following as available:

- Student Full Name
- USU Student ID (A-Number)
- Social Security Number (provided only in secure form)
- Date of Birth
- Permanent Address
- Phone Number
- Email Address

- Program/Major
- Degree Level (Undergraduate / Graduate / Certificate)
- Admit Term and Status
- FAFSA Submission Date
- Verification Group (V4, V5, or other)
- Loan Period Start/End Dates
- Disbursement Dates and Aid Types Received (Pell, Loans, FWS, FSEOG, State Aid, Institutional Aid)
- Refund Amount(s) and Date(s)
- Total Aid Disbursed
- Account Details for Disbursed Aid (if funds pulled back)
- Description of Suspected Fraud or Identity Theft
- Red Flags or Indicators Identified
- Summary of Actions Taken by USU
- Evidence Attachments (screenshots, documents, IP logs, transcripts, correspondence)
- Fraud Category (Potential Fraud, Confirmed Identity Theft, Abuse of Funds, False Documentation, Eligibility Manipulation, Refund Fraud, Account Compromise, Application Fraud, Academic Activity Fraud)
- Case Numbers (OIG, police, or other)
- USU Contact Person for Follow-up (name, title, phone, email)

4.3 Required FTC Reporting Fields

When assisting a victim to submit a report to the Federal Trade Commission at IdentityTheft.gov, the FTC form typically requires:

- Victim's full legal name
- Date of birth
- Current address and contact information
- Type of identity theft (e.g., student loan fraud, admissions fraud)
- Description of what happened (dates, suspected perpetrators if known)
- List of affected accounts or institutions (optional; provided at the victim's discretion)

Note: FTC reports are filed directly by the victim, not the institution, but staff may assist in guiding them through the process.

4.4 Required Law Enforcement (USU Police or Local PD) Reporting Fields

This reporting is done by the Director of Admissions. For police reports, provide:

- Victim's identifying information (name, date of birth, contact)
- Nature of the offense (fraudulent admission, identity theft, financial aid fraud)
- Timeline of events
- Known suspects or involved parties (if applicable)
- Relevant institutional actions taken (admission canceled, aid stopped)
- Copies of fraudulent documents or evidence (submitted securely)
- USU case/contact person for follow-up

5. Victim Communication – Fraudulent Admission

If fraudulent admission has occurred and it has been confirmed that it was **not** the result of a USU data breach:

1. Department that receives the report will refer it to the Privacy Officer (Liliana Acosta).
    a. Fill out the Fraud Claim Intake Form with the following information: student full name, date of birth, email address, mailing address
    b. Email form to Privacy Officer
2. Data Privacy Officer will submit report to fraudprevention@usu.edu and send a message to the Fraud Response Team to initiate the process
3. Office of Legal Affairs will make efforts to verify the identity of the person making the report and check for anomalies in the system that would confirm the report.
    a. Office of Legal Affairs: Communicate to victim, request police report or FTC report, explore possibilities of data breach
    b. Registrar: Check Canvas activity, Online only classes, verify with faculty member for attendance
    c. Admissions or Student Financial Support: Request an identity verification if available
4. Inform the victim that the fraud was not caused by a USU data breach.
5. Confirm cancellation of the admission, registration, and any financial aid, and flag future applications containing the victim's information.
6. Provide the victim with a designated USU point of contact.
7. Recommend that the victim:
    a. Contact their local police department to file a report.
    b. Report to the FTC at www.IdentityTheft.gov.
    c. Report to the U.S. Department of Education OIG at https://oig.ed.gov/oig-hotline.
    d. Contact their financial institutions and credit bureaus for fraud alerts and a security freeze.

6. Post-Reporting Actions

Upon receiving communications and developing reasonable suspicion, these steps must be initiated immediately, notifying the appropriate departments to implement the action plan, even before submitting formal reports to the respective agencies.

- Lock/disable victim's Anumber account in our Entra/AD systems (via ServiceNow security ticket).
- Place or maintain a Banner hold to prevent further disbursements. The Federal Aid team is using a ROAHOLD (IDVREQ does not prevent packaging/awarding or disbursement).
- Cancel fraudulent admissions and registrations in Banner.
- Retain all documentation in a FERPA/GLBA-compliant secure location.
- Await direction from the OIG or other relevant agency before releasing aid or closing the case.

7. Record Retention

- Maintain all fraud-related records in accordance with 34 CFR §668.24 and as detailed in Policy Section 2.1.1.3. for at least three years from the end of the award year in which the record was created or aid was disbursed, or the FISAP was submitted—whichever is later.
- Retain records longer if directed by the OIG, legal counsel, or regulatory agencies.
- Store records securely with access limited to authorized personnel.

ADDITIONAL INFORMATION

Related USU Policies

- Policy 2204: Student Aid Fraud Prevention and Identity Verification

Guidance

- Utah State University Consumer Information

- Student Financial Support Code of Conduct

Related Forms and Tools

- USU Incident Response Plan
- USU Vendor Management Plan

USU Contacts

- Student Financial Support, Director of Federal Aid