

## University Policy 2204: Student Aid Fraud Prevention and Identity Verification

**Category:** Community Expectations

**Subcategory:** Records Management & Privacy

**Covered Individuals:** Employees, Students, Prospective Students

**Responsible Executive:** Vice President of Strategic Enrollment Management

**Policy Custodian:** Student Financial Support, Director of Federal Aid

**Last Revised:** 2026/03/20

**Previous USU Policy Number:** N/A

---

### 2204.1 PURPOSE AND SCOPE

The purpose of this Policy is to prevent, detect, and respond to fraud and identity theft involving federal, state, institutional, donor, or private student financial aid administered by the University by establishing institutional standards in compliance with Title IV of the Higher Education Act of 1965, and other applicable regulations.

This policy establishes institutional standards for identity verification, fraud monitoring, data safeguarding, and reporting so that Utah State University remains compliant with applicable federal and state requirements.

This policy applies to

- all USU employees who handle or access student admissions, enrollment, registrar, financial aid, student account, or identity verification data;
- all students who apply for or receive university-administered financial support; and
- all Information Technology Resources and records used to collect, store, verify, or transmit student identity, enrollment, and financial aid information.

### 2204.2 POLICY

To maintain institutional compliance with the Administrative Capability requirements under 34 CFR § 668.16 and the Consumer Information regulations of the Federal Student Aid (FSA) Handbook, all departments at Utah State University (USU) must support and maintain systems and processes that prevent, detect, and report fraud involving any university-administered funds, including federal Title IV aid as well as state, institutional, donor-funded, and private financial support. These safeguards protect students and federal resources and preserve the university's eligibility to participate in federal student aid programs.

USU applies five core standards in fulfilling this responsibility:

- verifying student identity and eligibility before aid disbursement
- monitoring academic activity, enrollment, and financial transactions for anomalies
- safeguarding student records and personally identifiable information
- documenting and escalating all suspected cases for investigation

- reporting confirmed or suspected fraud promptly to the appropriate institutional and federal authorities

## 2.1 Institutional Standards

As part of its institutional obligations under 34 CFR §668.16, §668.24, and §668.25, USU establishes the following institutional standards for fraud prevention and identity verification:

**Identity Assurance:** Verify the identity of all students receiving any form of university-administered financial support, including federal Title IV aid as well as state, institutional, donor-funded, and private aid.

**Data Integrity:** Financial transactions include all monetary activity affecting student accounts or aid, such as disbursements, refunds, reversals, adjustments, over awards, and internal transfers in Banner, TouchNet, or related systems. The Controller's Office maintains fiscal accountability and reconciliation, while Student Financial Support and Student Privacy units ensure compliance, data integrity, and fraud monitoring for all federal, state, institutional, and private aid programs.

**Access Control:** Limit system access to authorized personnel and safeguard student information under FERPA and GLBA.

**Incident Response:** Document, investigate, and report suspected or confirmed fraud promptly.

**Record Retention:** In accordance with 34 CFR §668.24(e), USU will retain all Title IV program and fiscal records for three years from the end of the award year in which the aid was last disbursed. Records must be held indefinitely when an audit, program review, investigation, or OIG inquiry is pending. Retention requirements for state, institutional, and private financial aid records follow applicable state regulations, donor agreements, and university records management policies, and must be extended when necessary to support audits, investigations, or program integrity reviews.

These standards align with best practices outlined in the Federal Student Aid Handbook, National Association of Student Financial Aid Administrators (NASFAA) Ethical Principles and Standards, and the National Institute of Standards and Technology (NIST) Digital Identity Guidelines (SP 800-63).

### 2.1.1 Strategies

The institutional standards are supported and reinforced through the following practices:

#### 2.1.1.1 Employee Training

Training all relevant staff annually and ensuring that new hires complete fraud prevention training.

#### 2.1.1.2 System Requirements

- Maintaining systems and cross-departmental processes as required by [Policy 5200: Information Security and Appropriate Use](#), including the following standards:
  - **Security:** All student records must be safeguarded and accessed only by authorized personnel.
  - **Retention:** Records related to identity verification, fraud prevention, and Title IV eligibility must be retained for the federally required minimum period as specified in applicable U.S. Department of Education regulations, and extended if required for state reporting, audit, or investigation.
  - **Functionality:** Maintain audit trails to support fraud detection and reporting, and align with applicable federal requirements.

#### 2.1.1.3 Monitoring, Reviewing, and Retaining Records

- Verifying the identity and eligibility of all students receiving university-administered financial support.

- Confirming documented academic attendance in each course, which may include but is not limited to submitting an assignment, quiz, test, or graded discussion. For online courses, merely logging in or viewing content does not qualify.
- Monitoring and resolving discrepancies across student records and financial aid data.
- Ensuring that all Title IV-eligible students are subject to identity verification before disbursement of aid if selected by the Department of Education, or by the school as needed.
- Monitoring enrollment patterns, academic activity, and aid disbursements for anomalies.
- Retaining relevant records in compliance with 34 CFR §668.24 and any additional OIG directives.
- Retention Period: In accordance with 34 CFR §668.24(e), USU must retain all Title IV program and fiscal records for three years from the end of the award year in which the aid was last disbursed. Records must be retained longer if required for an audit, program review, program integrity inquiry, litigation hold, or OIG investigation, and must not be destroyed until all issues are fully resolved. Loan records may be subject to additional program-specific retention rules, such as Direct Loan reconciliation timelines.

## 2.2 Reporting Obligations

All suspected or confirmed cases of fraud or [Identity Theft](#) must be documented and escalated in accordance with the [University's Incident Response Plan \(IRP\)](#) and Fraud Prevention and Identity Verification Procedures, 2204-PR1. Reports may include referral to the Office of Inspector General (OIG) and other regulatory or law enforcement agencies, as appropriate.

### 2.2.1 Reporting Flow

1. Employees who identify [Red Flags](#) must document and report the concern to their supervisor or directly to the Fraud Prevention Committee. Membership for the Fraud Prevention Committee is outlined in 2204-PR1: Fraud Prevention and Identity Verification Procedures.
2. The Fraud Prevention Committee evaluates the case under the IRP and determines the next steps.
3. Confirmed or escalated cases are reported to the OIG and other authorities as required by the Director of Federal Aid or designee.

Additional details about reporting obligations are included in 2204-PR1: Fraud Prevention and Identity Verification Procedures.

### 2.2.2 Communication

USU will communicate with affected individuals when potential or confirmed fraud, Identity Theft, or data misuse involves their student records. Such notifications will be made in compliance with applicable federal and state laws (including Utah's data breach notification requirements), and in accordance with the University's Incident Response Plan (IRP) and 2204-PR1: Fraud Prevention and Identity Verification Procedures.

## 2204.3. RESPONSIBILITIES

Additional details for each role are included in 2204-PR1: Fraud Prevention and Identity Verification Procedures.

## 3.1 Student Financial Support

Student Financial Support provides institutional leadership for fraud prevention, identity verification, and financial aid compliance across all federal, state, institutional, donor-funded, and private financial aid programs. The office oversees the safeguarding, awarding, monitoring, and disbursement of all university-administered student financial support and ensures alignment with applicable federal, state, institutional, and donor regulations and requirements.

## 3.2 Admissions

Screens for suspicious applications and verifies transcripts. Prevents fraudulent enrollment prior to matriculation.

### 3.3 Information Technology

Reviews IP addresses, device data, and system security. Builds and maintains fraud-detection infrastructure.

### 3.4 Office of the Registrar

Monitors enrollment patterns and works with Student Financial Support on holds. Safeguards the integrity of official student records.

### 3.5 Controller's Office

Maintains internal controls that prevent improper payments, provides payment-related support during fraud reviews, and coordinates recovery of funds once fraudulent activity is confirmed.

### 3.6 Office of General Counsel

Reviews evidence and ensures legal and regulatory compliance.

### 3.7 Employees

Employees within USU departments handling, accessing, or processing student records, admissions, registration, and financial aid data must complete annual fraud prevention training. Report confirmed or suspected cases of fraudulent activity under the University's Incident Response Plan.

### 3.8 Data Privacy Officer, Chief Information Security Officer & Office of General Counsel

Share authority for incident classification, breach determination, and regulatory notification under the [University's Incident Response Plan \(IRP\)](#).

## 2204.4 REFERENCES

The following federal regulatory authorities directly govern identity verification, administrative capability, and fraud prevention for Title IV programs:

- 34 CFR § 668 Student Assistance General Provisions
- 34 CFR § 602.17 Application of Standards in Reaching Accreditation Decisions
- Fair Credit Reporting Act (15 U.S.C. §1681 et seq.)
- Family Educational Rights and Privacy Act (20 U.S.C. §1232g; 34 CFR Part 99)
- Federal Trade Commission's Safeguards Rule under the Gramm-Leach-Bliley Act (16 CFR Part 314)
- Federal Trade Commission's Identity Theft Red Flags Rule (16 CFR § 681)
- Title IV of the Higher Education Act of 1965 (HEA)
- 34 CFR § 668.16 (Standards of Administrative Capability)
- 34 CFR § 668.24 (Record Retention and Access)
- Federal Student Aid Handbook (Consumer Information & Verification)
- Privacy Act of 1974
- Gramm-Leach-Bliley Act (GLBA)
- Uniform Guidance (2 CFR Part 200)
- Applicable state laws on identity theft, fraud, and cybersecurity

## 2204.5 RELATED USU POLICIES

- [Policy 2201: Student Records \(FERPA\)](#)
- [Policy 3016: Information Privacy](#)
- [Policy 5200: Information Security and Appropriate Use](#)

## 2204.6 DEFINITIONS

- **Identity Theft.** The unauthorized use or attempted use of another individual's personal identifying information to impersonate them or obtain access to services, records, systems, financial benefits, or institutional resources. For purposes of this policy, Identity Theft includes any misuse of personal information—whether digital, verbal, or document-based—that could affect admissions, enrollment, student records, identity verification processes, or the awarding, disbursement, or safeguarding of any university-administered funds, including federal, state, institutional, or private financial aid.
- **Office of the Inspector General (OIG).** Independent investigative arm of the U.S. Department of Education responsible for detecting and preventing fraud, waste, misuse, and abuse of Title IV funds.
- **Red Flag.** A pattern, practice, or specific activity that indicates the possible occurrence of Identity Theft, fraud, or misuse of student information or university-administered funds. Within this policy, a Red Flag includes any inconsistency, anomaly, or suspicious behavior related to admissions, enrollment, student records, identity verification, financial transactions, or the awarding and disbursement of federal, state, institutional, or private financial aid.

---

**Information below is not included as part of the contents of the official policy.** It is provided only as a convenience for readers/users and may be changed at any time by persons authorized by the president.

## RESOURCES

### Procedures

- 2204-PR1: Fraud Prevention and Identity Verification Procedures

### Guidance

- [Utah State University Consumer Information](#)
- [Student Financial Support Code of Conduct](#)

### Related Forms and Tools

- [USU Incident Response Plan](#)
- USU Vendor Management Plan

### Contacts

- [Student Financial Support, Director of Federal Aid](#)

## POLICY HISTORY

Original issue date: 2026/03/20

Last revision date: 2026/03/20

Next scheduled review date: 2027/01/01

Previous revision dates: N/A