FEEDBACK

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

ADMINISTRATIVE POLICY STATEMENT

Policy Title: Red Flag Identity Theft Prevention Program

APS Number: 7010 **APS Functional Area:** RISK MGMT/PUBLIC SAFETY

Brief Description:	This administrative policy statement (APS) aligns the University of Colorado Red Flag Identify Theft Prevention Program and sets forth requirements for management of personal financial data, collected in the normal course of business, to help protect members of the University of Colorado community from damages related to identity theft.
Effective:	April 1, 2026 (Pending)
Approved by:	President Todd Saliman (Pending)
Responsible University Officer:	University Controller
Responsible Office:	Office of University Controller
Policy Contact:	Office of University Controller
Supersedes:	See history in section VIII.
Last Reviewed/Updated:	April 1, 2026 (Pending)
Applies to:	All campuses, including System Administration

Reason for Policy: This APS aligns requirements to detect, prevent, and mitigate the risk of *identity theft* in connection with sensitive financial account data, and serves as the university's Red Flag Identity Theft Prevention Program. The program sets parameters that must be followed by organizational units with responsibilities for collecting and managing financial account data when conducting business with students, employees, and other customers of the University of Colorado, and to provide for continuous compliance with federal law and regulations, specifically the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003 and serves as the university's Identity Theft Prevention Program.

I. INTRODUCTION

The University of Colorado Red Flag Identity Theft Prevention Program is designed to reduce the risk of *identity theft* through detection, prevention, and mitigation of patterns and practices that could be indicative of potential *identity theft (“Red Flag”)* involving the university, its students, employees, and other customers. It is designed to ensure compliance with 16 CFR § 681.2, the Federal Trade Commission's “Red Flags Rule.” This program is appropriate to the size and complexity of the university and the nature and scope of its activities and applies to employees and external *service providers* with whom the University of Colorado contracts to perform certain functions on its behalf for *covered financial accounts*, such as student payment plans and federal loan programs. It further sets forth requirements that must be followed by *organizational units* when conducting business with students, employees and other customers of the University of Colorado. These requirements include detecting the warning signs, or *“red flags,”* of *identity theft* in daily operations and taking steps to prevent a *red flag* from escalating into an episode of *identity theft*.

II. POLICY STATEMENT

The University of Colorado Red Flag Identity Theft Prevention Program shall include reasonable policies and procedures to:

1. Ensure the security of the data collected and maintained in *covered financial accounts;*
2. Establish a process to periodically review the security of *covered financial accounts;*
3. Maintain a list of possible *Red Flags*, including *Red Flags* that have been previously detected in university *covered financial accounts*;
4. Respond appropriately to any *Red Flags* that are detected to prevent and mitigate *identity theft*; and
5. Ensure the program is updated periodically.

The program shall, as appropriate, incorporate existing policies and procedures that control relevant reasonably foreseeable risks.

This program applies to all "*covered financial accounts*" and university departments which defer payments, allow multiple payments over time, or that use credit reports for employment or credit decisions. Departments at each of the campuses and System Administration will develop procedures tailored to the size, complexity, and nature of their operation designed to detect, prevent, and mitigate the risk of *identity theft* in accordance with this program. Each organizational unit that handles or maintains *covered financial accounts* must also follow CU's APS 6010 - Data Governance and APS 6005 - Information Technology (IT) Security Program policies and related guidance regarding the privacy and security of confidential and sensitive identifying information.

Relevant *Red Flags* include, but are not limited to:

- **Alerts** - alerts, notifications, or warnings from a consumer reporting agency, including fraud alerts, credit freezes, or official notice of address discrepancies.
- **Suspicious Documents -** such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut up, re-assembled and photocopied.
- **Suspicious Personal Identifying Information -** such as discrepancies in address, Social Security Number, or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; personal information of others already on file; and/or failure to provide all required information.
- **Unusual Use or Suspicious *Covered Financial Account* Activity -** such as material changes in payment patterns, notification that the account holder is not receiving mailed statements, or that the account has unauthorized charges.
- **Notice from Other Sources -** such as the institution receiving notice from a victim of *identity theft* or law enforcement, or another account holder reports that a fraudulent account was opened.

A *covered financial account* with respect to *identify theft* includes:

- Any financial account the university opens or maintains for students, employees or other customers that involves multiple payments or transactions, including deferred payments.
- Any other financial account the university opens or maintains for students, employees or other customers in which there is a reasonably foreseeable risk to the safety or soundness of the university from *identity theft*, including financial, operational, compliance, reputation, or litigation risks.

In order to identify and prevent potential *identity theft*, the university considers a number of factors including:

- the types of financial accounts that it offers and maintains;
- the methods used to open financial accounts; and
- the methods used to provide access to financial accounts.

If and when the University of Colorado engages a service provider to perform an activity in connection with a *covered financial account*, University organizational units have delegated responsibility for administering the program with respect to that particular *covered financial account* and should take steps necessary to ensure that the activity of the service provider is conducted in compliance with University policies.

III. DETECTION OF RED FLAGS

University of Colorado personnel must take appropriate steps to protect a customer's risk of *identity theft* when working with a transaction that involves a *covered financial account*.

Detection of *Red Flags* in connection with the opening of *covered financial accounts* as well as existing *covered financial accounts* can be made through such methods as:

- Obtaining and verifying customer identity
- Authenticating customers
- Monitoring transactions
- Ensuring that any data security incident allowing unauthorized access to a customer's account record is resolved

IV. PREVENTING AND MITIGATING IDENTITY THEFT

All University of Colorado employees who have access to *covered financial accounts* must take university training on recognizing and responding to potential Red Flags in order to maintain their access to *covered financial accounts*.

When potentially fraudulent activity is detected, an employee must act quickly because a rapid and appropriate response can protect the university and its customers from damages and loss.

An appropriate response can include any of the following, depending on the degree of risk posed by the incident:

- Gathering all related documentation and writing a description of the situation;
- Denying access to the *covered financial account* until other information is available to eliminate the possibility of *identity theft*;
- Contacting the student(s) and/or individual account holders;
- Changing any passwords, security codes or other security devices that permit access to the *covered financial account*;
- Cooperating with law enforcement;
- Determining that no further action is warranted under the circumstances; and
- Taking appropriate steps to modify the process to prevent similar activity in the future.

V. PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Related Administrative Policy Statements

1. APS 6005 - IT Security Program | University of Colorado
2. APS 6010 – Data Governance

B. Educational Resources

Educational resources including guides, training announcements, and newsletters are available on Office of University Controller and Office of Information Security websites.

1. https://www.cu.edu/security/worried-about-identity-theft (OIS)
2. https://www.cu.edu/treasurer/identity-theft-briefing-paper (Treasurer)
3. University System Percipio (Skillsoft) course: CU Identity Theft Prevention Program
4. Red Flag Rule Training

C. Related Policies and Laws

1. Red Flags Rule | Federal Trade Commission
   a. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681
2. Gramm-Leach-Bliley Act | Federal Trade Commission

VI. DEFINITIONS

For purposes of this policy, italicized terms used in this APS are defined in the APS Glossary of Terms or are defined in this APS:

- *Covered financial account* is defined as a "Covered account" in the Code of Federal Regulations Title 16, Chapter I, Subchapter F, Part 681.1, (a)(3).
- *Customer* is defined as a person who has a covered financial account with the University of Colorado and a service provider.
- *Identity theft* is a fraud committed or attempted using the identifying information of another person without authority.
- *Red Flag* is a pattern, practice, or specific activity that indicates the possible existence of *identity theft*.
- *Service provider* means a vendor that provides services directly to the University of Colorado related to *covered financial accounts*.

VII. OVERSIGHT OF PROGRAM

A. Oversight of the program shall reside with the Office of University Controller.

B. This policy should be reviewed and updated every three to four years by the Office of University Controller. The assessment should consider any changes in risks to students, employees and other customers of the University and to the safety and soundness of the university from identity theft.

C. Each university organizational unit that has *covered financial accounts* will be responsible for implementing procedures to ensure compliance with this policy and the FTC Red Flag Rule.

D. Training to identify and respond to potential Red Flags is required for all staff who work in an organizational unit with covered financial accounts.

VIII. HISTORY

The Identity Theft Prevention Program at the University of Colorado was previously in *APS 7003-Collection of Personal Data from Students and Customers*. The portions pertaining to "red flag" of identity theft in APS 7003 were updated and moved into the new *APS 7010-Red Flag Identity Theft Prevention Program* which was adopted on April 1, 2026. (Pending)

- Adopted: April 1, 2026. (Pending)
- Revised: N/A.
- Last Reviewed: April 1, 2026. (Pending)