UNIVERSITY OF DENVER
POLICY MANUAL
IDENTITY THEFT PREVENTION

Responsible Department: Information Technology **Recommended By:** Provost, SVC Business and Financial Affairs, Vice Chancellor for Information Technology **Approved By**: Chancellor	**Policy Number** IT 2.30.060	**Effective Date** 7/9/2021

I. INTRODUCTION

Pursuant to the Federal Trade Commission's (FTC) Red Flags Rule implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, the University is required to establish and administer an Identity Theft Prevention Program (Program). This *Identity Theft Prevention Policy* defines the requirements to build a compliant Program designed to detect, prevent, and mitigate Identity Theft associated with the University's operations and account systems and the nature and scope of the University's activities.

II. POLICY OVERVIEW

As stated in Process Overview.

III. PROCESS OVERVIEW

A. Required Policies and Procedures

The University shall implement reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing Covered Accounts and incorporate those Red Flags into the Program;

2. Detect 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; and

4. Ensure the Program is updated periodically to reflect changes in risks to Customers or to the safety and soundness of the University from Identity Theft.

B. Oversight

The Senior Vice Chancellor for Business and Financial Affairs, or a designee, shall be responsible for the delegation of a Program Administrator.

The Program Administrator shall:

1. Be responsible for the development, implementation, oversight and continued administration of the Program;

2. Review reports prepared by staff regarding compliance with the Program;

3. Recommend and approve all changes to the Program to address changing risks of Identity Theft, as necessary; and

4. Exercise appropriate and effective oversight of Service Provider arrangements.

C. Identification of Red Flags

In order to identify relevant Red Flags, each University department shall consider the types of accounts that it offers and maintains, methods it provides to open said accounts, methods it provides to access said accounts, and its previous experiences with Identity Theft in the development of procedures implementing this Policy.

The Program shall identify relevant Red Flags from the following categories, as appropriate:

1. Alerts, notifications, or other warnings received from consumer reporting agencies, or Service Providers (*e.g.*, fraud detection services);

2. The presentation of suspicious documents;

3. The presentation of suspicious personal identifying information;

4. The unusual use of, or other suspicious activity related to, a Covered Account; and

5. Notice from Customers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with a Covered Account.

When implementing the Program, each University department shall consider the following *Risk Factors* in identifying relevant Red Flags for Covered Accounts, as appropriate:

1. The types of Covered Accounts offered or maintained;

2. The methods provided to open Covered Accounts;

3. The methods provided to access Covered Accounts; and

4. Any previous experiences with Identity Theft.

The Program implementing policies and procedures shall incorporate relevant Red Flags from sources such as:

1. Incidents of Identity Theft previously experienced;

2. Methods of Identity Theft that reflect changes in risk; and

3. Applicable supervisory guidance.

D. Detecting & Preventing Red Flag Events

Methods of detection of Red Flags identified in Section III.C, *Identification of Red Flags,* shall be established and defined within each implementing policy or procedure and shall include the following, as appropriate:

1. Obtaining identifying information about and verifying the identity of an individual opening a new or accessing an existing Covered Account, enrolling as a student at the University, or applying for a position of employment or volunteer for which a credit or background report is sought; and

2. Authenticating individuals, monitoring transactions, and verifying the validity of a change of address request.

In order to mitigate and prevent Identity Theft, methods of responding to detected Red Flags shall also be established and defined within each implementing policy or procedure. Appropriate responses may include:

1. Monitor a student or Covered Account for evidence of Identity Theft;

2. Contact the individual whose identity may be at risk;

3. Change in any passwords, security codes or other security devices that permit access to Covered Accounts;

4. Re-open a Covered Account with a new account;

5. Close an existing Covered Account;

6. Notify law enforcement; or

7. Determine no response is warranted under the particular circumstances.

E. Program Administration & Management

To effectively implement the Program, University staff responsible for the implementation of associated policies and procedures shall be trained, as necessary, either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected.

Program trained University staff shall notify the Program Administrator once an incident of Identity Theft has occurred and/or the University failed to comply with the established Program.

At least annually, or at the request of the Program Administrator, Program trained University staff shall report on the University's compliance with the Program to the Board of Trustees, an appropriate committee of the Board of Trustees, or a designated employee at the level of senior management. The report shall address matters related to the Program (*e.g.,* effectiveness of the policies and procedures relating to the management, and mitigation and response to Red Flag; Service Provider arrangements; significant incidents involving identity theft and management's response) and recommendations for changes to the Program.

The activity of all Service Providers performing an activity in connection with one or more Covered Accounts shall be conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

The Program shall be periodically reviewed and updated to reflect changes in risks to students and the soundness of the University from Identity Theft based on factors such as:

1. The experiences of the organization with Identity Theft;

2. Changes in methods of Identity Theft;

3. Changes in methods to detect, prevent and mitigate Identity Theft;

4. Changes in the types of accounts that the organization offers or maintains; and

5. Changes in the business arrangements of the University.

IV. DEFINITIONS

1. **“Covered Account”** - An account which is primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, includes items such as a student’s tuition account, a student's ID card account (if financial transactions occur on said account), a student's financial aid account, an employee's payroll account, an employee's human resources file relating to a Social Security number, etc.; and any other account that the University offers or maintains for which there is a reasonably foreseeable risk to Customers or to the safety and soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

2. **“Customer”** - means a person that has a Covered Account with the University.

3. **“Identity Theft”** - Fraud committed or attempted using the identifying information of another individual without permission or authority.

4. **“Red Flag”** - A pattern, practice or specific activity that indicates the possible existence of Identity Theft.

5. **“Service Provider”** - A person that provides a service directly to the University.

Revision Effective Date	**Purpose**
7/9/2021	*Minor revisions*