Preamble. The U.S. Congress has provided protection for consumers from identity theft by enacting the Fair and Accurate Credit Transactions Act (“FACTA”) and the Fair Credit Reporting Act (“FCRA”). FACTA directed the Federal Trade Commission (“FTC”) to issue regulations, now generally referred to as the “Red Flags Rule” (the Rule), which require financial institutions and creditors to adopt policies and procedures that protect consumers from identity theft.

Accordingly, UI adopts this policy to identify, prevent and mitigate identity theft in compliance with the Rule; approve and establish an Identity Theft Prevention Program; and appoint a program administrator who has primary responsibility for oversight of the Program.

A. Definitions.

A-1. Creditor: any natural person, corporation or other entity that regularly, and in the ordinary course of business, advances funds to or on behalf of a person, based on an obligation to repay the funds or repayable from specific property pledged by the person.

A-2. Covered Account: an account that the university offers or maintains for individuals that are primarily for personal, family, or household purposes and designed to permit multiple payments or transactions, or is any account that is subject to a reasonably foreseeable risk of identity theft.

A-3. Identifying Information: any name or number that may be used alone or in conjunction with any other information to identify a specific person, including: name, address, telephone number, social security number, date of birth, driver’s license or identification number, alien registration number, passport number, employer or taxpayer identification number.

A-4. Identity Theft: a fraud committed or attempted using the identifying information of another person without authority.

A-5. Red Flag: a pattern, practice or specific activity that indicates the potential for identity theft.

A-6. Red Flag Rule (the Rule): regulations adopted by the FTC requiring creditors to adopt policies and procedures that protect consumers from identity theft.

A-7. Program Administrator: the individual designated to have primary responsibility for oversight of the Program.

B. Policy. It is the policy of UI to comply with the requirements of the Rule. Accordingly, UI has developed a program that is designed to meet the requirements of the Rule to identify, prevent, and mitigate identity theft. The Program contains mechanisms to identify and detect relevant Red Flags; respond appropriately to prevent identity theft and mitigate damages; and ensure that the Program is updated periodically to reflect changes in risks.

B-1. Identification of Red Flags. To identify relevant Red Flags, the UI considers the types of covered accounts that it offers and maintains; the methods it provides to open and access the covered
accounts, including in-person, mail or online methods, and the UI's previous experience with identity theft. Covered accounts examples include, but are not limited to the following:

1. Accounts managed by the Student Accounts Office
2. Accounts managed by the Student Financial Aid Office related to the administration of emergency short-term loans and disbursement of funds

The UI has identified the following Red Flags which may arise with respect to covered accounts and/or external accounts:

**a. Notifications or Warnings from Consumer/Credit Reporting Agencies:** Alerts, notifications, or other warnings received from consumer reporting agencies or service providers indicating:
   1. A credit freeze
   2. Active duty alert
   3. Address discrepancy in response to a credit report request
   4. Activity that is inconsistent with the usual pattern or activity of the account holder

**b. Suspicious Documents:** Presentation of suspicious documents which appear to be altered, forged or inauthentic, including inconsistent appearance of photographs or physical description on a document with the person presenting it.

**c. Suspicious Personal Identifying Information:** Presentation of inconsistent personal identifying information such as:
   1. An inconsistent birth date
   2. An address that does not match a prior address submitted on an application
   3. A social security number, telephone number or address that is the same as that given by another account holder
   4. Repeated failure to provide identifying information on an application

**d. Suspicious Use or Activity in Covered Account:** Unusual use of or other suspicious activity related to a covered account including, but not limited to:
   1. Requests made from a non-UI issued email account
   2. “Unofficial” forms which are presented with requests for information
   3. Mail returned as undeliverable
   4. Notice of change in payments for an otherwise consistent account

**e. Alerts from Others:** Notice from an account holder, victim of identity theft or law enforcement authorities that the UI has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

**B-2. Detection of Red Flags.** The Program is required to establish procedures for the detection of Red Flags in the designated areas of activity. These procedures are set forth below:

**a. Opening of Covered Accounts:** Identity verification of first-time account holders will be required, including presentation of identifying information such as name, date of birth, academic records or insurance card, and home address, which will be subsequently verified by review of driver’s license, passport or other government-issued photo identification and insurance company information.
b. **Existing Covered Accounts**: Authentication of account holders and monitoring of transactions on the covered account will be required, including:

- Verification of the identity of account holders if they request information (in person, via telephone, via facsimile, via email)
- Verification of changes in banking information given for billing or payment purposes
- Requests for billing address changes for covered accounts must be verified and means provided to account holders for notification of changed or incorrect billing addresses

c. **Consumer/Credit Report Requests**: When a consumer/credit report request results in notice of an address discrepancy from the reporting agency, UI personnel will request written verification from the subject of the report that the address he/she provided is accurate, and once an address is verified, UI personnel will report such address to the reporting agency.

d. **Risk Assessment**: A risk assessment will be conducted annually as well as in the event that actual instances of identity theft occur.

B-3. **Response to Red Flags**. In response to the detection of Red Flags, UI personnel will take the appropriate action to prevent and mitigate identity theft depending upon the degree of risk posed by the Red Flags, including:

1. Monitoring a covered account for suspicious activity
2. Denying access to the covered account until information is verified to eliminate Red Flags
3. Contacting the account holder to verify activity in the covered account
4. Changing passwords, security codes or other security devices
5. Closing and reopening the covered account
6. Refusing to open a new covered account
7. Notifying law enforcement
8. Determining that no response is warranted upon reasonable investigation of the particular circumstances

B-4. **Updating the Program**. UI shall update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to students or others or to the safety and soundness of UI from identity theft, based on factors such as:

1. The experiences of UI 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 UI offers or maintains
5. Changes in the business arrangements of UI, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements

B-5. **Methods for Administering the Program**.

a. **Oversight of Program**: This Program shall be overseen by the Vice President for Information Technology and the Vice President for Finance and Administration. This oversight shall include:

1. Implementation of the Program by the Vice President for Information Technology.
   Primary responsibility for oversight of the Program will belong to the Chief Information Security Officer, in the role of the Program Administrator.
2. Review of reports, prepared by staff regarding compliance by UI with the Identity Theft Prevention Policy and Program, by the Program Administrator.
3. Making material changes to the Program as necessary to address changing identity theft risks.

b. Staff Training and Reporting: UI personnel will be trained at least annually by or under the direction of the Program Administrator to effectively implement the Program and detect and respond to Red Flags. UI personnel will notify the Program Administrator of any incident of identity theft or failure to comply with the Program. UI personnel designated by the Program Administrator will report to the Program Administrator at least annually, or as requested. Such reports will include, among other relevant issues:
   1. The effectiveness of the specific policies and procedures for addressing the current risks of identity theft in connection with the covered accounts
   2. Any significant incidents involving identity theft and the response taken
   3. Recommendations for material changes to the Program

c. Oversight of Service Providers: In the event that the UI contracts with an outside service provider to perform any activity in connection with covered accounts, the UI will ensure that:
   1. The service provider’s activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate risk of identity theft
   2. The service provider reviews the Program and reports any Red Flags to the Program Administrator or the designated UI personnel with primary oversight of the service relationship

B-6. Noncompliance. Noncompliance with this policy may result, depending upon the nature of the non-compliance, in the user’s account or access to UI technology resources being temporarily suspended, or disabled, or permanently terminated. In the case of temporary suspension, UI may require implementation of certain remedial measures or satisfaction of certain educational courses prior to reinstatement of the user’s account or access. Additionally, the user may be referred for institutional sanctions to the appropriate UI disciplinary body.

C. Scope. This Policy applies to all UI employees, students, volunteers and agents who are involved in handling information that can be used to identify a specific person in connection with certain accounts of that person maintained by UI.

D. Exceptions. Requests for exceptions in all or part of this policy may be submitted in writing to the Program Administrator who will assess the risk and make a determination. Determinations will be provided back to the requestor in writing. Any exceptions must be reviewed at least annually.

E. Contact Information. The responsible party for this policy is Vice President for Information Technology, its-security@uidaho.edu. The Program Administrator can assist with questions regarding this policy and program.

F. References.

- Fair and Accurate Credit Transactions Act
- Fair Credit Reporting Act