BOISE STATE UNIVERSITY

University Policy #8120

Identity Theft Prevention Program

Effective Date

April 2009

Responsible Party

Information Security Officer (ISO), (208) 426-1159

Scope and Audience

This policy applies to all University employees, students, contractors, and affiliates who have access to personally identifying information and/or covered accounts.

Additional Authority

Fair and Accurate Credit Transactions Act (FACTA) of 2003.

1. Policy Purpose

To implement a prevention program to detect, prevent and mitigate identity theft in connection with new or existing covered accounts.

2. Policy Statement

In accordance with the Fair and Accurate Credit Transactions Act (FACTA) of 2003, the University has established an Identify Theft Prevention Program to identify relevant red flags for new and existing covered accounts, detect new red flags, and respond appropriately to any red flags that are detected.

3. Definitions

3.1 Covered Account

Includes all student accounts or loans administered by the University.

3.2 Identity Theft

Fraud committed or attempted using the identifying information of another person without authority.

3.3 Personally Identifying Information

Any name or number that may be used alone or in conjunction with other information to identify a specific person including an individual's name, address, date of birth, social security number, driver's license number, passport number, tax identification number, student identification number, or banking account information.

3.4 Red Flag

A pattern, practice or specific activity that indicates the possible existence of identity theft.

4. Responsibilities and Procedures

4.1 Identification of Red Flags

In order to identify relevant red flags, the University must consider the types of accounts it maintains, methods it provides to open and access these accounts and its previous experiences with identity theft. Accordingly, the following red flags have been identified for each of the categories listed:

4.1.1 Notifications and Warnings from Credit Reporting Agencies

- Report of fraud accompanying a credit report;
- Notice or report from a credit agency of a credit freeze on an applicant;
- Notice or report from a credit agency of an active duty alert for an applicant;
- Receipt of a notice of address discrepancy in response to a credit report request; and

- Indication from a credit report of activity that is inconsistent with an applicant's usual behavior or activity.

4.1.2 Suspicious Documents

- Identification document or card that appears to be forged, altered, or unauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with existing student information; and
- Application for services that appears to have been forged or altered.

4.1.3 Suspicious Personal Identifying Information

- Identifying information that is inconsistent with other information the student provides, for example two documents with different birth dates;
- Identifying information that is inconsistent with other sources of information, for example supplemental documentation for a student loan with a different address than that on file with the University;
- Identifying information that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity, for example an invalid phone number or fictitious address;
- Social Security Number that is the same as another student or employee;
- Address or phone number that is the same as another student or employee; and
- An individual who fails to provide complete personal identifying information on an application when prompted to do so.

4.1.4 Suspicious Covered Activity Account or Unusual Use of Account

- Change of address for an account followed by a request to change the student's name;
- Payments stop on an otherwise consistently up-to- date account;

- Account is used in a way that is not consistent with prior use;
- Mail sent to a student is consistently returned as "undeliverable;"
- A student notifies the University that s/he is not receiving mail sent by the University;
- A student notifies the University that an account has unauthorized activity;
- Breach in the University's computer system security; and
- Other unauthorized access to or use of student account information.

4.1.5 Alerts from Other Sources

Notice to the University from a student, identity theft victim, law enforcement or other individual that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft.

4.2 Detecting Red Flags

4.2.1 Student Enrollment

In order to detect any of the red flags identified above that are associated with the enrollment of a student, University personnel must take both of the following steps to obtain and verify the identity of the individual opening the account:

a. Require certain identifying information such as name, date of birth, academic records, home address or other identifying information; and

b. Verify the student's identity at the time of issuance of student Bronco Card by checking student's driver's license or other government issued identification.

4.2.2 Existing Accounts

In order to detect any of the red flags identified above for an existing covered account, university personnel must take all of the following steps to monitor transactions on an account:

a. Verify the identification of students requesting information in person, by mail, email or facsimile;

b. Verify the identity of individuals requesting to change billing addresses by mail or email;

c. Provide the student a reasonable means of promptly reporting incorrect billing address changes; and

d. Verify changes in banking information given for billing and payment purposes.

4.2.3 Consumer Credit Reports

In order to detect any red flags identified above for any covered account for which a credit report is required, university personnel will take both of the following steps to assist in identifying address discrepancies:

a. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and

b. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the report was requested and report to the consumer reporting agency an address for the applicant that the University has taken reasonable steps to confirm is accurate.

4.3 Preventing and mitigating Identify Theft

4.3.1 Reporting Requirement

In the event that university personnel detect any red flags, the Information Security Officer (ISO) must be contacted within one (1) business day. Thereafter, the ISO will determine whether one or more of the following steps should be taken, depending on the degree of risk posed by the red flag:

- Monitor the affected covered account for evidence of identity theft;
- Contact the student or applicant for which a credit report was run;
- Change any passwords or other security devices that permit access to covered accounts;
- Provide the student with a new student identification number;
- Notify law enforcement;

- File a Suspicious Activity Report (SAR); or
- Other action as recommended by the Information Security Officer.

4.3.2 Protecting Student Identifying Information

In order to prevent the likelihood of identity theft occurring, the University will take all of the following steps with respect to its internal operating procedures to protect student identifying information:

a. Ensure that institutional web pages are secure or provide clear notice where web pages are not or cannot be secured;

b. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision had been made to discard that information;

c. Avoid using social security numbers except when required for tax or other governmental reporting purposes;

d. Ensure computer virus protections are up to date; and

e. Require and maintain the minimum amount of student information that is necessary for institutional purposes.

4.4 Preventing and Mitigating Identify Theft

4.4.1 Reporting Requirement

In the event that university personnel detect any red flags, the Information Security Officer (ISO) must be contacted within one (1) business day. Thereafter, the ISO will determine whether one or more of the following steps should be taken, depending on the degree of risk posed by the red flag:

- Monitor the effected covered account for evidence of identity theft;
- Contact the student or applicant for which a credit report was run;
- Change any passwords or other security devices that permit access to covered accounts;
- Provide the student with a new student identification number;

- Notify law enforcement;
- File a Suspicious Activity Report (SAR); or
- Other action as recommended by the Information Security Officer.

4.4.2 Protecting Student Identifying Information

In order to prevent the likelihood of identity theft occurring, the University will take all of the following steps with respect to its internal operating procedures to protect student identifying information:

a. Ensure that institutional web pages are secure or provide clear notice where web pages are not or cannot be secured;

b. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision had been made to discard that information;

c. Avoid using social security numbers except when required for tax or other governmental reporting purposes;

d. Ensure computer virus protections are up to date; and

e. Require and maintain the minimum amount of student information that is necessary for institutional purposes.

4.5 Program Administration

4.5.1 Oversight

Responsibility for implementing and updating the identity theft prevention program lies with the ISO. The ISO will be responsible for training University staff about the program and for reviewing SARs on the detection of and response to red flags. The ISO is also responsible for determining which steps of prevention and mitigation are most appropriate in light of particular circumstances.

4.5.1A Staff Training and SARs

The ISO is responsible for training university employees to detect red flags and respond appropriately. The ISO will work with the appropriate personnel to effectively implement the program and to regularly monitor compliance with the program requirements. The ISO will develop a reporting procedure for employees to report red flag incidents and will summarize his/her findings for the Vice President for Finance and Administration on a biannual basis.

4.5.1B Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more covered accounts, both of the following steps will be taken to ensure the service provider performs its duties in accordance with all institutional policies and procedures designed to detect, prevent and mitigate the risk of identity theft:

a. Require, by contract, that service providers understand and agree to abide by university policies and procedures regarding identity theft: and

b. Require, by contract, that service providers report any red flags to the ISO or the university employee with primary oversight of the service provider.

4.5.1C Non-Disclosure of Specific Practices

In order to optimize the effectiveness of the Identity Theft Prevention Program, information regarding specific red flag identification, detection, mitigation and prevention practices may need to be limited to the ISO, his/her supervisor(s), and employees charged with identifying and reporting those red flags.

4.5.1D Program Updates

The ISO will periodically review and update the Identity Theft Prevention Program to reflect changes in risks. In so doing, the ISO will consider the institution's experiences with identity theft, changes in the means by which identity theft occurs, changes in identity theft prevention and detection methods, and changes in the way business relationships are structured with other entities. After considering these changes, the ISO will determine whether changes to the program, including the type of red flags, are warranted.

Revision History