BOISE STATE UNIVERSITY

University Policy 8120

Identity Theft Prevention Program

Effective Date

April 2009

Last Revision Date

January 19, 2023

Responsible Party

Chief Information Security Officer (CISO), (208) 426-4127

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
- University Policy 6340 (Payment Card Industry Data Security Standard (PCI DSS) Policy))
- University Policy 8000 (Information Technology Resource Use)

1. Policy Purpose

To outline the University's Identity Theft Prevention Program that serves to detect, prevent, and mitigate Identity Theft in connection with new or existing Covered Accounts.

2. Policy Statement

Boise State University has established an Identity Theft Prevention Program in accordance with the Fair and Accurate Credit Transaction Act that identifies relevant Red Flags for new and existing Covered Accounts, detects new Red Flags, and responds appropriately to any Red Flags that are detected.

3. Definitions

3.1 Covered Account

Student financial accounts and 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

4.1 Identification of Red Flags

University employees must exercise due-diligence in looking for Red Flags and indications of fraudulent activity in the following types of suspicious documents, Personally Identifying Information, and alerts:

a. Suspicious Documents

- Cards or documents that appear forged, altered, unauthentic, or in any way inconsistent with student information.

- Cards or documents containing photographs or physical descriptions that do not match the information to the person presenting the document.

b. Suspicious Personally Identifying Information

- Documents with different birth dates or information that is inconsistent with other sources of information, invalid phone numbers, or fictitious addresses.
- Duplications of Social Security Numbers, addresses, or phone numbers.
- Failure to provide complete Personally Identifying Information on an application when prompted to provide such information.

c. Alerts from Other Sources

- Red Flags from other sources, such as credit reporting agencies, governments, law enforcement, or Identity Theft victims.

4.2 Detecting Red Flags

4.2.1 Student Enrollment

To help detect any of the Red Flags identified in section 4.1 that are associated with the enrollment of a student, University employees must take both of the following steps to obtain and verify the identity of the individual opening the account:

a. Require certain Personally Identifying Information such as name, date of birth, academic records, home address, or other Personally Identifying Information; and

b. Check the student's driver's license or other government-issued identification to verify the student's identity at the time their Bronco Card is issued.

4.2.2 Existing Accounts

To help detect any of the Red Flags identified in section 4.1 for an existing Covered Account, University employees must take all of the following steps to monitor transactions on an account:

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

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

c. Provide the student with 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

To help detect any Red Flags identified in section 4.1 for any Covered Account for which a credit report is required, University employees must take the following step(s):

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. If a notice of 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 a University employee detects any Red Flags, the Office of Information Technology (OIT) must be contacted within one (1) University business day. Thereafter, the CISO 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); and/or
- Other action as recommended by the CISO.

4.3.2 Protecting Student Identifying Information

To prevent the likelihood of Identity Theft occurring, and to protect student Personally Identifying Information, the University will take all of the following steps:

a. Ensure that University web pages are secure;

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

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

d. Require and maintain only the minimum amount of student information that is necessary for institutional purposes (See procedure on minimum security standards for systems).

4.4 Program Administration

4.4.1 Oversight

The CISO is responsible for implementing and updating the Identity Theft Prevention Program, ensuring University employees receive training about the program, determining which steps of prevention and mitigation are most appropriate for a specific circumstance, and reviewing SARs on the detection of and response to Red Flags.

4.4.1A Staff Training and SARs

a. The CISO, in conjunction with other University leadership, is responsible for ensuring that University employees receive training to detect Red Flags and respond appropriately.

b. The office of the CISO will work with the appropriate employees to effectively implement the program and to regularly monitor compliance with the program requirements.

c. The CISO will develop a reporting procedure for employees to report Red Flag incidents and will summarize their findings for the Associate Vice President of Information Technology on an annual basis.

4.4.1B Service Provider Arrangements

When 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 University policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft:

a. Require, by contract, that the service provider understand and agree to abide by University policies and procedures regarding Identity Theft: and

b. Require, by contract, that the service provider report any Red Flags to OIT or the University employee with primary oversight of the service provider.

4.4.1C Non-Disclosure of Specific Practices

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 CISO's office and employees charged with identifying and reporting such Red Flags.

4.4.1D Program Updates

The CISO will periodically review and update the Identity Theft Prevention Program to reflect changes in risks. In so doing, the CISO will consider the University'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 such changes, the CISO will determine if changes to the program, including the types of Red Flags, are warranted.

5. Related Information

Minimum Security Standards for Systems
https://www.boisestate.edu/oit/itgrc/it-standards/minimum-security-standards-for-systems/

Revision History

January 19, 2023