Identity Theft Prevention Program

POLICY

In order to minimize the possibility of identity theft, University departments and personnel are responsible for observing the requirements of the Identity Theft Prevention Program.

Program Adoption

Washington State University establishes an Identity Theft Prevention Program, described in this section, pursuant to the Federal Trade Commission regulations, 16 *CFR* Part 681.2.

References

15 *USC* 1681a, 1691a
18 *USC* 1029(e)
16 *CFR* 603.2(a)
16 *CFR* 681: Identity Theft Rules (*Red Flag Rules*)
§ 334.82(b) Fairness and Accuracy in Credit Transactions Act

Definitions

Following are definitions used in this program.

Identity Theft

Identity theft is a fraud committed or attempted using the identifying information of another person without authority.

Red Flag

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

Covered Account

A covered account is an account that a creditor, e.g., WSU, offers or maintains, primarily for personal, family or household purposes that involve or are designed to permit multiple payments or transactions.

Purpose

The Identity Theft Prevention Program is designed to detect, prevent, and mitigate identity theft in connection with covered accounts. The program includes reasonable policies and procedures to:

- Identify relevant red flags for covered accounts offered or maintained by WSU or service providers.
- Detect red flags that have been incorporated into the program.
- Respond appropriately to any detected red flags.
- Ensure that the program is updated periodically to reflect changes in risks to customers including students or to the safety and soundness of the creditor, e.g., WSU, from identity theft.

Identity Theft Prevention Program

COVERED ACCOUNTS

University Accounts

Covered accounts administered by the University include accounts that are used to process the following:

- Student loan credit balances, including Federal Perkins, Health Professions, and WSU institutional loan programs.
- Student loan repayments.
- Student accounts and general accounts receivable accounts repayments.
- CougarCard accounts.

Service Provider Accounts

Covered accounts administered by service providers include services provided by contracted third-party commercial collection agencies for student loan accounts, student accounts, and general accounts receivable account collection and repayment.

IDENTIFICATION OF RELEVENT RED FLAGS

The program identifies the following as red flags:
(See also Appendix: Red Flag Indicators on 30.64.6-7.)

- Suspicious documents
- Suspicious personal identifying information
- Unusual use of, or suspicious activity related to the covered account
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Risk Factors

The program promotes consideration of risk factors in identifying relevant red flags for covered accounts, e.g., the types of covered accounts (see above) and the methods required to open covered accounts.

Methods of Opening Accounts

The following circumstances may lead to opening covered accounts:

- Acceptance to the University and enrollment in classes.
- Acceptance of financial aid award.

Identity Theft Prevention Program

Methods of Opening Accounts (cont.)

- Completion of a student long-term loan entrance interview that requests the following personally identifying information:

  Social security number
  Full name
  Permanent address
  Local address
  Telephone
  Date of birth
  Driver license information
  Next of kin information
  Two personal references, including address and telephone

Access Methods

The University responds to requests to access covered account information in accordance with the following requirements.

- In person access requires WSU ID card or picture identification.
- Correspondence is mailed only to an address on file in the WSU Directory or an address provided by the U.S. Postal Service.
- Online account access requires WSU Network ID and password.
- Refunds provided by direct deposit are electronically sent via Automated Clearing House to bank accounts previously designated by customers.

DETECTION OF RED FLAGS

The program provides for detection of red flags relevant to each type of covered account. See also *BPPM* 30.64 - Appendix: Red Flag Indicators.

Refund of Student Loan Credit Balance

As directed by federal regulation (U.S. Department of Education) and/or departmental procedures, student loan credit balances must be refunded to the student. The refund can only be mailed to an address on file with the University or direct-deposited into the student's bank account. If the refund is picked up *in person* a valid WSU ID or picture ID is required.

Red Flags

Picture ID not appearing to be authentic or not matching the appearance of the student presenting it.

Identity Theft Prevention Program

Student Loan Information

WSU has implemented specific procedures to protect confidential student information from being inappropriately released to third parties. Each involved employee receives training and is responsible for understanding and complying with department-specific procedures when responding to telephone calls.

Red Flags

While calls that resemble the following examples are not necessarily red flags; extra care should be taken to ensure the authenticity of the call:

- A caller who cannot provide all relevant information.
- A caller who is abusive and attempts to get information through intimidation.
- A caller who tries to distract WSU employee by being overly friendly or engaging the employee in unrelated "chit-chat" in an effort to change the employee's focus.
- Any caller who appears to be trying to get the employee to circumvent WSU policy through some tactic that is intended to persuade the employee.

RESPONSES TO RED FLAG DETECTIONS

If a red flag has been detected by WSU personnel, an appropriate response may be one of the following:

- Determine no response is warranted under the particular circumstances.
- Deny access to the covered account until other information is available to eliminate the red flag.
- Contact the student. (The employee confirms this action with the supervisor before initiating contact.)
- Inactivation of a network account. (The employee confirms this action with the supervisor before inactivation.)
- Notify the appropriate WSU department and cooperate with appropriate law enforcement. (The employee confirms this action with the supervisor.)

OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

The Bursar’s Office is responsible for ensuring that activities of all service providers and contractors are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Identity Theft Prevention Program

OVERSIGHT (cont.)

A service provider or contractor that maintains its own Identity Theft Prevention Program, consistent with the guidance of the red flag rules (16 *CFR* Part 681) may be considered to be meeting these requirements.

Contractors and service providers must notify WSU of any security incidents, even if such incidents have not led to any actual compromise of WSU data.

WSU contracts with third parties to collect delinquent covered accounts. The Bursar's Office requests and receives a red flag policy from each contracted service provider.