

**WEBSTER UNIVERSITY
IDENTITY THEFT PREVENTION PROGRAM**

Purpose:

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program.

Definitions:

Covered Accounts: an account that the University offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, or any other account that the University offers or maintains for which there is a reasonably foreseeable risk to customers from identity theft. A covered account includes certain types of arrangements in which an individual establishes a “continuing relationship” with the University, including billing for previous services rendered.

Customer: a person that has a covered account with Webster University.

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, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer’s Internet Protocol address, credit card number or expiration date, or bank account number and routing code.

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

Red Flag: a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Service Provider: any person or entity that provides a service to the University.

Procedure:

I. Recognizing Identity Theft

- A. Each University department which offers or maintains covered accounts must identify relevant Red Flags for that department. The following should be considered in identifying relevant Red Flags:
 - 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. Previous experiences with identity theft.
- B. The following are examples of Red Flags that should be considered recognizing potential identity theft:
 - 1. Suspicious Documents, such as the following:
 - a) Identification document or card that appears to be altered or forged, or give the appearance of having been destroyed and reassembled;
 - b) Identification document or card on which a person’s photograph or physical description is not consistent with the appearance of the person presenting the document;
 - c) Information on the identification that is not consistent with information provided by the person opening a new covered account or presenting the identification; and
 - d) Information on the identification that is not consistent with readily accessible information that is on file with the University.

2. Suspicious Personal Identifying Information, such as the following:
 - a) Identifying information presented that is inconsistent with other information the account holder or applicant provides (example: inconsistent birth dates);
 - b) Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
 - c) Identifying information presented that is associated with known fraudulent activity, such as information shown on other applications that were found to be fraudulent;
 - d) Identifying information presented that is of a type commonly associated with fraudulent activity (such as an invalid phone number or fictitious billing address);
 - e) Social security number presented that is the same as one given by another account holder or applicant;
 - f) A person fails to provide complete personal identifying information on an application when reminded to do so; and
 - g) A person's identifying information is not consistent with the information that is on file for the account holder.
3. Suspicious Account Activity or Unusual Use of Account, such as the following:
 - a) Change of address for an account followed by a request to change the account holder's name or add a additional name;
 - b) Account used in a way that is not consistent with established patterns of activity;
 - c) Mail sent to the account holder is repeatedly returned as undeliverable;
 - d) Notice to the University that an account has unauthorized activity, charges or transaction; and
 - e) The University is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that the covered account is being used for identity theft.

II. Detecting Identity Theft

- A. New Covered Accounts. University personnel will take the following steps to obtain and verify the identity of the person opening the account:
 1. Require specific identifying information, including at least full name, date of birth, and residential address; and
 2. Verify the applicant's identity (for instance, review a driver's license or other identification card);
- B. Existing Accounts. University personnel will take the following steps to monitor transactions with an account:
 1. Verify the identification of account holders if they request information (in person, via telephone, via facsimile, via email);
 2. Verify the validity of requests to change billing addresses and provide the account holder with a reasonable means of promptly reporting incorrect billing address changes; and
 3. Verify changes in banking information given for billing and payment purposes.
- C. Employment Background Report Requests. University personnel will take the following steps to assist in identifying address discrepancies:
 1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit and/or background report is made; and
 2. In the event that notice of an address discrepancy is received, verify that the credit and/or background report pertains to the applicant for whom the requested report was made and report to the appropriate agency an address for the applicant that the University has reasonably confirmed is accurate.

III. Responding to Red Flags and Mitigating Identity Theft

- A. In the event University personnel detect possible identity theft, they should take one or more of the following steps:
1. Monitor an account for evidence of Identity Theft;
 2. Contact the account holder;
 3. Change any passwords or other security devices that permit access to accounts;
 4. Notify their supervisor to determine additional steps needed;
 5. Notify law enforcement after consultation with Public Safety.

IV. Preventing Identity Theft

- A. The following steps should be taken with respect to Covered Accounts to protect those accounts from identity theft:
1. Ensure that any University website that is used to access Covered Accounts is secure or provide clear notice to all users that the website is not secure. Secure websites must be audited based upon the University's information security program to ensure that they remain secure.
 2. Ensure that paper documents which contain personal identifying information are maintained in a secure environment, and that such documents are shredded when the University no longer needs to retain them.
 3. Ensure that computer files containing personal identifying information are secure and that the only individuals who have access to such files are those with a need to access the files in order to perform their job duties.
 4. All office computers which store or access Covered Account information must be password protected and must follow all other computer security best practices as established by the University's information security program.

V. Program Administration

- A. Oversight. The Program Administrator, who has responsibility for developing, implementing and updating this Program, is the Vice President for Information Technology. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of the University's staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.
- B. Training Requirements. University staff working in departments subject to this program must complete identity theft prevention training to effectively implement the Identity Theft Prevention Program. This training will ensure that staff are knowledgeable and will be able to take steps to detect, prevent and mitigate identity theft of to the extent reasonably possible.
- C. Reporting. University employees are to notify the Program Administrator once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, University staff involved in the development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving Identity Theft and management's responses, and recommendations for material changes to the Program.
- D. Service Provider Arrangements. In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the University will take the following steps to ensure the service provider performs its contracted activities in a secure manner, and will require, by contract, that service providers have reasonable policies and procedures in place to detect, prevent and mitigate the risk of Identity Theft; and Require, by contract, that service providers review the University's Identity Theft Program and report any suspected or actual situations involving identity theft of Covered Accounts to the Program Administrator.