Seattle University
Identity Theft Prevention Program

Purpose

The purpose of the program 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 in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Definitions

Covered account means:

1. An account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions; and

2. Any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

Credit means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.

Creditor means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

Identifying information is 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, unique electronic identification number, computer's Internet Protocol (IP) address, or routing code.

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

Red flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Approved by the Board of Trustees
October 12, 2009

The Program

Seattle University establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program includes reasonable policies and procedures to:

- Identify relevant red flags for covered accounts it offers or maintains, and incorporate those red flags into the program;
- Detect red flags that have been incorporated into the Program;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Identification of Relevant Red Flags

In order to identify relevant red flags, the University and each department holding covered accounts considers:

- The *types of accounts* that it offers and maintains;
- The methods it provides to *open* its accounts;
- The methods it provides to *access* its accounts; and
- Its *previous experience* with identify theft.

The University identifies the following red flags, in each of the following five listed categories:

A. 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 a customer or applicant;
- Notice or report from a credit agency of an active duty alert for an applicant; and

- Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic;
- 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 customer information (such as if a person's signature on a check appears forged); and
- Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on the credit report);
- Identifying information presented 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 (such as an invalid phone number or fictitious billing address);
- Social Security number presented that is the same as one given by another customer;
- An address or phone number presented that is the same as that of another person;
- A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law Social Security numbers must not be required); and
- A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

- Change of address for an account followed by a request to change the account holder's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use (example: very high activity);
- Mail sent to the account holder is repeatedly returned as undeliverable;
- Notice to the University that a customer is not receiving mail sent by the University;
- Notice to the University that an account has unauthorized activity:
- Breach in the University's computer system security; or
- Unauthorized access to or use of customer account information.

E. Alerts from Others

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

Detection of Red Flags

A. New Accounts

In order to detect any of the red flags identified above associated with the opening of a new account, the University's staff will take the following steps to obtain and verify the identity of the person opening the account:

- Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
- Verify the customer's identity (for instance, review a driver's license or other government issued identification card);
- Review documentation showing the existence of a business entity; and
- Independently contact the customer.

B. Existing Accounts

In order to detect any of the red flags identified above for an existing account, the University's staff will take the following steps to monitor transactions with an account:

- Verify the identification of customers if they request information, whether in person, via telephone, via facsimile or via e-mail;
- Verify the validity of requests to change billing addresses; and
- Verify changes in banking information given for billing and payment purposes.

Response to Suspected Identity Theft

In the event University staff detects any identified red flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the red flag:

- Continue to monitor an account for evidence of identity theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account;
- Reopen an account with a new number;
- Notify the Program Administrator for determination of the appropriate step(s) to take;
- Notify law enforcement; or
- Determine that no response is warranted under the particular circumstances.

In order *to further prevent* the likelihood of identity theft occurring with respect to covered accounts, the University's staff will take the following steps with respect to its internal operating procedures to protect customer identifying information:

- Ensure that its website is secure or provide clear notice that the website is not secure;
- Ensure complete and secure destruction of paper documents and computer files containing customer information;

- Ensure that the office computers are password protected and that computer screens lock after a set period of time;
- Keep offices clear of papers containing customer information;
- Request only the last 4 digits of Social Security numbers (if any) unless the full Social Security number is required (e.g. financial aid);
- Ensure computer virus protection is up to date; and
- Require and keep only the kinds of customer information that are necessary for utility purposes.

Updating the Program

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft based on factors such as:

- The experiences of the organization with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent and mitigate identity theft;
- Changes in the types of accounts that the organization offers or maintains;
- Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Program Administration

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee ("Committee") for the University. The Committee is headed by a Program Administrator who may be the President of the University or his or her appointee. Two or more other individuals appointed by the President of the University or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for ensuring appropriate training of University 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. Staff Training and Reports

University staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of red flags and the responsive steps to be taken when a red flag is detected. University staff shall be trained, as necessary, to effectively implement the Program. University employees are expected 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 responsible for 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 response; and recommendations for material changes to the Program.

C. Oversight of Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more accounts, it will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

- Require, by contract, that service providers have such policies and procedures in place; and
- Require, by contract, that service providers review the University's Program and report any red flags to the Program Administrator.

Credit Reports: Duties Regarding Address Discrepancies

The University shall develop policies and procedures designed to enable the organization to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the organization receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.

The University may reasonably confirm that an address is accurate by any of the following means:

- Verification of the address with the consumer;
- Review of creditor's records;
- Verification of the address through third-party sources; or
- Other reasonable means.

If an accurate address is confirmed, the University shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

- The organization establishes a continuing relationship with the consumer; and
- The organization, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.