

Identity Theft Prevention Program

Purpose:

This document implements an Identity Theft Prevention Program (ITPP) as required by the Fair and Accurate Credit Transactions Act (FACT Act) of 2003. Park University has an obligation to take steps to detect, prevent and mitigate theft of personally identifiable financial information of the University's customers to the extent reasonably possible.

Definitions: The following definitions apply to this program:

Account: a continuing relationship established by a person with the University to obtain a product or service for personal, family, household or business purposes. This includes an extension of credit, such as the purchase of services involving a deferred payment.

Covered Account: 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 the University.

Identifying Information: information, such as a name or number, that may be used, alone or in conjunction with other information, to identify a specific person. Identifying information can include a person's name, address, telephone number, social security number, birth date, driver's license number, student identification number, or passport number.

Identity Theft: fraud or theft committed or attempted using the personal identifying information of another person without that person's 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.

Workplace Information Security Manual (WISM): a checklist which department administrators must complete, designed to identify and correct weaknesses in the area of information security within a given department or workplace.

Procedure:

I. Recognizing Identity Theft

- A. Each University department, college, or business unit which offers or maintains covered accounts must identify relevant Red Flags for that department, college, or business unit. 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 in identifying relevant Red Flags:

1. An alert, notification or warning from a consumer reporting agency (i.e., a fraud or active duty alert, or a credit freeze in response to a request for a consumer report).
2. Suspicious documents, such as the following:
 - a. Documents provided for identification that appear to have been altered or forged, or give the appearance of having been destroyed and reassembled;
 - b. A photograph or physical description on an identification that is not consistent with the appearance of the person presenting the identification;
 - c. Information on the identification that is not consistent with information provided by the person opening a new covered account or presenting the identification;
 - d. Information on the identification that is not consistent with readily accessible information that is on file with the University, such as a signature card or a recent check.
3. Suspicious personal Identifying information, such as the following:
 - a. Personal identifying information provided that is not consistent when compared against external information sources (i.e., the address does not match any address in a consumer report, or the social security number has not been issued or is listed on the Social Security Administration's Death Master File);
 - b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer;
 - c. Personal identifying information provided by the customer is associated with known fraudulent activity (i.e., the address or telephone number on the application is the same as the address or telephone number provided on a fraudulent application);
 - d. Personal identifying information provided by the customer is of a type commonly associated with fraudulent activity (i.e., the address is fictitious or a mail drop, or the telephone number is invalid or is associated with a pager or answering service);
 - e. The social security number provided is the same as that submitted by other customers;
 - f. The address or telephone number provided is the same or similar to the address or phone number submitted by an unusually large number of other persons;
 - g. The person opening the covered account fails to provide all required personal identifying information on an application or upon request of the University.
 - h. Personal identifying information provided is not consistent with personal identifying information that is on file with the University.
4. Unusual use of, or suspicious activity related to, the covered account, such as the following:
 - a. Shortly following the notice of a change of address of a covered account, the University receives a request for the addition of authorized users on the account;
 - b. The covered account is used in a manner that is not consistent with established patterns of activity;
 - c. Mail sent to the customer is returned repeatedly as undeliverable, although the customer continues to accrue charges on the covered account;
 - d. The University is notified of unauthorized changes or transactions in connection with a customer's covered account; and

5. 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. Opening New Covered Accounts.

In order to detect Red Flags associated with the opening of a new covered account, personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information, such as name, date of birth, home address or other identification; and
2. Verify the individual's identity by reviewing a driver's license or other government issued photo identification.

B. Existing Covered Accounts.

In order to detect Red Flags associated with an existing Covered Account, personnel will take the following steps to monitor transactions on that account:

1. Verify the identification of the individual if he/ she requests information either in person, via telephone, facsimile or email;
2. Verify the validity of any requests to change billing addresses by mail or email and provide the individual with a means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

III. **Mitigating Identity Theft**

A. In the event University personnel detect possible identity theft, they should take one or more of the following steps:

1. Contact the person who "owns" the covered account;
2. Change any passwords or other security devices that permit access to Covered Accounts;
3. Continue to monitor activity on the Covered Account;
4. Notify their supervisor to determine additional steps needed;
5. Notify law enforcement after consultation with the business unit's Identity Theft Committee representative and/or Office of General Counsel.

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 on 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.

B. Audit Requirements.

Periodic audits should be performed within the department to ensure that individuals who should not have access to such files are not accessing them. Each department subject to this program must perform an annual risk assessment by completing the Workplace Information Security Manual (WISM) annually. The manual must be completed within the first quarter of every

calendar year and submitted no later than March 31st. The completed WISM must be returned to the appropriate business unit's Identity Theft committee member. The committee members will review the WISM for completeness and accuracy and will forward the manual to the Program Administrator. The Program Administrator and the Information Security Officer (ISO) will be responsible for reviewing each completed WISM and will identify unresolved security risks that departments must address.

C. Incidents of identity theft.

Incidents of identity theft must be reported to the Program Administrator.

V. **Program Administration**

A. Oversight.

1. Responsibility for developing, implementing and updating this Program lies with the Program Administrator. The Program Administrator will designate an Identity Theft Prevention Program Committee for the University and will appoint members to this committee, including a representative from the department of Information Technology Services. A representative from the Office of General Counsel shall serve as an ex officio member of the Identity Theft Prevention Program Committee. The Identity Theft Prevention Program Committee is responsible for ensuring that University personnel are appropriately trained on this Program, for reviewing any staff reports regarding the detection of possible identity theft and steps for preventing and mitigating identity theft. The committee is also responsible for periodically reviewing and updating this Program to reflect changes in risks to Covered Accounts in the University, taking into account the University's experiences with identity theft situations and changes in detection and prevention of identity theft.
2. Program Administrator.
The Program Administrator shall be the Vice President for Finance and Administration.
3. Committee Members.
Identity Theft Prevention Program (ITPP) committee members are responsible for the implementation of the ITPP activities. Committee members are the primary point of contact for department administrators. The Program Administrator will be responsible for coordinating the activities system wide, working with Counsel and the ISO.

B. Reports.

The Program Administrator will report to the Executive Staff at least annually, on compliance by the University. The report should address material matters related to the Program, including, but not limited to, effectiveness of the policies and procedures of the University in addressing the risk of identity theft in connection with the University's covered accounts; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

C. Training Requirements.

Staff working in departments subject to this program who are involved in the creation, modification or administration of covered accounts 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 financial information of the University's customers to the extent reasonably possible. Information security awareness training is also required for all staff working in offices affected by this program. Training can be obtained by contacting the Human Resources department.

D. Service Provider Arrangements.

1. In the event the University contracts with a service provider to perform an activity in connection with one or more Covered Accounts, the University

will take the following steps to ensure that the service provider performs its contracted activities in a secure manner:

- a. Require by contract, that service providers have reasonable policies and procedures in place to prevent, detect and mitigate the risk of identity theft; and
- b. 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.

Reviewed: April 30, 2009