IDENTITY THEFT PREVENTION PROGRAM
"Red Flags"

Pursuant to the regulations implementing the federal Fair and Accurate Credit Transactions Act (FACTA), the University is required to establish an "Identity Theft Prevention Program" with reasonable to detect, identify, and mitigate identity theft in its Covered Accounts.

DEFINITIONS: The following definitions are adapted from the definitions contained in the Red Flag regulations, found at 16 C.F.R. Part 681, and shall apply to this Program:

"Covered Account" means a consumer account designed to permit multiple payments or transactions.These are accounts where payments are deferred and made periodically over time such as tuition or fee installment payment plan. It also includes any other account the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from Identity Theft.

"Customer" means any person with a Covered Account with the University.

"Identifying Information" means 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 address or routing code

"Identity Theft" means a fraud committed using the identifying information of another person.

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

"Service Provider" means a person that provides a service directly to the University.

I. Program Adoption

Pittsburg State University has adopted an Identity Theft Prevention Program (''Program'') in compliance with the "Red Flags" rules issued by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions Act ("FACTA"). The University engages in some activities that are covered by the FACTA Red Flag rules; therefore, offices or units subject to the provisions of the rules are required to develop and implement procedures in compliance with this policy. For purposes of this policy,

“Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.Responsible University Official.

II. Responsible University Official

The President designates the Chief Financial Officer to serve as the Program Administrator. The Chief Financial Officer shall exercise appropriate and effective oversight over the Program. The Chief Financial Officer may delegate day-to-day responsibility for aspects of the program to others as appropriate.

III. Program Administration and Maintenance

The Program Administrator is responsible for developing, implementing and on a periodic basis updating the Program throughout the University and will provide staff support, including the following:

- Periodic identification of Covered Accounts
- Review of public reports regarding the detection of Red Flags
- Establishment of processes for identifying, preventing and mitigating identity theft
- Determination of prevention and mitigation steps
- Periodic review of the overall Program

The Program will be periodically reviewed and updated to reflect changes in identity theft risks and technological changes, and in consideration of the University’s experiences with identity theft, changes in identity theft methods,

changes in identity theft detection, mitigation and prevention methods, changes in types of accounts the University maintains, changes in the University’s business arrangements with other entities, and any changes in legal requirements in the area of identity theft. After considering these factors, the Program Administrator, in consultation with others, will determine whether changes to the Program, including the listing of Red Flags, are warranted.

Consistent with the Program requirements set forth below, all units of the University with Covered Accounts are required to:

- Identify relevant Red Flags, as described further below, for Covered accounts it offers or maintains and incorporate those Red Flags into its unit-level policies and procedures
- Detect Red Flags that have been incorporated into the unit-level policies and procedures, as described further below
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft, as described further below
- Update periodically unit-level policies and procedures to reflect changes in risks to students, staff, faculty, the University and others from Identity Theft
- Train unit staff appropriately to effectively implement the program
- Review and exercise appropriate and effective oversight of Service Provider arrangements (such oversight shall include steps to ensure that the activity of the Service Provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft)

Affected units should designate an appropriate Identity Theft Liaison for coordination of activities under this Program.

Units may incorporate, as appropriate, existing policies, procedures and other arrangements that control reasonably foreseeable risks from Identity Theft.

Units shall report to the Program Administrator at least annually on compliance with the Program, including the effectiveness of unit policies and procedures in addressing the risk of Identity Theft, Service Provider Arrangements, management response to significant incidents involving Identity Theft and recommendations for material changes to the Program.

Any unit or department that requires access to a Consumer Report must obtain prior approval from the Director of Equal Opportunity.

IV. Identification of Relevant Red Flags

The Program shall include relevant Red Flags from the following categories, as appropriate:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services
- The presentation of suspicious documents
- The presentation of suspicious personal Identifying Information, such as a suspicious address change
- The unusual use of, or other suspicious activity related to, a Covered Account
- Notice from Customers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with Covered Accounts.

The Program shall include the consideration of the following risk factors in identifying relevant Red Flags for Covered Accounts, as appropriate:

- The types of Covered Accounts offered or maintained
- The methods provided to open Covered Accounts
- The methods provided to access Covered Accounts
- Its previous experience with Identity Theft

The Program shall incorporate relevant Red Flags from sources such as:

- Incidents of Identity Theft previously experienced
- Methods of Identity Theft that reflect changes in risk
- Applicable supervisory guidance

V. Detection of Red Flags

The Program shall address the detection of Red Flags in connection with the opening of Covered Accounts and existing Covered Accounts. At minimum, the Program Administrator and each campus department/unit administering Covered Accounts will develop and implement procedures appropriate to meet the requirements of this Program.

New Covered Accounts. In order to detect any of the Red Flags associated with the opening of a new Covered Account, University personnel will take steps to obtain and verify the identity of the person opening the Covered Account.

Existing Covered Accounts. In order to detect any of the Red Flags identified for an existing Covered Account, University personnel will take steps to authenticate customers, such as by verifying identity, and to monitor transactions with a Covered Account.

VI. Response

The Program shall provide for appropriate responses to detected Red Flags that are commensurate with the degree of risk posed. Appropriate responses may include, but are not limited to, the following:

- Monitoring a Covered Account for evidence of Identity Theft
- Contacting the Customer, student or applicant (for or about which a consumer report was run)
- Changing any passwords, security codes or other security devices that permit access to a Covered Account
- Reopening a Covered Account with a new account number
- Not opening a new Covered Account
- Closing an existing Covered Account
- Not attempting to collect on a Covered Account
- Notifying law enforcement
- Determining no response is warranted under the particular circumstances

VII. Duties of card issuers regarding changes of address

The Red Flag rules issued by the Federal Trade Commission provide, in part, that a debit or credit card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards, the card issuer receives a request for an additional or replacement card for the same account.

Under these circumstances, the card issuer may not issue an additional replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer notifies the cardholder of the request.

The University Card Center operates the University's Banana Bucks program. In order to be issued a card, the students, faculty, and staff must physically go to the Card Center Office with a valid driver's license, state issued photo identification card, military identification card, or passport. Individuals are required to show their identification to the office staff to verify their identity.

No cards are issued through the mail. Students wishing to change their address in University records must do so through the University's Registrar's Office or through GUS; faculty and staff must do so through Human Resource Services or GUS.

Issuance of credit or debit cards by a University unit other than the University Card Center is prohibited.

- Non-disclosure of Specific Practices

To ensure the effectiveness of this Identity Theft Prevention Program, it may be necessary to limit knowledge about specific Red Flag identification, detection, mitigation and prevention practices to the Program Administrator who developed this Program and to those employees with a need to know them.Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered “confidential” and should not be shared with other University employees or the public.

IX. Security Procedures

Departments/units with Covered Accounts must ensure they have sufficient physical, technical and administrative safeguards to protect the information in accordance with applicable University policies and procedures.

X. Service Provider Arrangements

In the event a University unit engages a Service Provider to perform an activity in connection with one or more Covered Account(s), the University unit should take 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. These steps should include a requirement in the contract that the Service Provider have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider’s activities, and that the Service Provider either report the Red Flags to the unit or take appropriate steps to prevent or mitigate identity theft.

Approved June 13, 2011

(Download PDF of original Policy)

Page revision date: 04/23/2018

Download PDF

Revised: 04/23/2018

Pittsburg State University