Red Flag Rule Procedures
Under Princeton University's
Identity Theft Prevention Program
Effective: December 31, 2010

Princeton University employees are responsible for detecting "Red Flags" consistent with the University's Identity Theft Prevention Policy. This document identifies the red flags that Princeton University has determined to be relevant to its business and describes appropriate practices for detection and response. Employees whose job duties involve Covered Accounts are expected to be familiar with these procedures and to also complete required training on this issue. These Red Flags are examples of activities that warrant concern; however, employees should be alert to any suspicious activity regarding covered accounts and should immediately report any suspicious activity to their supervisor.

The University categorizes Red Flags as follows:

A. Red Flags raised by notifications, alerts, and warnings from consumer reporting agencies and service providers, as well as detection services.

1. Red Flags: Alerts, Notifications, Warnings, re: Consumer Reports

a. Examples

- ❖ A consumer reporting agency provides a notice of address discrepancy.
- ❖ A fraud or active duty alert is included with a consumer report.
- ❖ A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- ❖ A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or account holder such as:
  - A recent and significant increase in the volume of inquiries
  - An unusual number of recently established credit relationships
  - A material change in the use of credit, especially with respect to recently established credit relationships
  - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor

b. Detection

A consumer report is run for certain loan applications, delinquent account assessments, and background checks for potential new hires. Consumer reports are reviewed by a loan officer, collection staff, and management personnel in the Loans

and Receivables, Real Estate Finance, and Human Resources departments. The report may contain either an alert, notification, or discrepancy or such notification may be received directly from the consumer reporting agency or a service provider vendor.

c. Response

All alerts, notifications, or discrepancies warrant action. First, attempt to determine from the applicant or account holder why the consumer reporting agency or service provider has provided an alert, notification or discrepancy.

Confirm the identity of the applicant or account holder by comparing the address and/or other identifying information with the information Princeton University has on file or by verifying the information with an appropriate 3rd party.

Advise your manager that a notice was received. Business activity regarding this applicant or account holder should be suspended while action steps are being determined by your manager. The issue and resolution of the event will be documented and sent to the Red Flag Coordinator.

B. Red Flags associated with the application process and/or consistency of the supporting information.

1. Red Flags: Suspicious Documents

a. Examples

- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- Documents provided for identification appear to have been altered or forged.
- Other information on the identification is not consistent with information provided by the person opening a new covered account.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or account holder presenting the identification.

b. Detection

Any documents presented should be critically reviewed for consistency and appearance.

New Account: Prior to opening a new account, an applicant is required to complete an application that is reviewed and approved by a department representative or loan officer. Documents used to verify identity of an applicant may include a Princeton University photo identification card or an unexpired, government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard,

such as driver's license or passport, federal income tax forms and other supporting documents.

Existing Account: The identity of the applicant or account holder is verified prior to granting access to information regarding the account. Acceptable forms of identification include a Princeton University photo identification card, a driver's license, or a passport. For telephone inquiries, the account holder must be able to provide a "shared secret", such as last 4-digits of SSN, student's account number, or any combination of non-public information.

c. Response

New Account:

1) Determine from the applicant the reason for the appearance of the application and/or inconsistency of information. If necessary, require the applicant to submit a new application or identification documents.
2) Determine if a new account should or should not be opened.

Exiting Account:

3) Continue to monitor account activity.
4) If an account was compromised, change any passwords or other security devices that permit access to covered accounts.

For either situation, take other actions, as appropriate:

5) Verify the address and affiliation status with the information Princeton University has on file.
6) Obtain verification of identity via other means such as an appropriate third-party (consumer reporting agency, dean or supervisor, etc.)
7) Determine if law enforcement should be notified.
8) Determine if nothing should be done.

Advise your manager of the suspicious documents. Business activity will be suspended and action steps determined by your manager. The issue and resolution will be documented and sent to the Red Flag Coordinator.

C. Red Flags: Suspicious Personal Identifying Information

Red Flags associated with the presentation of suspicious personal identifying information, such as suspicious address change.

1. Examples of Red Flags

- ❖ The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

- ❖ Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

    - The address on an application is the same as the address provided on a fraudulent application;
    - The phone number on an application is the same as the number provided on a fraudulent application.

- ❖ Personal identifying information provided is inconsistent when compared against external information sources. For example:

    - The address does not match any address in the consumer report;
    - The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.

- ❖ Personal identifying information provided is not consistent with personal identifying information that is in the University's central data repository (Campus Community).

- ❖ Personal identifying information provided is not consistent with other personal identifying information. For example, there is a lack of correlation between the SSN range and date of birth.

- ❖ Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

    - The address on an application is fictitious, a mail drop, or a prison;
    - The phone number is invalid, or is associated with a pager or answering service.

- ❖ The SSN provided is the same as that submitted by other persons opening an account.

2. Detection

The identity of the applicant or account holder is verified prior to opening an account, making changes to an account (e.g. address change), or providing information regarding the account.

Documents used to verify the identity of an applicant may include a Princeton University photo identification card or an unexpired, government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport.

Documents used to verify identity should be carefully examined and compared to all available information.

3. Response

If the documents and information provided appear to be suspicious after examination, then determine from the applicant the reasons for the red flags; e.g. why the application is incomplete or why there are inconsistencies with identifying information. Require the applicant to complete all required portions of the application.

Take other actions, as appropriate:

1) Verify the address and affiliation status with the information Princeton University has on file.
2) Obtain verification of identity via other means such as an appropriate third-party (consumer reporting agency, dean or supervisor, etc.)
3) Continue to monitor account activity.
4) If an account was compromised, change any passwords or other security devices that permit access to covered accounts.
5) Determine if a new account should or should not be opened.
6) Determine if law enforcement should be notified.
7) Determine if nothing should be done.

Advise your manager of the suspicious identification information. Business activity regarding this applicant will be suspended and action steps determined by your manager. The issue and resolution will be documented and sent to the Red Flag Coordinator.

D. Red Flags: Unusual Use or Suspicious Activity

Red Flags associated with the unusual use of, or other suspicious activity related to, a covered account.

1. Red Flags

- ❖ Mail sent is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account.

- ❖ Notification is received of unauthorized charges or transactions in connection with a covered account.

- ❖ Notification is received that an account holder is not receiving paper account statements.

2. Detection

Returned mail is researched by staff to identify any unusual activity regarding an account holder's change of address. Suspicious account activity may be detected or notification

received by the account holder that statements have not been received and/or that unauthorized transactions appear on their statement.

3. Response

An attempt to contact the account holder will be made by other means (e.g., phone, email) to determine the reason for the returned mail. If the address is different from the address on file, the reason for the change of address should be determined. If a change of address is required, Princeton will follow the appropriate procedures for identity verification prior to making any address change. If online secured self-service is appropriate, the account holder will be directed to the website.

Princeton University will research the reason for missing account statements and will ensure the account holder is configured to receive paper statements and/or electronic billing notifications.

In the case of unauthorized transactions, all relevant documentation will be gathered and immediately presented to your manager, who will work with law enforcement to resolve the claim, as necessary.
Take other actions, as appropriate:

1) If an account was compromised, change any passwords or other security devices that permit access to covered accounts.
2) Determine if a new account should or should not be opened or if an existing account should be closed.
3) If the account remains open, continue to monitor account activity.
4) Notify the credit reporting agency.
5) Determine if nothing should be done.

In all cases, advise your manager of the problem. Business activity regarding this applicant will be suspended and action steps determined by your manager. The issue and resolution will be documented and sent to the Red Flag Coordinator.

E. Red Flags: Notice Given

Red Flags associated with notice from students or employees, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by Princeton University.

1. Red Flag

- ❖ Princeton University is notified by a victim of identity theft, a law enforcement authority, or any other person that Princeton University has opened a fraudulent account for a person engaged in identity theft.

2. Detection

Notification acts as the detection.

3. Response

Your manager will be immediately advised of the notification and the account will be suspended while follow up occurs. The University will work with law enforcement, as necessary. The issue and resolution will be documented and sent to the Red Flag Coordinator.