Identity Theft Prevention Policy
Overview of Red Flag Rules
2011
Background

- Issued by the Federal Trade Commission (FTC) and Federal banking agencies.
- Red Flag Rules went into effect in December 2010.
- Intended to help detect and mitigate identity theft.
- New law covers creditors who regularly, and in the ordinary course of business, meet one of three general criteria. They must:
  - obtain or use consumer reports in connection with a credit transaction;
  - furnish information to consumer reporting agencies in connection with a credit transaction; or
  - advance funds to – or on behalf of – someone, except for funds for expenses incidental to a service provided by the creditor to that person.
Requirements

• Develop and implement an identity theft prevention program for new and existing accounts.

• Employees whose job duties involve covered accounts are expected to...
  • Become familiar with the Red Flag Rules procedures.
  • Complete required training.
Definitions

- **Identity Theft** - a fraud 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.

- **Covered Account** - a consumer account that involves multiple payments or transactions, such as a loan that is billed or payable monthly. Covered accounts include arrangements in which an individual establishes a continuing relationship with the University as a creditor.

- **Identifying Information** - personal information that may be used, alone or in conjunction with any other information, to identify a specific person. Includes: 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, Princeton University identification number, computer’s Internet Protocol address, or routing code.
Identifying Red Flags

- Employees are responsible for detecting “Red Flags” consistent with the University’s Identity Theft Prevention Policy*, effective December 2010.

- Red Flags are examples of activities that warrant concern.

- Identifying Red Flags in advance helps employees to spot suspicious patterns of activity.

- Be alert to any suspicious activity regarding covered accounts and immediately report it to a supervisor.

*Policy can be found on the Finance & Treasury website
Categories of Red Flags

The University categorizes Red Flags as follows:

- Alerts, Notifications, or Warnings
- Suspicious Documents
- Suspicious Personal Identifying Information (PII)
- Unusual Use or Suspicious Activity
- Notice Given
Red Flags raised by alerts, notifications, and warnings from consumer reporting agencies and service providers, as well as detection services.

**Examples of Red Flags**
- A consumer reporting agency provides a notice of address discrepancy.
- A recent and significant increase in the volume of inquiries.
• A consumer report is run for:
  • certain loan applications
  • delinquent account assessments
  • background checks for potential new hires

• Reports may be reviewed by a loan officer, collection staff, and/or management personnel in the Loans and Receivables, Mortgage Services, and HR departments.

• The report may contain either an alert, notification, or discrepancy.
Possible Response

- Attempt to determine why the agency or service provider has provided an alert, notification, or discrepancy.

- Confirm the identity of the applicant or account holder.

- Advise your manager that a notice was received.
Red Flags associated with the application process and/or consistency of the supporting information.

**Examples of Red Flags**
- An application or document appears to have been altered or forged.
- ID information is not consistent with information provided by the person opening a new covered account.
Any documents presented should be critically reviewed for consistency and appearance.

New Account:
- Department representative or loan officer reviews and approves completed loan application.
- Acceptable documents to verify identity: unexpired, government-issued ID evidencing nationality or residence and bearing a photograph or similar safeguard (e.g., driver’s license or passport).

Existing Account:
- Identity is verified prior to granting access to information regarding the account. Acceptable forms of ID include a driver’s license, passport or other unexpired, government issued ID.
- For telephone inquiries, the account holder must be able to provide a “shared secret”, which consists of non-public information.
Possible Response

New Account:
- Determine from the applicant the reason for the inconsistency of information.
- Determine if a new account should or should not be opened.

Existing Account:
- If account was compromised, change any passwords or other security devices that permit access to covered accounts.

For either situation, take other actions, as appropriate:
- Verify the address and affiliation status with the information on file.
- Obtain verification of identity via other means such as an appropriate third-party (consumer reporting agency, supervisor, etc.).
- Determine if law enforcement should be notified.
- Determine if nothing should be done.
Red Flags associated with the presentation of suspicious PII, such as suspicious address change.

**Example of Red Flag**
- The person opening the covered account fails to provide all required PII on an application or in response to notification that the application is incomplete.
- PII provided is not consistent with other identifying information.
The identity of an applicant or account holder is verified prior to:
- Opening an account
- Making changes to an account (e.g. address change)
- Providing information regarding the account

Documents used to verify identity may include an unexpired, government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard.

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

- Determine from the applicant the reasons for the red flags. Ask about inconsistencies.
- Require the applicant to complete all required portions of the application.

Take other actions, as appropriate:
- Verify the address and affiliation status with the information on file.
- Obtain verification of identity via other means such as an appropriate third-party (consumer reporting agency, supervisor, etc.).
- Continue to monitor account activity.
- If an account was compromised, change any passwords or other security devices that permit access to covered accounts.
- Determine if a new account should or should not be opened.
- Determine if law enforcement should be notified.
Unusual Use or Suspicious Activity

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

**Examples of 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.
Detection

- Returned mail is researched to identify any unusual activity regarding an account holder’s change of address.

- Suspicious activity may be detected or a notification is received explaining that statements have not been received and/or that unauthorized transactions appear on their statement.
Possible Response

Account holder is contacted by phone or email to determine the reason for the returned mail.

Address Updates
- If the address is different from the address on file, determine the reason for the change of address.
- Prior to making any address change, follow the appropriate procedures for identity verification.
- If online secured self-service is appropriate, the account holder will be directed to the website.

Missing Account Statements
- Research the reason for missing account statements.
- Ensure the account holder is configured to receive paper statements and/or electronic billing notifications.

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.
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.

**Examples of Red Flags**
- 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.
Detection & Possible Response

Detection

Notification acts as the detection.

Possible 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.
As a General Rule...

Always be prudent and professionally skeptical!

Resources Available to help you

- Peer or Co-worker
- Manager
- University Hotline
- Red Flag Rules Coordinator

University Hotline: 866-478-9804; [www.princeton.edu/compliance/hotline.html](http://www.princeton.edu/compliance/hotline.html)
Red Flag Rules Coordinator: Carolyn Ainslie
Things to Consider

• Be alert: Always be alert to suspicious activities regarding Covered Accounts.

• Always ask for proper ID or PII from the account holder to ensure authenticity.

• Ensure that office computers with access to Covered Account information are password protected.

• Always lock your computer when leaving your desk to prevent unauthorized access.

• Ensure the complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information.

• If you come across something that seems out of the ordinary, contact your manager immediately.
## Contact Information

<table>
<thead>
<tr>
<th>Contact</th>
<th>Phone Number and/or email</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Hotline</td>
<td>866-478-9804</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.princeton.edu/compliance/hotline.html">www.princeton.edu/compliance/hotline.html</a></td>
</tr>
<tr>
<td>Office of Finance and Treasury</td>
<td><a href="mailto:finance@princeton.edu">finance@princeton.edu</a></td>
</tr>
<tr>
<td>Maria Bizzarri</td>
<td><a href="mailto:mbizzarri@princeton.edu">mbizzarri@princeton.edu</a></td>
</tr>
<tr>
<td>Allison Petito</td>
<td><a href="mailto:apetito@princeton.edu">apetito@princeton.edu</a></td>
</tr>
</tbody>
</table>