

Identify Theft Prevention Program
Wilmington University
November, 2009

I. Purpose

On November 9, 2007, the Federal Trade Commission (FTC), the Federal bank regulatory agencies, and the National Credit Union Administration jointly issued regulations (72 FR 63718) requiring financial institutions and creditors to develop and implement a written identity theft prevention program. Activities that may indicate identity theft are known as “Red Flags.” The “Red Flag” regulations require implementation of an identity theft prevention program to detect, prevent and respond to patterns, practices or specific activities that may indicate identity theft. They were included in the Fair and Accurate Credit Transactions Act (FACT Act). On October 14th, 2008 the Department of Education announced the “Red Flag Rules” apply to institutions participating in the Federal Perkins Loan Program and may apply to other credit programs administered by an institution. The rule states that “creditors” holding “covered accounts” must comply with the law. The rules have a broad definition of “creditors” and “covered accounts” that is applicable to many colleges (NASFAA publication October, 23, 2008). Wilmington University seeks to be in compliance with the FACT Act and seeks to put into place training, policies and procedures to prevent the Identify Theft of students, faculty, alumni and staff.

II. Program Administration

- Responsibility for developing, implementing and updating the Program lies with an Identity Theft Committee. The committee is headed by a Program Administrator. The Program Administrator will be responsible for ensuring the appropriate training of WU staff on the Program, for being a point of contact for particular circumstances of risk, for involving other departments as needed, and for considering periodic changes and auditing of the Program.
- WU staff responsible for implementing and maintaining the Program shall be trained by their management under the direction of the Program Administrator. All individuals who access confidential account information will be educated in the detection of Red Flags and the responsible steps to take when a Red Flag is detected.
- The committee will review and update this Program annually to reflect changes in risks to students, faculty and staff. Any risks that were identified or any other potential vulnerabilities of the security of the system will be addressed and incorporated into the Program.
- A log will be maintained to record incidents of Red Flags and ensuing action taken. The Program Administrator will report number of incidents annually

to the Executive Team and recommend changes needed, if necessary, to strengthen the policy.

III. Definitions

“Identity Theft” is a fraud committed or attempted using the identifying information of another person without authority.

A “Red Flag” is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

A “Covered Account” includes all student, faculty, alumni and employee accounts.

“Program Administrator” is the individual designated with primary responsibility for oversight of the Program.

University Community is comprised of faculty, staff, students and alumni.

IV. Covered Accounts include, but are not limited to:

- Federal Loan Programs
- Employee accounts, files and records
- Student accounts
- Faculty accounts
- Alumni records

V. Identification of Red Flags

The 26 Red Flags or alerts that are outlined in the regulation are included as Appendix I. Key signs are the following:

- Identification document or card that appears to be forged, altered or inauthentic, or does not look consistent with the person presenting the document
- Identifying information presented that is inconsistent with other information the employee, alum or student provides (e.g. birth dates) or information that is inaccurate (e.g. addresses and social security or other identification numbers)
- Unauthorized activity on an account which may be a result of attempts to gain unauthorized access into another person’s account.
- Opening or maintaining of a fraudulent account
- Notification by a member of the University Community of unauthorized access to or use of another’s account information
- Notification of a loss of or an unauthorized person being in possession of hardware or software that contains account information

- Notification by a third party vendor of attempts to retrieve access to an account or fraudulent activity (e.g. Higher One, Presidium, National Clearing House, credit reporting agencies) by unauthorized users
- Notification to the University from an Identity Theft victim, law enforcement, or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft

VI. Detecting Red Flags

Agreed upon steps will be taken by any person providing private University community information to increase the ability to detect Red Flag behavior. These steps will be taken in face to face interactions, as well as phone and electronic interactions. Some examples of identifiers include:

- Certain identifying information such as name, date of birth, academic records, social security verification, and photo identification will be included in the authentication process.
- Where appropriate, unique challenge questions will be inserted into the verification process to reduce ability to break into another's account.

The University will also request and maintain the Identity Theft Prevention Programs of the organizations that give confidential information to students.

VII. Responding to Red Flags

In the event University personnel detect any identified Red Flags, the appropriate staff member, student service employee, Program Administrator or IT staff, shall take all appropriate steps to respond and mitigate identity theft depending on the degree and nature of risk posed by the Red Flag, including but not limited to the following examples:

- Continue to monitor the account for evidence of Identity Theft.
- Identify the facts associated with the incident.
- Fill out the designated Identity Theft Form and forward to Program Administrator electronically or on paper. (Appendix II)
- Take necessary precautions to freeze the account or prevent Identity Theft incident if possible.
- Communicate to the person whose identity may have been compromised.
- Change any passwords or other security devices that permit access to accounts.
- Take other recommended actions to mitigate risk.

VIII. Prevention and Mitigation of Identity Theft

In order to prevent the likelihood of identity theft occurring with respect to covered accounts, the University will take the following steps with its internal operating procedures to protect University community identity information:

- Ensure systems are secured and that authentication information changes frequently and at prescribed times.
- Ensure that each system has its own security mechanisms that are monitored

IX. Additional Sound Practices

- Take precautions with printed and electronic reports to minimize opportunities for social security numbers and other identifying information to be compromised. Therefore, reports will mask SSNs by indicating xxx-xx- last 4 digits.
- Investigation of instances of repeated attempts to access an account with multiple lockouts. The Information Technology department will define which repeated attempts to access an account are unacceptable and communicate these instances.
- More thorough monitoring and alerts of all confidential information systems will be developed.
- Training will be done for all staff that has access to student, alumni, faculty or staff records. This training will be documented and available through a tutorial, as well as on paper.
- The Identity Theft policy, tutorial and form will be added to our website.
- Each department will define the procedures for ensuring proper verification takes place.
- The Employee Handbook will be updated.

Some portions of this document were taken from policies from the following institutions:

- University of Massachusetts
- Ohio State University
- Carroll Community College
- The Federal Trade Commission Business Center

Appendix I
26 Red Flags

1. A fraud alert included with a consumer report
2. Notice of a credit freeze in response to a request for a consumer report
3. A consumer reporting agency providing a notice of address discrepancy
4. Unusual credit activity, such as an increased number of accounts or inquiries
5. Documents provided for identification appearing altered or forged
6. Photograph on ID inconsistent with appearance of customer
7. Information on ID inconsistent with information provided by person opening account
8. Information on ID, such as signature, inconsistent with information on file
9. Application appearing forged or altered or destroyed and reassembled
10. Information on ID not matching any address in the consumer report, Social Security number has not been issued or appears on the Social Security Administrator's Death Master File, a file of information associated with Social Security numbers of those who are deceased.
11. Lack of correlation between Social Security number range and date of birth
12. Personal identifying information associated with known fraud activity
13. Suspicious addresses supplied, such as a mail drop or prison, or phone numbers associated with pagers or answering service
14. Social Security number provided matches that submitted by another person opening an account or other customers
15. An address or phone number matching that supplied by a large number of applicants
16. The person opening the account unable to supply identifying information in response to notification that the application is incomplete
17. Personal information inconsistent with information already on file
18. Person opening account or customer unable to correctly answer challenge questions
19. Shortly after change of address, creditor receives request for additional users of account
20. Most of available credit used for cash advances, jewelry or electronics, plus customer fails to make first payment
21. Drastic changes in payment patterns, use of available credit or spending patterns
22. An account that has been inactive for a lengthy time suddenly exhibits unusual activity
23. Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account
24. Customer indicates that they are not receiving paper account statements
25. Customer notifies that there are unauthorized charges or transactions on customer's account
26. Institution notified that it has opened a fraudulent account for a person engaged in identity theft



Identity Theft Incident Form

Nature of Incident	
Name of Identity Theft Victim	
Identifying Information Of Victim	
Your Name (Person Reporting the Incident)	
Your Department	
Your Phone Number	
Date of Incident	
Additional Information	

Please print the form and send it via inter-office mail to Red Flag Administrator, Dave Lewis in the Pratt Building at the New Castle site . If there are any questions, please call Dave at 356-6824. If Dave is not available, please contact the Executive Director of University Safety, Dr. Jack Cunningham at john.l.cunningham@wilmu.edu or 356-6921.