Responsible University Officials: Controller, Director of Student Accounts, Compliance Office, Campus Safety and IT
Responsible Office: Finance
Origination Date: September 2014

Policy 6.6

IDENTITY THEFT PREVENTION

POLICY STATEMENT

This policy requires affected Roosevelt University departments to develop and implement Identity Theft Prevention Programs that include reasonable policies and procedures to:

1. Secure personal identifying information and, thereby, reduce opportunities for identity theft;
2. Identify patterns, practices, and specific forms of activity that indicate possible opportunities for identity theft ("Red Flags");
3. Detect Red Flags that signal potential identity theft situations;
4. Execute an incident response plan when a suspected identity theft occurs;
5. Train staff, faculty, and contractors so that University employees and contractors are aware of identity theft risks and appropriate responses for their departments; and
6. Schedule an annual review of the Identity Theft Prevention Program, related training, and service provider compliance.

The goal of an effective Identity Theft Prevention Program is to assure that personal identifying information collected and managed by the University is secure. This document provides guidance for individual departments to establish programs to identify and respond to the specific identity theft risks in their units.

The Red Flags Rule, Section 114 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003 issued by the Federal Trade Commission (FTC), requires financial institutions and creditors that hold accounts covered under the regulation to develop and implement an identity theft prevention program for new and existing accounts.

Universities are subject to this regulation where a department establishes an account or processes an application for an account ("a covered account"):

- That allows an individual to make periodic payments to the University; or
- For which there is a reasonably foreseeable risk of identity theft to an individual or to the safety and soundness of the University, including financial, operational, compliance, reputation, or litigation risks.

The FTC Red Flags Rule does not address all situations where risks of identity theft may present themselves at the University. For example, internal use of credit cards and procurement cards for payments, acceptance of credit cards for purchases of items sold by University units, as well as numerous other activities at Roosevelt University may not technically involve "covered accounts" as defined by the FTC. Nonetheless, University schools and departments are responsible for defining and communicating appropriate procedures to protect personal identifying information in all situations where employees and/or contractors come in contact with it.

REASON FOR POLICY/PURPOSE

Through the Identity Theft Prevention policy and procedures outlined in this document, Roosevelt University intends to comply with the FTC Red Flags Rule identity theft detection and prevention guidelines. The purpose of University departments establishing effective identity theft prevention programs is to secure personal identifying information provided to the University by individual students, faculty, staff, or others, and thereby prevent its unauthorized and fraudulent use.

TABLE OF CONTENTS

WHO APPROVED THIS POLICY

CFO
Board of Trustees

WHO NEEDS TO KNOW THIS POLICY

All departments that collect and/or process personal identifying information as outlined in this document.

DEFINITIONS

Account holder	An individual who has established an account at the University that is covered by the FTC Red Flags Rule (a "covered account")
Covered account	Any account established by the University or for which the University accepts an application: • That allows an individual to make periodic payments to the University, or • For which there is a reasonably foreseeable risk of identity theft to an individual or to the safety and soundness of the University, including financial, operational, compliance, reputation, or litigation risks
Identity theft	A fraud committed or attempted using the "personal identifying information" of another person without authority
Personal identifying	Credit card information, tax identification numbers, Social Security numbers, payroll information, medical information, account security codes or PIN numbers, or any other information associated with an individual that could identify a specific person by itself or in combination with other information
Red Flags	Patterns, practices, and specific forms of activity that indicate possible opportunities for identity theft
Service Provider	An external entity that, in order to provide a contracted service to the University, has access to University "covered accounts", University "covered account" applications, and/or any "personal identifying information" associated with those accounts or with University employees or contractor

POLICY/PROCEDURES

PROCEDURES FOR AN EFFECTIVE IDENTITY THEFT PREVENTION PROGRAM

Each department's Identity Theft Prevention Program should be customized to the size, complexity, nature and scope of its particular activities.

The intent of each department's Program is to protect students, faculty, staff, and other University constituents, and the University itself from damages resulting from the fraudulent activity of identity theft. The FTC guidelines focus on identity theft risks associated with the opening of a new account or to the maintenance or use of any existing account at the University that is covered under the FTC Red Flags Rule.

A complete Identity Theft Prevention Program includes procedures for each of the following steps:

1. Secure personal identifying information

It is the responsibility of each department to secure all personal identifying information that they come in contact with and, thereby, reduce opportunities for identity theft.

a. Personal identifying information
The following sensitive information must be secured whether stored in paper (hard copy) or electronic format:

1) Credit card information, including any of the following:
- Credit card number (in part or whole)
- Credit card expiration date
- Cardholder name
- Cardholder address

2) Tax identification numbers, including:
- Social Security number
- Business identification number
- Employer identification numbers

3) Payroll information, including, among other information:
- Paychecks
- Paystubs

4) Medical information, including but not limited to:
- Doctor names and claims
- Insurance claims
- Prescriptions
- Any related personal medical information

5) Other personal information, examples of which include:
- Date of birth

• Address
• Phone numbers
• Maiden name
• Names

b. Best practices
Best practices for securing documents and data, verifying identity, and monitoring service provider compliance are outlined below.

1) Best practices for paper documents:

• File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive data must be locked when not in use.
• Storage rooms containing documents with sensitive data and record retention areas must be locked at the end of each workday or when unsupervised.
• Desks, workstations, work areas, printers and fax machines, and common shared work areas must be cleared of all documents containing sensitive data when not in use.
• Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas containing personal identifying information must be erased, removed, or shredded when not in use.
• University records may only be destroyed in accordance with the University's records retention policy and applicable law.
• Documents containing personal identifying information must be destroyed in a secure manner such as via document shredding.

2) Best practices for electronic documents and data:

• Personal identifying information in an electronic format must be protected from unauthorized access or disclosure at all times and may only be transmitted using approved methods including encryption as required using a University approved encryption program.

3) Best practices for identity verification

Before an individual may open an account, his/her identity must be verified to determine if s/he is actually the person s/he claims to be. Similarly, before an individual may access or be provided with information concerning an existing account, s/he must demonstrate that s/he is authorized to access the account. Be sure to consider the different ways that an account-holder interacts with the school or department regarding their new or existing account including in-person, via phone, mail, or email, or online through a system.

• For opening a new account
Check a current government-issued identification card, like a driver's license or passport.

• For existing accounts
An account holder may be asked to enter previously established confidential passwords and PIN numbers online to verify his/her identity and gain access to his/her existing account. For higher-risk situations, multi-factor authentication techniques including using passwords, PIN numbers, smart cards, tokens, and biometric identification are

recommended. The University will never ask account holders to share their password or PIN with anyone else. Certain types of personal information – like a Social Security number, date of birth, mother's maiden name, or mailing address – are not good authenticators because they are so easily accessible.

4) Best practices for service provider compliance

• Service providers that handle University accounts covered by the Red Flags Rule must comply with the standards and best practices outlined in the University's Identity Theft Prevention Guidelines and the department's Identity Theft Prevention Program. A provision in the University's contract with the service provider that requires them to have compliant policies and procedures in place will obligate the service provider to meet University Red Flags Rule standards. Service provider performance relative to identity theft prevention procedures can be monitored by the department by conducting an annual assessment of the service provider's policies and procedures and by requiring reports from the service provider about incidents detected and their responses.

2. Identify Red Flags

Identify patterns, practices, and specific forms of activity that indicate possible opportunities for identity theft ("Red Flags") in the department.

The FTC has identified twenty-six Red Flags for possible incorporation into an identity theft prevention program. The department should review these Red Flags and determine which situations constitute risks for the accounts they are responsible for and what personal identifying information might be involved. Each applicable Red Flag should be included in the department's Identity Theft Prevention Program documentation. Each applicable Red Flag should be described in detail in language that employees and contractors in the area can readily understand. Each potential identity theft situation should be listed along with the related personal identifying information and specific accounts involved. It is important for the generic descriptions of the FTC Red Flags to be customized to the department's accounts, activities, forms, reports and computer applications so that employees and contractors can clearly and easily identify Red Flag situations.

The twenty-six FTC-defined Red Flags are grouped in five sections, a-e, below. A sixth category, section f, has been added to include possible red flags arising from identity theft experience within the University and recent guidance disseminated by the University.

a. Consumer reporting agency/credit bureau alert or notice

1) A fraud or credit alert is included with a consumer report from a consumer reporting agency. This indicates that identity fraud is suspected.
2) A notice of credit freeze on a consumer report is provided from a consumer reporting agency. A credit freeze prevents updates to consumer data such as name, address, SSN and date of birth due to suspected identity fraud.
3) A consumer reporting agency provides a notice of address discrepancy.
4) A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a customer.

b. Suspicious documents

5) Documents provided for identification appear to have been altered or forged.

6) The photograph or physical description on the identification is not consistent with the appearance of the customer presenting the identification.
7) Other information on the identification is not consistent with information provided by the person opening an account or presenting the identification.
8) Other information on the identification is not consistent with readily accessible information that is on file with the University.
9) An application appears to have been altered or forged, or gives the Appearance of having been destroyed and reassembled.

c. Suspicious personal identifying information
(Refer to the personal identifying information outlined in the step 1 above.)

10) Personal identifying information provided is inconsistent when compared against external information sources used by the University.
11) Personal identifying information provided by the account holder or applicant is not consistent with other personal identifying information provided by the same individual.
12) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University.
13) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by the internal or third-party sources used by the University.
14) The Social Security Number provided is the same as that previously submitted by other persons opening an account or an existing account holder.
15) The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts.
16) The person opening the account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17) Personal identifying information provided is not consistent with personal identifying information that is on file with the University.
18) If the University uses a challenge question, the account holder or applicant cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

d. Unusual use of, or suspicious activity related to, a covered account

19) Shortly following the notice of a change of address, the University receives a request for a new or replacement card (for accounts for which a card is issued), or the addition of authorized users on the account.
20) A new revolving credit account is used in a manner commonly associated with known patterns of fraud.
21) An account is used in a manner that is not consistent with established patterns of activity on the account.
22) An account that has been inactive for a reasonably lengthy period of time is used.
23) Mail sent to the account holder is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account.
24) The University is notified that the account holder is not receiving account statements.
25) The University is notified of unauthorized charges or transactions in connection with an account.

e. Notification regarding possible identity theft

Notification in connection with covered accounts may be provided to the University by account holders, victims of identity theft, law enforcement authorities, or other person.

26) The University is notified by an account holder, a victim of identity theft, a law enforcement authority, or anyone else that the University has opened a fraudulent account for a person engaged in identity theft.

f. University experience and guidance
In addition to the Red Flags provided by the FTC above, departments should also incorporate applicable identity theft experience of the University or department such as:

- Actual past incidents of identity theft
- Additional methods of identity theft that the University has identified that reflect changes in identity theft risks
- Updates from University Identity Theft Prevention Guidelines

3. Detect Red Flags

Red Flags signal potential identity theft situations. Each employee or contractor who comes in contact with personal identifying information in any form must be aware of the potential identity theft situations for his/her area and job responsibilities as outlined in the department's Identity Theft Prevention Program. The employee must be prepared to initiate the appropriate action steps to be taken in accordance with the department's Identity Theft Prevention Program when fraudulent activity is suspected. Any time an employee suspects fraudulent activity involving personal identifying information and/or University accounts, the employee should assume that the department's Identity Theft Prevention Program applies and s/he should immediately follow protocols established by his/her unit for reporting the suspected identity theft incident.

If an employee suspects fraudulent activity, reports the activity to his/her supervisor or other designated individual in the department, and does not believe that the appropriate follow up action is taken according to the published Identity Theft Prevention Program for the school or department, s/he may file a report.

4. Execute an incident response plan

When a potential Red Flag is detected, the department should respond to the suspected identity theft by contacting the Campus Safety to protect from further damages and loss.

a. Immediate response to a suspected identity theft
The department should:

1) Maintain confidentiality concerning the suspected identity theft particularly if department employees may be involved.
2) Designate a contact person within your organization for gathering and releasing information. This person will be the primary contact between the department and the Office of Risk Management, Campus Safety, and for all information released within the University or outside of it.
3) Gather all documentation related to the suspected fraudulent activity.
4) Write a description of the situation. This should include how the incident was discovered, who discovered the incident, when and where the incident occurred.
5) Present this information to the Roosevelt University Campus Safety.
6) Contact the University Office of Risk Management to alert them to the situation and seek their advice before contacting potentially affected account holders or applicants, service providers, banks, credit issuers, or credit bureaus.
7) Review your response plan, including the advice of the Office of Risk Management, with Campus Safety to make sure no action will interfere with or impede their investigation.

b. Role of University's Campus Safety

Campus Safety shall initiate response and notification protocols contained in the Roosevelt University Information Security Incident Response Protocol if the facts of the case indicate that the reported incident is an Information Security Incident. The department will continue to cooperate with Campus Safety throughout the investigation as they further investigate whether the activity is fraudulent and take appropriate action.

c. Additional incident response steps
Additional steps may be taken to protect the account holder and the University. The appropriate response may depend upon the degree of risk posed by the situation, the confidentiality required, possible legal obligations related to the account, particularly related to termination of service, and advice of the RU Office of Risk Management. The facts of a particular case may warrant using one or several of the following steps or other responses determined to better suit to the situation.

Appropriate actions may include, but are not limited to, the following:

- Cancel the suspected fraudulent transaction if possible.
- Account actions:
  - Monitor the affected account for further evidence of identity theft.
  - Change any passwords, security codes or other security devices that permit
    - Access to the affected account.
    - Place a 'hold' on the affected account.
    - Close the affected account.
    - Reopen the account with a new account number.
    - Do not open the new account.
    - Delay collection activity on the affected account.
    - Delay transferring/selling the account to a third-party outside of the University.

- Notifications:
  - Notify faculty, staff and contractors in the unit of the occurrence
  - Notify the affected account holder or applicant that identity fraud has been attempted.
    - Notify affected service providers who exchange relevant data with Roosevelt University.
    - Advise credit bureaus if a large number of University account holders are being advised to request fraud alerts for their files.
- Determine that no action is necessary at this time.

5. Train employees and contractors

University employees and contractors must be aware of identity theft risks and appropriate responses for their department. Each affected department will provide training on an annual basis for its faculty, staff, and contractors who come into contact with accounts covered by the Red Flags Rule. The rule requires that relevant staff only be trained as "necessary" – for example, staff that has received anti-fraud prevention training may not need to be re-trained each year if no changes are made to the Program. Remember, though, that employees at many levels of the organization can play a key role in identity theft deterrence and detection.
Training will also be provided on an ongoing basis as changes are incorporated into the University's Identity Theft Prevention Guidelines or the department's Identity Theft Prevention Program.

6. Schedule an annual review of the Program

Annually, each affected school or department will schedule a risk assessment for all accounts covered by the Red Flags Rule including a review of their Identity Theft Prevention Program. The risk assessment should include controlled monitoring and testing of their identity theft prevention procedures.

The annual risk assessment and Program review should especially take into consideration:

- Effectiveness of the current Program
- Changes in methods to open accounts
- Changes in methods to access existing accounts
- Changes in methods of contact with account holders affecting identity verification procedures
- Changes in recommended methods to detect, prevent, and mitigate identity theft
- Previous, and especially recent, experience with identity theft in the school or department and in the University
- Changes in the business arrangements of the school or department, including changes in service provider arrangements
- Effectiveness of school or department procedures for monitoring service provider compliance
- Changes in service provider procedures for compliance with University and department requirements

As a result of the annual review, the department should update their Identity Theft Prevention Program, training materials, and service provider monitoring procedures as necessary. Once the Program, training materials and monitoring procedures are updated, the department must make sure all affected faculty, staff, contractors, and service providers are aware of and implement the changes.

RELATED INFORMATION

Red Flags Rule references:

- FTC Guide and Tutorial: "Protecting Personal Information, A Guide for Business" http://www.ftc.gov/infosecurity/

- FTC: "Fighting Fraud with the Red Flags Rule, a How-to Guide for Business" http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml

- NACUBO FTC Red Flags Rule Initiative page, including links to other reference materials: http://www.nacubo.org/Initiatives/FTC_Red_Flags_Rule.html

HISTORY/REVISION DATES

Origination Date: April 2014