NUMBER: FINA 4.12 (formerly BUSF 4.12)

SECTION: Administration and Finance

SUBJECT: University Identity Theft and Detection Program

DATE: March 3, 2011

REVISED: March 8, 2016

Policy for: All Campuses and All Service Providers Subject to the "Red Flags Rule"
Procedure for: All Campuses
Authorized by: Vice President for Finance and Chief Financial Officer
Issued by: University Finance – Bursar's Office

Congress amended the Fair Credit Reporting Act in 2003 by enacting the Fair Trade and Accurate Credit Transaction Act of 2003 (FACT Act). The FACT Act required the Federal Trade Commission (FTC) to issue regulations that require "Creditors" to adopt policies and procedures to prevent identity theft. The FTC subsequently promulgated regulations that are known collectively as the "Red Flags Rule." The Red Flags Rule requires "Financial Institutions" and "Creditors" holding "Covered Accounts" to develop and implement a written Identity Theft prevention program designed to identify and respond to Red Flags that are detected in order to prevent or mitigate Identity Theft. The Red Flags Rule applies to the University because the University meets the definition of "Creditor" set forth in the regulations, and because the University holds "Covered Accounts" as defined by the regulations.

I. Policy

A. The purpose of this policy is to establish an Identity Theft Prevention Program to ensure that the University complies with the Red Flags Rule ("the Rule") and to establish procedures to prevent, detect, and mitigate Identity Theft.

Pursuant to this policy, each campus shall:

1. Identify all Covered Accounts maintained by departments on campus.

2. Require each department that is affected by the Rule to create an Identity Theft plan consistent with the University's Identity Theft Prevention Program described herein.

3. Review and update departmental plans on an annual basis.

B. Definitions

1. "Account" means a continuing relationship established by a person with the University to obtain a product or service for personal, family, household or business purposes.

2. "Covered Account" means: (a) an account that constitutes a continuing financial relationship between the University and a person for a service, or that is designed by its nature to permit multiple payments or transactions between the University and a person for a service. By way of examples, "Covered Accounts" may include Perkins Loan accounts, institutional loan accounts, internal tuition payment plan accounts, and tuition payment plan accounts administered by a payment plan Service Provider, or (b) any other account the University offers or maintains for which there is a reasonably foreseeable risk of Identity Theft to holders of the account.

3. "Customer" means a person that has a Covered Account with the University.

4. "Identity Theft" means a fraud committed or attempted using identifying information of another person without authority.

5. 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, but not limited to:

    a. Name
    b. Address
    c. Telephone number
    d. Social security number
    e. Date of birth
    f. Government-issued driver's license or identification number
    g. Alien registration number
    h. Government passport number
    i. Employer or taxpayer identification number
    j. Individual identification number
    k. Bank or other financial account routing code

6. "Red Flag" means a pattern, practice, alert or specific activity that indicates the possible existence of Identity Theft.

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

II. Procedures

The Chief Financial Officer (CFO) shall oversee the Identity Theft Prevention Program.

The CFO shall ensure that each University department that maintains Covered Accounts ("affected department") implements the following Program:

A. Creation and Implementation of Departmental Plans and Training

1. Each affected department shall develop and implement a written plan that identifies administrative controls designed to prevent, detect, and respond to Red Flags in connection with opening of a Covered Account or administering an existing Covered Account.

2. Each University department that is not an affected department on the date this policy becomes effective shall periodically determine whether it offers or maintains Covered Accounts and, if it offers or maintains Covered Accounts, it shall develop a written plan in accordance with this policy.

3. Each departmental written plan shall (a) identify and document Covered Accounts, (b) identify potential sources of Red Flags, including but not limited to notifications from credit reporting companies, suspicious documents, suspicious account activity, and suspicious identifying information, (c) identify actions to be taken to verify identity and verify the validity of address changes, (d) identify actions to be taken to respond to and to mitigate Identity Theft if it is discovered, (e) establish procedures to review the written departmental plan on an annual basis, and (f) establish procedures to ensure that departmental employees are aware of this Policy and the written departmental plan and are trained in the procedures established by the department to detect and respond to Red Flags.

4. The head of each affected department (or his or her designee) shall conduct an annual risk assessment to review methods used to open Covered Accounts, methods used to access Covered Accounts, any previous experiences with Identity Theft, and any new risks or threats that have emerged since the most recent review. The head of each affected department (or his or her designee) shall update the written departmental plan on an annual basis.

B. Red Flags

Affected departments shall monitor activity connected with Covered Accounts for the detection of Red Flags. Examples of Red Flags identified by the Federal Trade Commission are as follows:

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or Customer, such as (a) a recent and significant increase in the volume of inquiries; (b) an unusual number of recently established credit relationships; (c) a material change in the use of credit, especially with respect to recently established credit relationships; or (d) an account that was closed for cause or identified for abuse of account privileges by the University.

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 applicant or Customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or Customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the University, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the University. For example: (a) the address does not match any address in the consumer report; or (b) the Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

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

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example: (a) the address on an application is the same as the address provided on a fraudulent application; or (b) the phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University. For example: (a) the address on an application is fictitious, a mail drop, or a prison; or (b) the phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other Customers.

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 or by other Customers.

16. The person opening the covered account or the Customer 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 challenge questions, the person opening the covered account or the Customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the University receives a request for a new, additional, or replacement card or a cell phone, or for 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. For example: (a) the majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or (b) the Customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A Covered Account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: (a) nonpayment when there is no history of late or missed payments; (b) a material increase in the use of available credit; (c) a material change in purchasing or spending patterns; (d) a material change in electronic fund transfer patterns in connection with a deposit account; or (e) a material change in telephone call patterns in connection with a cellular phone account.

22. A Covered Account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the Customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Customer's Covered Account.

24. The University is notified that the Customer is not receiving paper account statements.

25. The University is notified of unauthorized charges or transactions in connection with a Customer's Covered Account.

C. Reporting and Responding to Incidents

As indicated above, each departmental plan shall identify actions to be taken in response to and in mitigation of Identity Theft if it is discovered, including but not limited to the following:

1. An employee who detects a Red Flag shall report the detection to his or her supervisor or other appropriate administrator (department head or designee) as provided in the departmental plan.

2. Departmental responses to detection of Red Flags may include, but are not limited to, (a) monitoring and/or examining a Covered Account for evidence of Identity Theft, (b) contacting the Customer, (c) changing passwords, security codes, or other security devices that permit access to a Covered Account, (d) reopening a Covered Account with a new account number, (e) not opening a new Covered Account, (f) closing an existing Covered Account, (g) notifying law enforcement, or (h) determining that no response is warranted under the circumstances.

If upon investigation it appears to the department head or designee that Identity Theft has occurred, then the department head or designee shall inform University Law Enforcement and Safety, the University Risk Manager, and the Office of General Counsel of the incident.

D. Service Providers

If an affected department contracts with a Service Provider to perform an activity in connection with a Covered Account, then the affected department shall ensure that the contract between the parties requires the Service Provider to (1) have reasonable policies and procedures in place to detect, prevent and mitigate Identity Theft, (2) review the affected department's written Identity Theft plan, and (3) report any Red Flags that it detects to the department head or designee.

III. Reason for Revision:

Change is needed due to departmental reorganization and name changes.