IDENTITY THEFT PREVENTION PROGRAM

Title: Identity Theft Prevention Program

Type: Administrative

Number: 41-07 (2014)

Approved: 05/12/2015

Responsible Office: University Controller

Responsible Executive: Vice President for Finance and Administration

Applies to: University Community

POLICY STATEMENT

The Norfolk State University Board of Visitors has directed the Division of Finance and Administration to implement Federal regulations, commonly referred to as the "Red Flags Rule" to combat identity theft (see BOV Policy #24 (2016) Statement on Identity Theft Prevention). The Red Flags Rule was issued in 2007 by the Federal Trade Commission and federal banking regulatory agencies under sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003, Public Law 108-159 and requires creditors (as defined in these regulations) to develop a written program which includes reasonable policies and procedures to identify, detect, and respond to relevant Red Flags for covered accounts to prevent and mitigate identity theft.

TABLE OF CONTENTS — PAGE NUMBER

PURPOSE

The purpose of this policy is to establish procedures that will ensure compliance with the Federal Trade Commission's "Red Flags Rule." These procedures provide for the identification, detection and response to patterns, practices, or specific activities known as "Red Flags" that could indicate the possible risk of identity theft.

CONTACTS

The University Controller officially interprets this policy and is responsible for matters pertaining to this policy as it relates to students. The Vice President for Finance and Administration is the Executive responsible for obtaining approval for any revisions as required by BOV Policy # 01 (2014) *Creating and Maintaining Policies t*hrough the appropriate governance structures. Questions regarding this policy should be directed to the University Controller.

DEFINITIONS

Confidential Data: includes information that the University is under legal or contractual obligation to protect.

Covered Account: an account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. All student accounts or loans that are administered by the University are covered accounts.

Identifying Information: any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: 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, student identification number, computer's internet protocol address; credit card or other account information such as credit card number (in whole or in part), and credit card expiration date; payroll information such as paycheck, paystub, or bank account/routing number.

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

Need to Know: authorization is given to user for whom access to the information must be necessary for the conduct of one's official duties and job functions as approved by the employee's supervisor.

Public Record: is a record or data item that any entity, either internal or external to the College, can access.

Program Administrator: the individual designated with primary responsibility for oversight of the program (see Program Administration, page 4).

Red Flag: a pattern, practice, or specific activity that indicates the possible existence of identity theft.

THE RED FLAGS RULE IMPLEMENTATION

Under the Red Flags Rule, the University is required to establish an Identity Theft Prevention Program (Program) tailored to the size, complexity and the nature of its operation. An Identity Theft Committee (ITC) shall be established to develop a program which is comprised of existing University policies and procedures that relate to identity theft and incident reporting, along with a plan for the development of new policies and procedures in specific areas. The ITC shall include the following individuals: Controller, Assistant Controller, Bursar, ARMICS Coordinator, Chief Information Officer, Associate Vice President for Human Resources, Associate Vice President for Enrollment Management, and University Compliance Officer. The ITC shall report annually, and as requested, to the Finance and Administration Committee of the Board and the President.

The Identity Theft program shall include reasonable policies and procedures that control reasonably foreseeable risks by:

1. Identifying relevant Red Flags for covered accounts it offers or maintains and incorporating those Red Flags into the program;
2. Detecting Red Flags that have been incorporated into the Program;
3. Responding appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
4. Ensuring the Program is updated periodically to reflect changes in risks to students and employees, and to the safety and soundness of the creditor from identity theft.

Covered Accounts

The following types of accounts are identified as "Covered Accounts" administered by the University or administered by a service provider:

- University Covered Accounts:
  - Deferment of Tuition payments
  - Refunds of credit balances involving Plus Loans
  - Refunds of credit balances without Plus Loans
  - Background checks and credit reports in the employee hiring process and for students enrolled in certain programs
  - Meal plans
  - Fines or fees for parking or the Library
- Service Provider Covered Accounts:
  - Federal Perkins Loan Program
  - Tuition payment plans

IDENTITY THEFT PREVENTION PROGRAM

Program Administration

Oversight

Responsibility for the developing, implementing and updating this Program lies with an Identity Theft Committee (ITC) for the University. The Committee will be chaired by the Program Administrator or Controller who is responsible for ensuring appropriate training of the University's staff, reviewing reports regarding the detection of Red Flags, identifying the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program.

Staff Training and Reports

Training shall be conducted for all University employees for whom it is reasonably foreseeable that may come in contact with covered accounts or personally identifiable information. Training in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected shall be either by, or under the direction of the Program Administrator. Staff shall be trained as necessary to effectively implement the Program. Employees are expected to notify the Program Administrator once they become aware of an incident of identity theft or of the University's failure to comply with this Program.

Periodic Updates

At least annually or as otherwise requested, the Identity Theft Committee shall re-evaluate the Program to determine whether all aspects are up to date and applicable in the current business environment and to make recommendations for changes.

Identification of Red Flags

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with identity theft. The University identifies the following Red Flags in each of the listed categories:

Notification and Warnings from Credit Reporting Agencies - Red Flags include:

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency or a credit freeze on an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Receipt of notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

Suspicious Documents - Red Flags include:

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student information; and
4. Application for service that appears to have been altered or forged.

Suspicious Personal Identifying Information - Red Flags include:

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another student;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so; and
8. A person's identifying information is not consistent with the information that is on file for the student.

Suspicious Covered Account Activity or Unusual Use of Account - Red Flags include:

1. Change of address for an account followed by a request to the student's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the student is repeatedly returned as undeliverable;
5. Notice to the University that a student is not receiving mail sent by the University;
6. Notice to the University that an account has unauthorized activity;
7. Breach in the University's computer system security; and

8. Unauthorized access to or use of student account information.

Alerts from Others – Red Flags include:
Notice to the University from a student, 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.

Detecting Red Flags
Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

Existing Accounts
In order to detect any of the Red Flags identified above for an existing covered account, University personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

Consumer ("Credit") Report Requests
In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit report is sought, University personnel will take the following steps to assist in identifying address discrepancies:

1. Compare the address provided by the applicant on his/her employment application to the address on the credit report that is received from the consumer reporting agency; and
2. In the event of an address discrepancy, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting

agency an address for the applicant that the University has reasonably confirmed is accurate.

Preventing and Mitigating Identity Theft

In the event University personnel detect any identified Red Flags, such personnel will take one of more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Prevent and Mitigate

1. Monitor a covered account for evidence of identity theft;
2. Contact the student or applicant (for which a credit report was run);
3. Change any passwords or other security devices that permit access to a covered account;
4. 4. Not open a new covered account;
5. Provide the student with a new student identification number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. File or assist in filing a Suspicious Activity Report or "SAR;" or access the BSA E- Filing System (see How to Report Suspicious Activity, p. 8); or
9. Determine that no response is warranted under the particular circumstances.

B. Protect Student Identifying Information

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

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to covered accounts information are password protected;
4. Avoid use of social security numbers;
5. Ensure computer virus protection is up to date;
6. Require and keep only relevant student information that is necessary for University purposes;

7. Ensure file cabinets, desk drawers, overhead cabinets, and other storage space containing documents with sensitive information are locked when not in use;
8. Ensure storage rooms containing documents with sensitive information and record retention areas are locked at the end of each workday or when unsupervised;
9. Ensure desks, workstations, work areas, printers and fax machines, and common work areas are cleared of all documents containing sensitive information when not in use;
10. Ensure documents containing sensitive information are shredded before being discarded;
11. Ensure internally sensitive information is transmitted using approved University email. All sensitive information must be encrypted when stored in an electronic format; and
12. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients.

How to Report Suspicious Activity

1. Record relevant information on a Suspicious Activity Report by MSB (SAR-MSB) form available at www.msb.gov or by calling the IRS Forms Distribution Center: 1-800-829-3676.
2. Submit completed SAR to: Detroit Computing Center Attn: SAR-MSB P.O. Box 33117 Detroit, MI 48232-5980.
3. Keep a copy of the report and any supporting documentation for 5 years from the date of filing the report.

PUBLICATION

This policy shall be widely published or distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office shall make every effort to:

1. Communicate the policy in writing, electronically or otherwise, to the University community affected by this policy as soon as feasible;

2. Submit the policy for inclusion in the online Policy Library within 14 days of approval; and

3. Post the policy on the appropriate SharePoint Site and/or Website.

4. Failure to satisfy procedural requirements does not invalidate this policy.

NORFOLK STATE UNIVERSITY
We see the future in you.

IDENTITY THEFT PREVENTION PROGRAM

REVIEW SCHEDULE

Next Scheduled Review: 03/15/2021

Approved by, date: President, 05/12/15

Revision History: 9/23/2009; 05/07/2010; 04/19/2010; 09/23/2016; 03/14/2017; 03/15/2018

Supersedes: Policy # 41.216 Identity Theft Prevention Program (2010)

RELATED DOCUMENTS

- BOV Policy #24 (2016) Statement on Identity Theft Prevention https://www.nsu.edu/policy/bov-24.aspx
- Federal Trade Commission- Part 681- Identify Theft Rules https://www.gpo.gov/fdsys/pkg/CFR-2012-title16-vol1/pdf/CFR-2012-title16-vol1-part681.pdf
- Department of Treasury, Financial Crimes Enforcement Network https://www.fincen.gov/
- Bank Secrecy Act E-Filing System http://bsaefiling.fincen.treas.gov/main.html
- Office of Information Technology Policy #32.8.100 Security Control Catalog- Access Control https://www.nsu.edu/its/policies

FORMS

- Department of Treasury, Financial Crimes Enforcement Network https://www.fincen.gov/
- Bank Secrecy Act E-Filing System http://bsaefiling.fincen.treas.gov/main.html