BOARD OF TRUSTEES
Florida Atlantic University

Item: AF: A-1

AUDIT AND FINANCE COMMITTEE

Wednesday, June 17, 2009

SUBJECT: REQUEST FOR APPROVAL OF FLORIDA ATLANTIC UNIVERSITY'S IDENTITY THEFT PREVENTION PROGRAM.

PROPOSED COMMITTEE ACTION

Recommend to the Board of Trustees approval of FAU's Identity Theft Prevention Program.

BACKGROUND INFORMATION

In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACT Act) which required the Federal Trade Commission (FTC) to issue regulations requiring "creditors" to adopt policies and procedures to prevent identify theft. In 2007, the Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule. The rule requires "financial institutions" and "creditors" holding "covered accounts" to develop and implement a written identity theft prevention program designed to identify, detect and respond to "Red Flags."

It has been determined that certain FAU accounts may constitute "covered accounts", making FAU a "creditor" under the Red Flag Rule. As such, an Identity Theft Prevention Program ("ITPP") has been drafted to comply with the FTC Regulation. The proposed ITPP is designed to: (i) identify risks/red flags that signify potentially fraudulent activity within new or existing covered accounts; (ii) detect risks/red flags when they occur in covered accounts; (iii) respond to risks/red flags to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and (iv) ensure the ITPP is updated periodically to reflect changes in risks to covered account holders. A "red flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft. "Covered accounts" under the FAU ITPP include all financial accounts or loans that are administered by the University.

Specifically, the ITPP identities categories of potential red flags, i.e. alerts, notifications, or other warnings received from consumer reporting agencies or service providers; the presentation of suspicious documents; the presentation of suspicious personal identifying information; and unusual use of, or other suspicious activity related to, a covered account). The ITTP further identifies certain precautionary steps that will be taken by University personnel in obtaining and verifying the identity of persons opening a covered account and appropriate responses to the detection of red flags. The ITTP will be updated periodically and staff training will be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to FAU or its account holders.

The Red Flag Rule requires that the ITPP be approved by a creditor's governing body or a duly authorized committee thereof. For purposes of efficiency, the administration proposes that the Board's Audit & Finance Committee approve the ITPP and any future amendments. The FAU Office of Financial Affairs, with the assistance

of the Office of the General Counsel, will be responsible for the development, implementation, oversight and continued administration of the ITPP. Oversight responsibility is delegated to the Controller. Operational responsibility is delegated to the applicable supervising authorities for FAU colleges, departments or divisions with covered accounts.

IMPLEMENTATION PLAN/DATE

Upon Committee approval.

FISCAL IMPLICATIONS

None.

Supporting Documentation: Identity Theft Prevention Program

Presented by: Elizabeth F. Rubin, Associate General Counsel Phone: 561-297-3007

FAU

FLORIDA ATLANTIC UNIVERSITY

Identity Theft Prevention Program

June 17, 2009

FACT & Red Flag Rule

- Fair and Accurate Credit Transaction Act (FACT Act):
  - enacted by US Congress in 2003
  - required the Federal Trade Commission (FTC) to issue regulations requiring creditors to adopt policies and procedures to prevent identify theft

- Red Flag Rule:
  - regulation issued by the FTC in 2007
  - applies to financial institutions and creditors holding "covered accounts"
    - required to develop and implement a written identity theft prevention program designed to identify, detect & respond to "Red Flags"

FAU's Identity Theft Prevention Program

FAU's Identity Theft Prevention Program (the "Program") will help FAU:

- Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
- Detect risks when they occur in covered accounts; and
- Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed.

Program Definitions

- Identity theft
  - fraud committed or attempted using the identifying information of another person without authority;
- Covered account
  - all financial accounts or loans that are administered by FAU;
- Red flag
  - a pattern, practice or specific activity that indicates the possible existence of identity theft; and
- Personally identifiable information
  - first, middle, or last name, legal name, date of birth, addresses, telephone or wireless numbers, social security number, government-issued identification number, passport number, maiden name, account number, credit card information (number, expiration date, name, address), and emergency contact information.

Administration of the Program

- General administration
  - The Office of Financial Affairs, with the assistance of the Office of the General Counsel
    - responsible for the development, implementation, oversight and continued administration
- Oversight responsibility
  - Delegated to the Controller
- Operational responsibility
  - Delegated to the applicable supervising authorities for FAU colleges, departments or divisions with covered accounts

Identification of Red Flags

- Red flags (examples):
  - alerts, notifications, or other warnings received from consumer reporting agencies or service providers
  - suspicious documents
  - suspicious personal identifying information
  - the unusual use of, or other suspicious activity related to, a covered account

Detection of Red Flags

- Require certain identifying information to open an account;
- Verify the student's identity at time of issuance of student identification card;
- Verify identification if information is requested in person, via telephone, via facsimile, or via email;
- Verify the validity of requests to change billing addresses by mail or email; and
- Verify changes in banking information given for billing and payment purposes.

Responding to Red Flags

- Notify law enforcement
- Monitor the account for future evidence of identity theft
- Contact the account holder
- Change any passwords, security cords or other security devices that permit access to the account
- Close the account

Program Updates

- Re-evaluated periodically
- Assessment of which accounts are covered
- Red flags may be added, revised, replaced or eliminated
- Review the University's experiences with identity theft situations
- Review changes in identity theft methods
- Review changes in identity theft detection and prevention
- Review changes in the University's business arrangements with other entities

Other Program Features

- Address discrepancies (and confirmation)
- Security of personal identifying information
  - stored in locked areas/limited access
  - IRM to establish best practices for securing personal information on servers and computers
- Staff training
  - for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to FAU or its account holders
- Ensuring security practices of contractors and service providers
  - responsibility of FAU to ensure compliance with reasonable policies and procedures to detect, prevent and mitigate the risk of identity theft
  - must notify FAU of security incidents
- Proper disposal of personal identifying information

FLORIDA ATLANTIC UNIVERSITY

Office of the President
University Policy

SUBJECT:	**Effective Date:**	**Policy Number:**
IDENTITY THEFT PREVENTION PROGRAM	6-17-09	5.6
	Supersedes:	**Page** **Of**
	New	**1** **7**
	Responsible Authority:	
	Senior Vice President, Finance & Administration	

APPLICABILITY/ACCOUNTABILITY:

This policy is applicable to all members of the university community, including all employees, contractors, consultants, temporary workers, and service providers, including all personnel affiliated with third parties.

POLICY STATEMENT:

I. Purpose

To establish an Identity Theft Prevention Program ("Program") designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide continued administration of the Program in compliance with 16 C.F.R. Part 681.

This Program enables Florida Atlantic University (“FAU” or “University”) to protect existing accounts, reduce risk from identity fraud, and minimize potential damage to FAU from fraudulent new accounts. The Program will help FAU:

A. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
B. Detect risks when they occur in covered accounts;
C. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
D. Update the Program periodically, including reviewing the accounts that are covered and the identified risks that are part of the Program.

II. Definitions

A. *Identity theft* means fraud committed or attempted using the identifying information of another person without authority.
B. A *covered account* means all financial accounts or loans that are administered by FAU.

C. A *red flag* means a pattern, practice or specific activity that indicates the possible existence of identity theft.
D. *Personally identifiable information* includes the following items whether stored in electronic or printed format: first, middle, or last name, legal name, date of birth, addresses, telephone or wireless numbers, social security number, government-issued identification number, passport number, maiden name, account number, credit card information (number, expiration date, name, address), and emergency contact information.

III. The Program

FAU establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

A. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the Program;
B. Detect red flags that have been incorporated into the Program;
C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
D. Ensure the Program is updated periodically to reflect changes in risks to covered account holders.

IV. Administration of the Program

The FAU Office of Financial Affairs, with the assistance of the Office of the General Counsel, shall be responsible for the development, implementation, oversight and continued administration of the Program. Oversight responsibility of the Program is delegated to the Controller. Operational responsibility of the Program is delegated to the applicable supervising authorities for FAU colleges, departments or divisions with covered accounts.

V. Identification of Relevant Red Flags

In consideration of the types of covered accounts offered or maintained by FAU, the methods provided to open and access covered accounts, and FAU's previous experience with identity theft, FAU identifies the following red flags in each of the following categories:

A. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, including:
    1. A fraud or activity duty alert included with a consumer report;
    2. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;
    3. A notice of address discrepancy from a consumer reporting agency;
    4. Notice or report from a credit agency of an active duty alert for an applicant;
    5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. The presentation of suspicious documents, such as:
    1. Documents provided for identification that appear to have been altered or forged;

2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or account holder presenting the identification;
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or account holder presenting the identification;
4. An application appears to have been altered or forged, or gives the appearance of having been destroyed and re-assembled.

C. The presentation of suspicious personal identifying information, including:
1. Personal identifying information provided is inconsistent when compared against external information sources used by FAU;
2. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by FAU;
3. The social security number provided is the same as that submitted by another account holder;
4. 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 account holders or other persons opening accounts;
5. The account holder or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete;
6. Personal identifying information provided is not consistent with personal identifying information that is on file with FAU;
7. When using security questions, the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. The unusual use of, or other suspicious activity related to, a covered account, such as:
1. Shortly following the notice of a change of address for a covered account, FAU receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account**;**
2. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns;
3. A covered account is used in a manner that is not consistent with established patterns of activity on the account;
4. A covered account that has been inactive for a reasonably lengthy period of time is used;
5. Mail sent to the account holder is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account holder's covered account;
6. FAU is notified the account holder is not receiving paper account statements;

7. FAU is notified of unauthorized charges or transactions in connection with a covered account;
8. FAU receives notice from account holders, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by FAU;
9. FAU is notified by an account holder, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

VI. Detection of Red Flags

The Program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

A. New Accounts and Student Enrollment. In order to detect any of the Red Flags identified above associated with new accounts and 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).

B. 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 identification if information is requested in person, via telephone, via facsimile, or via email;
2. Verify the validity of requests to change billing addresses by mail or email and provide the account holder a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

VII. Responding to Red Flags

A. Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect from damages and loss. The employee must gather all related documentation and write a description of the situation. This information must be presented to the applicable supervising authority for determination. The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

Appropriate responses to the detection of red flags include:

1. Notify law enforcement;
2. Monitor a covered account for evidence of identity theft;
3. Contact the account holder;
4. Change any passwords, security codes or other security devices that permit access to a covered account;

5. Reopen a covered account with a new account number;
6. Not open a new covered account;
7. Close an existing covered account, and/or
8. Determine no response is warranted under the particular circumstances.

B. 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 account holder identifying information:

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

VIII. Periodic Updates to the Program

A. At periodic intervals established in the Program, or as required, the Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current business environment.
B. Periodic reviews will include an assessment of which accounts are covered by the Program.
C. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.
D. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to FAU and its account holders.

IX. Program Updates

The Office of Financial Affairs will periodically review and update this Program to reflect changes in risks to account holders and the soundness of the University from Identity Theft. In doing so, the University's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities shall be considered. After considering these factors, the Office of Financial Affairs will determine whether changes to the Program, including the listing of Red Flags and additional training, are warranted. If warranted, the Program shall be updated appropriately.

X. Duties Regarding Address Discrepancies

A. FAU may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the account holder;
2. Review of FAU’s records;
3. Verification of the address through third party sources; or

4. Other reasonable means.

B. If an accurate address is confirmed, FAU shall furnish the account holder's address to the consumer reporting agency from which it received the notice of address discrepancy if:

1. FAU establishes a continuing relationship with the account holder; and
2. FAU regularly and in the ordinary course of business, furnishes information to the consumer agency.

XI. Security of Personal Identifying Information Is Protected

A. All paper documents or files, as well as CDs, floppy disks, zip drives, flash drives, tapes, and backups containing personally identifiable information will be stored in a locked area.

B. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of FAU.

C. No visitor should be given any entry codes or allowed unescorted access to areas where personally identifiable information is stored.

D. Access to personally identifiable information will be limited to those with a legitimate business need for such information.

E. Information Resource Management (IRM) shall establish best practices and procedures for securing personal information on servers and computers that house personally identifiable information.

XII. Staff Training

A. Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to FAU or its account holders.

B. The Office of Financial Affairs is responsible for ensuring identity theft guidelines for all supervising authorities.

C. Employees should receive training as necessary to effectively implement the Program.

XIII. Security Practices of Contractors and Service Providers

The Program shall exercise appropriate and effective oversight of service provider arrangements.

A. It is the responsibility of FAU to ensure that the activities of all service providers and contractors are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

B. A service provider or contractor that maintains its own Identity Theft Prevention Program, consistent with the guidance of the red flag rules (16 C.F.R. Part 681) and validated by appropriate due diligence, may be considered to be meeting these requirements.

C. Any specific requirements should be specifically addressed in appropriate contract arrangements.

D. Contractors and service providers must notify FAU of any security incidents experienced, even if such incidents may not have led to any actual compromise of FAU's data.

XIV. Disposal of Personal Identifying Information

A. When documents contain personal identifying information are discarded, they should be placed inside a locked shred bin or immediately shredded.

B. When disposing of old computers and portable storage devices containing personal identifying information, a disc wiping utility program should be used.

C. Any CD-rom, DVD-rom, floppy disk, or flash drive containing personal identifying information should be disposed of by shredding, punching holes in, or incineration.

INITIATING AUTHORITY: Senior Vice President, Finance & Administration

---

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: __5.6__

Initiating Authority
Signature: _____ Date: _____
Name: _____

Policies and Procedures Review Committee Chair
Signature: _____ Date: _____
Name: _____

President
Signature: _____ Date: _____
Name: _____

Board of Trustees Audit & Finance Committee Chair
Signature: _____ Date: _____
Name: _____
