Data Security and Identity Theft Program "Red Flag Policy"

(Excerpt from Finance Policies and Procedures Manual)

5.7 Red Flag Policy

Data Security and Identity Theft Program

Stetson University is concerned about the serious issue of identity theft. Thus, the University developed this Program to establish a cohesive and integrated set of policies and practices to protect sensitive information and to detect, prevent, and mitigate identity theft in connection with covered accounts. The Program encompasses the Federal Trade Commission's "Red Flags" rule requirements and Florida data breach law requirements, with cross-references to other applicable policies that concern privacy and data security.

A. Definitions

1. "Identity theft" means fraud committed or attempted by using the identifying information of another person without authority.
2. A "covered account" means an account that the University offers or maintains— primarily for personal, family, or household purposes—and that involves or is designed to permit multiple payments or transactions. The term also encompasses any other account that the University maintains and for which there is a reasonably foreseeable risk—including financial, operational, compliance, reputation, or litigation risk—to members of the campus community or to the safety and soundness of the University regarding identity theft.
3. A "red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
4. "Sensitive information" is confidential or proprietary information that, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the individual to whom the information belongs, or to the University.

B. Program Overview:

This Program:

1. Designates responsibility for program administration, including establishing processes for training and periodic updating to reflect changes in risks to students and others, and to the safety and soundness of the University;
2. Provides guidance in protecting sensitive information;
3. Delineates specific covered accounts subject to red flag scrutiny;
4. Delineates processes for identifying relevant red flags for covered accounts the University offers or maintains;
5. Establishes processes to prevent and mitigate identity theft by detecting and responding appropriately to red flags; and
6. Incorporates—as appropriate—existing policies and procedures that control reasonably foreseeable risks.

C. Program Adoption and Updates

1. Adoption: This Program has been adopted by the University's Board of Trustees.
2. Responsibility to implement and update: The Vice President for Finance is responsible for updating and implementing this policy. The College of Law's Executive Director of Business and Finance will work with the Vice

President for Finance and the Dean of the College of Law to ensure local conformance at the Gulfport and Tampa campuses.

3. Program Administrators: The Vice President of Finance and the College of Law's Executive Director of Business and Finance are designated as Program Administrators. The Program Administrators are responsible for the following:
    a. Staff training: The Program Administrators are responsible for arranging for appropriate staff training. Training will encompass general data security practices, covered accounts, methods for detecting red flags, and reporting and response obligations. Training updates will be conducted as reasonably needed and when material program changes are made. Training processes will be implemented for new hires or current employees who transfer into positions in which they may have red flag detection responsibilities.
    b. Report review and response: The Program Administrators are responsible for reviewing any staff reports regarding red flag detection and the steps for preventing and mitigating identity theft. In addition, the Program Administrators, in consultation with the Director of Internal Audit, will determine which prevention and mitigation steps should be taken in particular circumstances.
    c. Program updates: The Program Administrators are responsible for recommending future Program updates and changes to the President, who has been delegated authority by the Board of Trustees to manage the Program. This Program will be periodically reviewed and updated to reflect changes in risks related to identity theft, including any instances of identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the University maintains and changes in the University's business arrangements with other entities. After considering these factors, the Program Administrators will recommend whether changes to the Program, including changes to the listing of red flags, are warranted.
    d. Other general program administration: The Program Administrators are responsible for any other aspects of Program administration, including developing reporting forms and processes, training content and delivery methods, and coordinating Program activities with other legal or policy requirements or obligations, including but not limited to University or College of Law policies on confidentiality, privacy of student and employee records, and computer and network use. Section 5 Finance Policies Revised through October 2009

D. Data Security for Sensitive Information

Each employee is responsible for protecting sensitive information, including using appropriate security controls to eliminate a significant source of risk. The repercussions of data security breaches that stem from lax attention to security, carelessness with passwords, theft or loss of electronic devices, laptops, and USB flash drives are significant in both cost and reputation. In addition, unauthorized use or release of sensitive information by any member of the campus community may subject the violator to personal, civil, and criminal liability, and legal penalties in addition to corrective action up to and including termination of employment or student status.

1. Types of sensitive information: Sensitive information may be stored electronically or in paper format. University students and personnel are encouraged to use common sense judgment in securing sensitive information. If a student is uncertain about the sensitivity of a particular piece of information, he or she should contact the

Program Administrator for the campus. If an employee is uncertain about the sensitivity about a particular piece of information, the employee should seek guidance from his or her supervisor.

2. Examples of sensitive information: Examples of sensitive information include—but are not limited to—the following:
    a. Credit card information;
    b. Tax information numbers, including Social Security Numbers (SSNs), Business Identification Numbers, and Employer Identification Numbers;
    c. Payroll information;
    d. Cafeteria plan check requests and associated paperwork;
    e. Medical information for any student or employee;
    f. Other personal information that belongs to a student, employee, or contractor and that is either protected by law from disclosure, or if improperly disclosed could cause potential harm or compromise identity security.
3. Relationship to FERPA: Notwithstanding the examples above, this policy does not preclude disclosure of student "directory information" or other information the University is permitted to disclose under the Family Educational Rights and Privacy Act.
4. Security of paper records:
    a. Security controls: Departments and offices that store confidential paper records will use standard security controls to avoid inadvertent disclosure. These controls include (i) supervising file cabinets, desk drawers, overhead cabinets, and other storage spaces containing documents with sensitive information, (ii) locking these areas and spaces when not in use, when office staff are absent, and when the office is closed; and (iii) keeping desks, workstations, work areas, printers and fax machines, and common shared work areas clear of documents containing sensitive information when the documents are not in use.
    b. Document disposal: To help avoid issues of identity and data theft, and to meet confidentiality requirements, the University follows uniform and appropriate disposal processes for all sensitive information records. On a routine basis, using local shredders within an office or department will meet this requirement. In addition, the University has placed secure bins in various offices across campus to facilitate the centralized on-site records destruction process. In accordance with the requirements of the Fair and Accurate Credit Transaction Act of 2003, the University also requires that a "due diligence" review be conducted for all vendors to whom the University outsources the disposal of sensitive material.
5. Security of Electronic Data:
    a. Computers: Offices and departments that use computers will implement standard security controls, such as ensuring that employees use passwords for logging into the network and screen locks when an employee is away from his or her desk. In addition, offices and departments will stress that employees must keep passwords confidential to avoid improper access. Sensitive data that is transmitted externally should be sent only to qualified recipients and should be password-protected.
    b. Laptop computers and small electronic devices:
        i. Laptops and personal digital assistants (PDA) like BlackBerry devices and iPhones warrant special attention. In general, sensitive data should not be maintained on laptops or PDAs, which can be lost or stolen. For electronic devices that can and are frequently taken off campus, users should

consider using password protection and other similar steps to avoid improper access if the device is lost or stolen.

ii. The loss or theft of a device linked to the network should be reported immediately to the Office of Information Technology so the access connection can be terminated.

iii. Information stored electronically on items such as old computers, computer discs, flash drives, or hard drives, must be overwritten or wiped clean using tools provided by the Office of Information Technology before these items are disposed of.

c. USB flash drives: A USB flash drive (also known as a thumb drive, jump drive, or key drive) is a small device that can store vast amounts of data. Although highly beneficial, these devices pose high security risks if proper controls are not followed. The following are some key points to remember about USB flash drives:

i. USB flash drives are susceptible to viruses and malware. If an employee uses a USB flash drive in a public or foreign computer system, the flash drive can become infected.

ii. USB flash drives can be configured to be bootable and run programs. If you plug a USB flash drive configured by someone seeking improper access into a PC running Windows, the device can take over the machine, search for confidential documents, copy them back to the USB's internal storage, and hide them as "deleted" files.

iii. USB flash drives can become corrupted.

iv. USB flash drives can be used by employees to remove sensitive data from the workplace.

v. USB flash drives can be easily lost or stolen.

d. To avoid the most pronounced of these risks, the following protocols have been established:

i. Store sensitive information on the University server. Unless absolutely necessary, do not copy sensitive data to a USB flash drive. If you must download sensitive information, use only USB flash drives that include built-in security features such as encryption and password protection, and be sure to use these functions. Contact the Office of Information Technology for assistance. Section 5 Finance Policies Revised through October 2009 ii. Have USB devices configured by the Office of Information Technology with anti-virus applications that can be run directly from the flash drive to ensure that it will not become infected by a public or foreign computer system that may have a virus.

ii. Always keep any USB flash drive or other removable media (such as CD-ROM discs) physically secure.

iii. If you find a USB flash drive that someone lost, do not plug it into your computer, as it could be infected or contain malicious software.

iv. Because flash drives and other removable media can become corrupted, always backup your data to the network server. No flash drive or other removable media should be the sole location for important data. If you lose or destroy your flash drive, the data should exist in another location, such as the network server.

6. Banner Access: Banner—the University's database system—is managed through a series of controls. New hires can be given system access only by the Office of Information Technology after official notification of hire by the Office of Human Resources. Only employees who need access to perform their jobs are granted access to specific areas of information. Under the Banner standards, the University has assigned various offices with specific module responsibility (i.e., the Finance Department is the module owner of the Finance component in

Banner). Within a given department, the department head determines the proper level of access for its employees. An employee seeking access to a Banner module outside his or her department's control must obtain the module owner's approval. All new employees to be granted Banner access must attend a training session with Office of Information Technology to learn the proper Banner security measures.

7. Data Breaches: Florida law provides steps to be followed if certain data breaches occur. In general, because the University maintains computerized data in a system that includes personal information, a Program Administrator or his or her designee must notify individuals whose personal information may be at risk as a result of an information system breach.
    a. Electronically maintained personal information for purposes of a Florida law data breach is the combination of (1) an individual's name (first name or initial and last name, or middle name and last name) and (2) one of several data elements that are not encrypted, such as SSN, driver's license or state identification card number or account, credit or debit card number, along with the password or other information allowing access to an individual's financial account.
    b. Under this provision, the University must notify Florida residents if there is a "breach of the security of the system," which is the "unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information." Depending on the scope of the breach and who is affected, other notification requirements may also apply.
    c. If any member of the campus community becomes aware of a potential or active breach of any University computer or electronic system (regardless of whether data has been compromised), he or she immediately must report the potential or actual breach to the Office of Information Technology, which in turn is responsible for immediately notifying the Program Administrator for initiation of applicable breach notification requirements.
    d. Depending on the nature and scope of the breach, the Program Administrator will also coordinate compliance with other state and federal requirements as applicable. If a breach requires outside assistance to effectuate compliance with all applicable breach laws, the Program Administrator may retain vendors to assist.

E. Covered Accounts for Red Flag Purposes:

The University offers or maintains the following covered accounts:

1. Accounts related to the Federal Perkins Loan Program, which provides low-interest loans to help needy students finance the costs of postsecondary education;
2. Refund of credit balances from Parent Plus loans;
3. Refund of other credit balances from student accounts;
4. Deferment of tuition or housing payments; and
5. Cash advances or emergency loans.
6. Red flags may also arise in the context of employment and applicant screening processes.

F. Identifying Relevant Red Flags:

To establish a framework for identifying relevant red flags, this section first identifies the methods by which covered accounts are opened and then accessed, which allows the University to understand the information that may be on file

and the potential vulnerabilities that may exist. This section is followed by a general description of the categories of red flags that have been considered by the University in conjunction with each covered account.

1. Methods of Opening Covered Accounts: University admission, acceptance and enrollment—which is a prerequisite to open a covered account—requires some or all of the following information, depending on the academic program:
    a. Application with personally identifying information;
    b. High school transcript, undergraduate, or graduate transcripts, as applicable;
    c. Official test scores (e.g., ACT, SAT, GRE, LSAT, MCAT, GMAT);
    d. Letters of recommendation, as applicable;
    e. Entrance Medical Record, for undergraduates;
    f. Medical history, for undergraduates;
    g. Immunization history, for undergraduates;
    h. Insurance card, for undergraduates;
    i. TOEFL scores, as applicable; and
    j. Immigration information and visa application, as applicable.
2. Methods Provided to Access Covered Accounts:
    a. Online view access and the capacity for online payments;
    b. Disbursements obtained in person requires picture identification; and
    c. Disbursements obtained by mail can only be mailed to an address on file.
    d. In assessing vulnerabilities, the University will also consider any previous history of identity theft.
3. Types of Red Flags: In general, red flags typically fall into one of the following five categories, the first four of which relate to covered accounts; the last category relates to employment and applicant screening:
    a. Suspicious Documents: This category encompasses documents available for physical review. Examples of items to watch for include:
        i. Documents provided for identification that appear to have been altered or forged;
        ii. The photograph or physical description on the identification is not consistent with the appearance of the applicant presenting the identification;
        iii. Other information on the identification is not consistent with information provided by the person presenting the identification, like a signature card or a recent check; or
        iv. An application appears to have been altered or forged, or torn up and reassembled.
    b. Suspicious Personal Identifying Information: On occasion, identity thieves may use personally identifying information that is suspicious. Examples of items to watch for include:
        i. Personal identifying information provided is inconsistent when compared with external information sources (Examples include where the address does not match any address in the credit report; the SSN has not been issued[6] or is listed on the Social Security Administration's Death Master File; or personal identifying information provided by the person is not consistent with other personal identifying information provided by the person with whom the University is dealing);

[6] To determine if a Social Security number has been issued, see http://www.ssa.gov/employer/ssnvhighgroup.htm.

ii. A lack of correlation between the SSN range with the Social Security Administration's issuance tables and date of birth;
iii. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources;
iv. Personal identifying information provided is a type commonly associated with fraudulent activity as indicated by internal or third-party sources (Examples include when the address on an application is fictitious, a mail drop, or to an address appearing to be a prison; the phone number is invalid or is associated with a pager or answering service; the SSN provided is the same as that submitted by other persons; or 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.);
v. 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; or
vi. The person cannot supply any information beyond what would typically be available in a wallet or credit report.

c. Suspicious Account Activity: A red flag may arise in the context of how an account is used rather than through the actions or inactions of the specific individual with whom the University is dealing. The following are examples of account activity that may be significant:
   i. Shortly following the notice of change of address for a covered account, the University receives a request for new, additional, or replacement goods or services;
   ii. A new account is used in ways associated with fraud (for example, purchased goods are converted to cash, refund on pre-paid rent or meal plan, etc.);
   iii. Mail sent to the person is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the person's covered account;
   iv. The University is notified that the person is not receiving paper account statements; and
   v. The University is notified of unauthorized charges against an account.
d. Notices from Other Sources: In this category, the University receives notice from members of the campus community, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with a covered account.
e. Alerts, Notifications, and Warnings from a Credit Reporting Company: In the context of a University setting, this category does not involve a covered account. Rather, this category of red flag encompasses screening processes used for employment where a consumer or credit report has been obtained. To the extent screening is performed for student applicants using a third party, this issue may also arise. Examples of activity that may signal identity theft include:
   i. A fraud or active duty alert included with a credit report;
   ii. A notice of credit freeze from a credit or consumer reporting agency in response to a request for a consumer report;
   iii. A notice of address discrepancy from a credit or consumer reporting agency; or
   iv. A credit or consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant—such as a recent and significant increase in the volume

of inquirers, an unusual number of recently established credit relationships, or a material change in the use of credit—especially with respect to recently established credit relationships.

G. Detecting Red Flags: Using the types of red flags listed above, each covered account has been assessed and this Program established to identify and detect red flags relevant to each type of covered account. Detecting red flags in the screening process is also addressed.

1. **Participation in the Federal Perkins Loan Program:** All institutions offering Perkins loans are subject to the red flag rule. Possible red flags relevant to Perkins loan activity are:
    a. Picture ID not appearing to be authentic or not matching the appearance of the student presenting it;
    b. Requests in connection with account originating from other than a University-issued e-mail account; or
2. **Refund of credit balances from Parent Plus Loans:** Under applicable federal regulations, these balances are required to be refunded in parent's name and mailed to the parent's address on file within the time period specified. No request is required. Parents may elect in writing that the University refund the balance to the student. Possible red flags relevant to Parent Plus refund activity are:
    a. An address change submitted before refund disbursement is fictitious, a mail drop, or to an address appearing to be a prison, or is the same as or similar to the address or telephone number submitted by an unusually large number of other persons;
    b. Shortly following the notice of change of parental address for a covered account, the University receives a request for new, additional, or replacement refund check;
    c. Mail sent to the parent is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the student's covered account;
    d. The University is notified that the parent is not receiving paper correspondence or loan information;
    e. A student requests a refund check when no parental election form is on file;
    f. An election form authorizing the student to be refunded the balance appears suspicious;
    g. Where a refund check is picked up in person, a picture ID is offered that does not appear to be authentic or does not match the appearance of the person presenting it; or
    h. The University receives a fraud alert from an external source.
3. **Refund of other credit balances from student accounts:** In general, refund check requests from current students must be made in person by presenting a picture ID or in writing from the student's University issued e-mail account. The refund check typically can be mailed only to an address on file or picked up in person by showing picture ID. Requests from students not currently enrolled or graduated from the University must be made in writing. Possible red flags relevant to other refund activity are:
    a. An address change submitted before refund disbursement is fictitious, a mail drop, or to an address appearing to be a prison, or is the same as or similar to the address or telephone number submitted by an unusually large number of other persons;
    b. Shortly following the notice of change of address for a covered account, the University receives a request for new, additional, or replacement refund check;
    c. Mail sent to the student is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the student's covered account;
    d. The University is notified that the student is not receiving paper correspondence or loan information;
    e. A student requests a refund check after creating a balance through a credit card payment;
    f. A student requests a refund check from an email address other than the one issued by the University;

g. An election form authorizing someone other than the student to pick up the refund check appears suspicious;
h. Where a refund check is picked up in person, a picture ID is offered that does not appear to be authentic or does not match the appearance of the student presenting it; or
i. The University receives a fraud alert from an external source.

4. **Deferment of tuition or housing payments:** Requests are typically made in person only and require the student's signature. No red flags relevant to tuition deferment have been identified. For housing payments, possible red flags are likely to arise only in the context of a requested refund of a portion of pre-paid housing fees as a deduction from financial aid. When this occurs, possible relevant red flags are:
    a. An address change submitted before refund disbursement is fictitious, a mail drop, or to an address appearing to be a prison, or is the same as or similar to the address or telephone number submitted by an unusually large number of other persons;
    b. Shortly following the notice of change of address for a covered account, the University receives a request for new, additional, or replacement refund check;
    c. Mail sent to the student is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the student's covered account;
    d. The University is notified that the student is not receiving paper correspondence or loan information;
    e. A student requests a refund check from an email address other than the one issued by the University;
    f. An election form authorizing someone other than the student to pick up the refund check appears suspicious;
    g. Where a refund check is picked up in person, a picture ID is offered that does not appear to be authentic or does not match the appearance of the student presenting it; or
    h. The University receives a fraud alert from an external source.
5. **Cash advances or emergency loans:** Requests are typically made in person only and require the student's signature. In hardship cases, requests may be processed electronically. Possible red flags relevant to cash advances or emergency loans are:
    a. An address change submitted before the advance or loan request is fictitious, a mail drop, or to an address appearing to be a prison, or is the same as or similar to the address or telephone number submitted by an unusually large number of other persons;
    b. Shortly following the notice of change of address for a covered account, the University receives a request for a cash advance or emergency loan;
    c. A student requests a cash advance or emergency loan from an email address other than the one issued by the University;
    d. An election form authorizing someone other than the student to pick up the cash advance or emergency loan appears suspicious;
    e. Where a cash advance or emergency loan is picked up in person, a picture ID is offered that does not appear to be authentic or does not match the appearance of the student presenting it; or
    f. The University receives a fraud alert from an external source.
6. **Red flags in employment screening processes:** Red flags in the employment screening process can arise during the background check process when consumer reports indicate a fraud alert, address discrepancy, or other indicia of possible fraudulent activity in connection with the applicant's identity.

H. Red Flag Responses to Possible Fraud

1. When potential fraud affecting a covered account is detected: This Program provides for appropriate responses to detect red flags to prevent and mitigate identity theft. Once potentially fraudulent activity is detected, the employee detecting the activity must act promptly. A rapid and appropriate response is the key to protecting the campus community and the University from damages and loss. The employee who detects the potential fraud should take the following steps:
    a. Gather all related documentation and write a description of the situation. Present the information through the chain to the Program Administrator for determination.
    b. The Program Administrator will complete any additional authentication reasonably needed to determine whether the attempted transaction was fraudulent or authentic.
    c. The Program Administrator will also contact the University's Director of Internal Audit to assist in the investigation process.
    d. Interim measures such as changing passwords or security codes that permit account access may be suspended pending investigation to reduce possible risk.
2. When a transaction related to a covered account is determined to be fraudulent: If a transaction is determined to be fraudulent, the Program Administrator or designee will take appropriate actions immediately. Actions may include, but are not limited to:
    a. Denying access to the covered account;
    b. Canceling or reversing the transaction;
    c. Notifying the affected person that fraud has been attempted or has occurred;
    d. Notifying and cooperating with appropriate law enforcement;
    e. Assessing possible liability for the University;
    f. Taking additional mitigation actions where required based on the circumstances, such as state law data breach notification requirements;
    g. Determining no further response is warranted under the particular circumstances.
3. Identity theft issues in employment screening processes: Red flags associated with consumer reports will be managed by Human Resources. Responsive steps may include contacting the applicant to inquire further, determining the underlying basis for a substantial discrepancy between an applicant's reported address and the third-party credit reporting agency address notification, and conducting such further screening as is reasonably necessary to resolve any concerns. Upon hire, identity verification is also required in accordance with Form I-9 requirements. Withdrawal of job offers based on a consumer report will be done in accordance with Fair Credit Reporting Act requirements.

I. Oversight of Service Provider Arrangements

1. Outside service providers: If the University engages a service provider to perform an activity in connection with one or more covered accounts, the University will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft:
    a. Require, by contract, that the service provider has such policies and procedures in place; and

   b. Require, by contract, that the service provider review this Program and report any red flags to the responsible Program Administrator or the employee with primary oversight of the service provider relationship.

2. Contract review: To comply with these requirements, it is expected that all current contracts will be reviewed to determine if they concern covered accounts and, if appropriate, to propose an amendment to the appropriate vendor acknowledging the vendor's responsibilities to (a) comply with the Federal Trade Commission's Red Flag Rules, implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003, (b) maintain policies and procedures to detect relevant red flags that may arise in the performance of any agreements, and (c) take appropriate steps to prevent or mitigate identity theft relating to this agreement. The vendor will also be required to provide a copy of its written program to the University, and if requested by the University will report any red flags concerning the University's covered accounts and the applicable contract to the University's Program Administrator. This obligation is in addition to the existing requirements for outside consultants and contractors handling records and data falling within the definition of "educational records" covered under the Family Educational Rights and Privacy Act.

Adopted and approved by the Stetson University Board of Trustees on Friday, October 23, 2009.