FINANCE PROCEDURE MANUAL	TITLE: Identity Theft Prevention Procedures	
	NUMBER: FIN-CON-005	VERSION: 03
	ISSUED DATE: **9/30/2011**	REVISION DATE: 2/10/2016

➢ Purpose:

To document Palm Beach State's administrative controls used to detect, prevent, and mitigate identity theft in connection with the opening, maintenance, and use of employee, customer, and student accounts.

➢ Definitions:

Accounts: Records the College maintains in connection with official business, including admissions and student applications, financial accounting records, financial aid records, and related identification records in various systems.

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

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

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 (SSN)
- Date of birth
- Government issued driver's license or identification number
- Alien registration number
- Government passport number
- Employer or taxpayer identification number
- Unique electronic identification number
- Computer's Internet Protocol (IP) address or routing code

➢ Responsibility:

Identification Theft Task Force (IDTTF): A cross-functional group of College personnel tasked with coordination of the administration, reporting, and modification of this procedure.

IDTTF Members:

Finance Department: Controller

Enrollment Services: College Registrar

Enrollment Services: Financial Aid Director

Finance/Accounts Receivable/Cashiering: Assistant Controller, Revenue & Operations

Finance/Purchasing/Accounts Payable: Assistant Controller, Treasury & Reporting

Human Resources: Executive Director, Human Resources

Information Technology: Chief Information Officer and Information Security Manager

Security Department: Chief of Security

➢ Procedure Details:

1. The IDTTF will meet regularly to implement these procedures. The IDTTF shall, at a minimum, consist of key personnel from Student Registration, Financial Aid, Finance, Academic Admissions, Information Technology, Human Resources, and Security.

2. The IDTTF shall maintain a listing of those items that are deemed to indicate that there could be possible ID theft problems (‘Red Flags’-See Checklists), and direct the key areas that have access to such documents and processes to their existence, recommended remediation, and follow-up steps as outlined in this procedure.

3. This procedure will be periodically reviewed and updated to reflect changes in identity theft risks and technological changes. The IDTTF will consider the College’s experiences with identity theft, changes in identity theft methods; changes in identity theft detection, mitigation and prevention methods; changes in types of accounts the College maintains; changes in the College’s business arrangements with other entities, and any changes in legal requirements in the area of identity theft.

4. After considering these factors, the IDTTF will determine whether changes to the procedures, including the listing of Red Flags, are warranted.

5. The IDTTF shall confer with all appropriate College personnel as necessary to ensure compliance with the Program. The IDTTF shall present any recommended changes to the President for approval. The President's approval shall be sufficient to make changes to the College Identity Theft Prevention Program.

1. Suspicious Documents:
    a. Identification document or card that appears to be forged, altered or inauthentic;
    b. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
    c. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
    d. Application for service that appears to have been altered or forged.
2. Suspicious Personal Identifying Information:
    a. Identifying information presented that is inconsistent with other information the customer provides (e.g., inconsistent birth dates);
    b. Identifying information presented that is inconsistent with other sources of information (e.g., an address not matching an address on a credit report);
    c. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
    d. Identifying information presented that is consistent with fraudulent activity (i.e., an invalid phone number or fictitious billing address);
    e. Social security number presented that is the same as one given by another customer;
    f. An address or phone number presented that is the same as that of another person;
    g. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
    h. A person's identifying information is not consistent with the information that is on file for the customer.
3. Suspicious Account Activity or Unusual Use of Account:
    a. Change of address for an account followed by a request to change the account holder's name;
    b. Payments stop on an otherwise consistently up-to-date account;
    c. Account used in a way that is not consistent with prior use (example: very high activity)

d. Mail sent to the account holder is repeatedly returned as undeliverable;
e. Notice to the College that a customer is not receiving mail sent by the College;
f. Notice to the College that an account has unauthorized activity;
g. Breach in the College's computer system security; and
h. Unauthorized access to or use of customer account information.

4. Notifications and Warnings from Credit Reporting Agencies
   a. Report of fraud accompanying a credit report;
   b. Notice or report from a credit agency of a credit freeze on a customer or applicant;
   c. Notice or report from a credit agency of an active duty alert for an applicant; and
   d. Indication from a credit report of activity that is inconsistent with a customer's usual pattern
5. Alerts from others:
   a. Notice to the College from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

➢ References:

Florida Statutes:

FS 501.171

https://www.flsenate.gov/Laws/Statutes

Red Flags Rule:

15 USC § 1601; 16 CFR 681 et seq.

http://www.gpo.gov/help/parallel_table.pdf

Finance Procedures:

FIN-SAS-025

http://www.palmbeachstate.edu/finance/Documents/FIN-SAS-025.pdf

Board Policy:
http://www.palmbeachstate.edu/boardoftrustees/Documents/1.30_Identity_Theft_Prevention_Program.pdf