SUNY DOWNSTATE MEDICAL CENTER
POLICY AND PROCEDURE

Department: Office of Compliance & Audit Services

Subject: Identity Theft Prevention

Approved by: Renee Poncet
VP, Compliance & Audit

Renee Poncet
Signature

Original Issue Date: 10/1/09

Revision Date: July 2013

Policy Number: OCA-2

I. Background:

Pursuant to the Federal Trade Commission (FTC), Fair and Accurate Credit Transaction Act of 2003 (FACTA) Red Flags Rule (16 CFR 681.2), the State University of New York (SUNY) has developed an Identity Theft Prevention Program hereafter the "Program" which was adopted by the SUNY Board of Trustees on May 12, 2009. The Program's purpose is to prevent frauds committed by the misuse of identifying information. Per the Program, the Downstate Medical Center (DMC) campus President is responsible for ensuring implementation of the Program at DMC. To that end, the President has designated the AVP of the Office of Compliance & Audit Services (OCAS) as the Program Administrator (PA) to implement the DMC Identity Theft Prevention Policy and Procedure (P&P) in accordance with the SUNY Program. This P&P identifies "covered accounts"; identifies relevant patterns, practices, and forms of activity within those accounts that are "red flags" signaling possible identity theft; describes the detection of red flags and responses to any red flags that are detected in order to prevent and mitigate identity theft; and outlines the administration of the Program.

II. Policy:

It is DMC's policy to comply with the FTC, FACTA Red Flags Rule (16 CFR 681.2).

III. Definitions:

Account:	A relationship established with an institution by a student, employee, or other person to obtain educational, medical, or financial services.
Covered Account:	An account that permits multiple transactions or poses a reasonably foreseeable risk of being used to promote an identity theft.
Responsible Staff:	Personnel, based on title, who regularly work with Covered Accounts and are responsible for performing the day-to-day application of the Program to a specific Covered Account by detecting and responding to Red Flags.
Red Flag:	A pattern, practice, or specific activity that indicates the possible existence of identity theft.
Response:	Action taken by Responsible Staff member(s) upon the detection of any Red Flag to prevent and mitigate identity theft.
Service Provider:	A contractor to the campus engaged to perform an activity in connection with a Covered Account.

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

IV. Procedures:

A. PA Responsibilities:

1. Implement and apply the Program.
2. As necessary, identify and train responsible staff.
3. Review service provider agreements and monitor service providers, where applicable, to ensure that such providers have adequate identity theft prevention programs in place. (In the event that it is determined that a service provider is not adequately guarding against threats of identity theft, the PA should escalate the issue to the appropriate senior administrator who will take corrective action as indicated.)
4. Investigate reported suspicion/confirmation of identity theft or attempted identity theft through resolution.
5. Determine and recommend any corrective action steps.
6. Maintain records relevant to the Program, including:
   a. P&P
   b. Documentation on training
   c. Documentation on instances of identity theft and attempted identity theft, including the investigation steps, outcomes and or resolutions and corrective action recommendations
   d. Contracts with service providers that perform activities related to covered accounts

B. Business Units; Covered Accounts; Responsible Staff; Red Flags; Responses:

1. Academic

a. ACADEMIC	
Covered Account:	Academic Development
Responsible Staff:	Academic Development staff
Red Flag:	Suspicion/Confirmation that student payroll files have been compromised.
Response:	Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

b. ACADEMIC	
Covered Account:	Bursar
Responsible Staff:	Bursar Office staff
Red Flag 1:	Student with no ID or suspicious ID who is trying to obtain information and or a refund check.
Response 1:	Inform the student that no information and or refund checks are released without SUNY Downstate ID or NYS Drivers License. In the event the ID presented remains suspicious, notify immediate supervisor and the PA (718-270-4033) who will investigate and take appropriate actions.
Red Flag 2:	A change of address request occurs under suspicious circumstances.
Response 2:	Request that the student come in and provide valid ID, (e.g., Drivers License, tax returns) in order to verify address. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

c. ACADEMIC	
Covered Account:	Financial Aid
Responsible Staff:	Financial Aid staff
Red Flag 1:	Suspicion/Confirmation that student/parent information has been compromised.
Response 1:	Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.
Red Flag 2:	Student submits multiple Free Applications for Federal Student Aid "FAFSA" containing conflicting personal information.
Response 2:	Notify immediate supervisor and contact student to attempt to resolve conflict and verify information. In the event that conflict cannot be resolved & activity appears suspicious report incident to PA (718-270-4033) who will investigate and take appropriate actions.

d. ACADEMIC	
Covered Account	Registrar
Responsible Staff:	Registrar Office staff
Red Flag 1:	A change of address request form is filled out under suspicious circumstances.
Response:	Ask student to provide valid ID, (e.g., Drivers License, tax returns) in order to verify address. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.
Red Flag 2:	Receipt of outside email requesting confidential information.
Response:	Notify immediate supervisor and contact student to resolve conflict and verify information. In the event that conflict cannot be resolved & activity appears suspicious report incident to PA (718-270-4033) who will investigate and take appropriate actions.

e. ACADEMIC	
Covered Account	Student Admissions
Responsible Staff:	Student Admissions staff
Red Flag:	Suspicion/Confirmation that student information has been compromised.
Response:	Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

f. ACADEMIC	
Covered Account:	Student Affairs
Responsible Staff:	Student Affairs staff
Red Flag:	Suspicion/Confirmation that student health information and or foreign student information may have been compromised.
Response:	Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

g. ACADEMIC	**NOTE: The process for confirming a student's identity must NEVER delay the provision of an appropriate medical screening exam or necessary stabilization treatment for an emergency medical condition. Providing identification is NOT a condition for a student obtaining the emergency care needed.**
Covered Account:	Student Health
Responsible Staff:	Student Health staff
Red Flag:	Suspicion/Confirmation that student medical information compromised.
Response:	Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

2. Administration

a. ADMINISTRATION / FINANCE	
Covered Account:	Email Accounts
Responsible Staff:	Information Technology staff
Red Flag:	Notification from student/employee/faculty that email has been accessed without authorization.
Response:	Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

b. ADMINISTRATION / FINANCE	**NOTE: The process for confirming an employee's identity must NEVER delay the provision of an appropriate medical screening exam or necessary stabilization treatment for an emergency medical condition. Providing identification is NOT a condition for an employee obtaining the emergency care needed.**
Covered Account:	Employee Health
Responsible Staff:	Employee Health staff
Red Flag:	Suspicion/Confirmation that employee medical records have been compromised
Response:	Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

c. ADMINISTRATION / FINANCE	
Covered Account: Responsible Staff: Red Flag: Response:	Human Resources/Personnel Personnel Staff Suspicion/Confirmation that employee records have been compromised. Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

d. ADMINISTRATION / FINANCE	
Covered Account: Responsible Staff: Red Flag: Response:	Payroll Payroll Staff Suspicion/Confirmation that employee records have been compromised. Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

e. ADMINISTRATION / FINANCE	
Covered Account: Responsible Staff: Red Flag: Response:	University Police/Public Safety University Police/Public Safety staff Suspicion/Confirmation that Employee/Student Data has been compromised (e.g., Parking Office/ID Office). Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

3. Hospital

a. HOSPITAL	**NOTE: The process for confirming a patient's identity must NEVER delay the provision of an appropriate medical screening exam or necessary stabilization treatment for an emergency medical condition. Providing identification is NOT a condition for a patient obtaining the emergency care needed.**
Covered Account:	Admission/Registration
Responsible Staff:	Admissions/Registration staff
Red Flag 1:	Insurance information does not match personal identification documentation provided and or no valid photo ID.
Response 1:	Request supplemental identification to confirm patient identity prior to non-emergency treatment. In the event the conflict cannot be resolved & activity appears suspicious, notify immediate supervisor and the PA (718-270-4033) who will investigate and take appropriate actions.
Red Flag 2:	During Patient registration via the Eagle System a red flag warning message from Hospital Finance is indicated.
Response 2:	Interview patient and attempt to resolve issue. In the event there is not a satisfactory resolution, notify immediate supervisor and the PA (718-270-4033) who will investigate and take appropriate actions.

b. HOSPITAL	**NOTE: The process for confirming a patient's identity must NEVER delay the provision of an appropriate medical screening exam or necessary stabilization treatment for an emergency medical condition. Providing identification is NOT a condition for a patient obtaining the emergency care needed.**
Covered Account:	Health Information Management
Responsible Staff:	Health Information Management staff
Red Flag:	Notification from the patient and/or Hospital Finance that a discrepancy exists in communications the patient has received from the hospital.
Response:	Retrieve the patient record to determine if the discrepancy can be resolved. In the event the discrepancy cannot be resolved, notify immediate supervisor and the PA (718-270-4033) who will investigate and take appropriate actions.

c. HOSPITAL	**NOTE: The process for confirming a patient's identity must NEVER delay the provision of an appropriate medical screening exam or necessary stabilization treatment for an emergency medical condition. Providing identification is NOT a condition for a patient obtaining the emergency care needed.**
Covered Account:	Hospital Finance
Responsible Staff:	Hospital Finance staff
Red Flag:	Receipt of information suggesting a patient has been the victim of medical identity theft.
Response:	Create a red flag in the patient's account in the Eagle System and require verification of patient identity prior to non-emergency treatment. Advise Health Information Management who should retrieve the patient record to determine if the concern can be resolved. In the event the concern cannot be resolved, notify immediate supervisor and the PA (718-270-4033) who will investigate and take appropriate actions.

4. Scientific Affairs

SCIENTIFIC AFFAIRS	
Covered Account:	Institutional Research
Responsible Staff:	Institutional Research Staff
Red Flag:	Suspicion/Confirmation that research subject data may have been compromised.
Response:	Notify immediate supervisor and research the red flag. In the event the red flag remains suspicious or is confirmed, notify the PA (718-270-4033) who will investigate and take appropriate actions.

V. Reporting:

Any reports or suspicions of Identity Theft can be reported directly to the Program Administrator in the Office of Compliance & Audit Services at (718) 270-4033.

Alternatively, Reports may also be made to the Compliance Line:

* (877) 349-SUNY (7869) – Toll Free, 24-hours-a-day, 7-days-a-week; or
* Click on the "Compliance Line" link at www.downstate.edu to make a report via the web.