State University of New York at Fredonia

Administrative Policy

TITLE: Identity Theft Prevention Program
POLICY NUMBER: 019

I. REASON FOR POLICY

The Federal Trade Commission (FTC), under the authority granted by the Fair and Accurate Credit Transaction Act (FACTA), has issued a Red Flags Rule (16 CFR 681.2) requiring that any financial institution and creditor develop an Identity Theft Prevention Program ("Program") focused on recognizing and preventing activity related to identity theft. All SUNY campuses, including SUNY Fredonia, fall within the definition of a creditor and, therefore, must develop an Identity Theft Prevention Program.

Each Program must include written policies and procedures for: (1) identifying "covered accounts"; (2) identifying relevant patterns, practices, and types of activity within those accounts that are “red flags” indicating possible identity theft; (3) detecting red flags; (4) responding appropriately to any red flags that are detected in order to prevent and mitigate identity theft; and, (5) administering the program in a manner that ensures proper staff training, implementation, oversight, and updating.

II. POLICY STATEMENT

This Policy was developed in order to comply with the Federal Trade Commission's Red Flags Rule (16 CFR 681.2). The purpose of this Policy is to prevent frauds committed by the misuse of identifying information (i.e. identity theft). The Policy intends to accomplish such by identifying accounts maintained by the University which may be susceptible to fraud (hereinafter "Covered Accounts"), identifying possible indications of identity theft activity associated with those accounts (hereinafter "Red Flags"), developing methods to detect such activity, and responding suitably when such activity has occurred.

A. Definitions

Account:	A relationship established with an institution by a student, employee, or other person to obtain educational or financial services.
Covered Account:	An account that permits multiple transactions or may pose a foreseeable risk of being used to promote an identity theft.
Identity Theft:	A fraud committed or attempted using the identifying information of another person without authority.
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.
Responsible Staff:	Personnel, based on title, who regularly work with Covered Accounts and are responsible for performing the routine application of the Program to a specific Covered Account by detecting and responding to Red Flags.
Service Provider:	A contractor to the University engaged to perform an activity In connection with a Covered Account.

B. Program Administration and Oversight

The President has designated the Vice President for Administration as Program Administrator to oversee administration of this Policy and Program. The Program Administrator may designate additional staff of the University to undertake responsibility for training personnel, monitoring service providers, and updating the Program, all under the supervision of the Program Administrator.

The Program Administrator or designees shall identify and train responsible staff, as necessary, to effectively implement and apply the Program. All University personnel are expected to assist the Program Administrator in implementing and maintaining the Program.

The Program Administrator or designees shall review service provider agreements and monitor service providers, where applicable, to ensure that such providers have adequate identity theft prevention programs in place. When the Program Administrator determines that a service provider is not adequately guarding against threats of identity theft, he/she shall have the authority to take necessary corrective action, including termination of the service provider's relationship with the University.

On an annual basis, the Program Administrator shall evaluate the Program to determine whether it is functioning adequately. This evaluation shall include: a case-by-case assessment of incidents of identity theft or attempted identity theft that occurred during the previous year; interviews with Responsible Staff; and a survey of all accounts maintained by the University to identify any additional Covered Accounts. In response to this annual evaluation, the Program Administrator shall recommend amendments to this Program for approval by the President.

The Program Administrator shall maintain records relevant to the Program, including: the Written Policy; documentation on training; documentation on instances of identity theft and attempted identity theft; contracts with service providers that perform activities related to Covered Accounts; and updates to the Written Program. Occasionally, the Vice President for Administration, or other designated internal control officer, may perform audits to determine if various segments of the University are in compliance with the Policy and Program.

C. Process: Covered Accounts; Responsible Staff; Red Flags; Responses:

Covered Account:	**Student Accounts**
Responsible Staff:	**All Student Accounts Staff**
Red Flag 1:	Suspicious ID presented by a student who is trying to access or alter an account.
Response:	Deny access to account until the student's identity has been established through acceptable means.
Red Flag 2:	A change of address request occurs under suspicious circumstances.
Response:	Ask student to verify address and any suspicious usage activity.
Red Flag 3:	Suspicious or no ID presented by a student who is trying to pick up a student refund check.
Response:	Withhold refund check until the student's identity has been verified through acceptable means.
Red Flag 4:	A student calls and asks what the credit card number is that will be refunded (if they withdraw, for example).
Response:	Do not give credit card numbers out over the phone.
Red Flag 5:	Student calls and requests that a refund check be sent to an alternate address that is not in Banner database.
Response:	Develop a "secret question" for each student that assists in identifying a student.

Red Flag 6:	Requests from a third party by telephone for information about a student account.
Response:	Must have authorization on file (or be part of an agreement on a third party voucher).

Covered Account:	**Financial Aid Account**
Responsible Staff:	**Financial Aid Advisors**
Red Flag 1:	Department of Education selects student's FAFSA for verification.
Response:	Collect supplemental information from student and resolve any conflict between FAFSA and supplemental information provided by student.
Red Flag 2:	Student submits multiple FAFSAs containing conflicting information.
Response:	Contact student to resolve conflict and verify information.
Red Flag 3:	Requests from a third party by telephone for information about a student account.
Response:	Must have authorization on file (or be part of an agreement on a third party voucher).

Covered Account:	**Web Services**
Responsible Staff:	**Information Technology Help Desk (FredQuest)**
Red Flag 1:	Notification from student or employee that email has been accessed without authorization or that the password has been exposed.
Response:	Freeze account; secure account; investigate unauthorized use; issue new password/account if necessary; monitor account if necessary.
Red Flag 3:	Notification that password has been changed by someone other than account owner or that password has been locked due to failed login attempts by someone other than account owner.
Response:	Disable account and investigate unauthorized access or attempted Access. Require password change. Issue a new account and monitor account activity.

Covered Account:	**System Account(s)**
Responsible Staff:	**Appropriate System Security Administrator**
Red Flag:	Multiple failed login attempts
Response:	Freeze account and/or reset password

Covered Account:	**Student Personal Information**
Responsible Staff:	**Registrar's Office, Admissions Office, Lifelong Learning And Special Programs, Graduate Studies, Payroll, Human Resources staff**
Red Flag:	Suspicious change of address form (e.g., Multiple address changes in a short time frame, lack of zip code information, lack of official signature, etc.).
Response:	Appropriate office must call the individual and request him/her to come to office (with identification) to complete the paperwork. If the individual is unable to appear in person, additional paperwork will be requested.
Covered Account:	**Employee Records**
Responsible Staff:	**Payroll, Internal Control and Human Resources**
Red Flag 1:	An employee attempts to pick up his or her paycheck without picture Identification.
Response:	Paycheck cannot be released without proper photo identification
Red Flag 2:	An individual requests to pick up someone else's paycheck for him or her.
Response:	Written permission must be obtained from the individual whose paycheck they are picking up and they must show valid photo identification.
Red Flag 3:	A call is received requesting verification of employment.
Response:	If the caller provides a Social Security Number, responsible staff can respond to the inquiry only by indicating that the employee in question is either 1) employed at SUNY Fredonia or 2) not employed at SUNY Fredonia. Any additional information will need a release of authorization from the employee. The requestor can also be directed to our online phone directory.
Red Flag 4:	Receive a faxed verification of employment request.
Response:	Do not complete the request until a signed release of authorization from the employee is received.
Red Flag 5:	A call from someone other than the employee (e.g., Parent, spouse, friend etc.) is received requesting information about the employee's paycheck.
Response:	Do not divulge the information. This information can only be Given to the employee him/herself.
Red Flag 6:	An address change is requested via telephone call.
Response:	Address changes are accepted through completion of proper

address change paperwork or by emailing it through properly authorized email account only.

Red Flag 7: An individual calls and requests his/her paycheck be mailed to him/her.

Response: Written permission is required from the employee via completion of proper paperwork or by emailing the request through authorized email account only.

Red Flag 8: Missing signature for a paycheck on the paycheck distribution list.

Response: Contact the authorized person who signed for the bundle of paychecks, and request they obtain the employee's signature (if, in fact, the employee did receive his/her paycheck).

Red Flag 9: Employee requests information from his or her personnel file.

Response: Must confirm Fredonia ID number or Social Security Number and see photo identification before the file can be shared.

Covered Account: Alumni Records

Responsible Staff: Employees of the College Foundation

Red Flag 1: Database file requested for purposes outside of normal university-related programs or from person(s) not normally submitting such requests.

Response: Notify Director of Alumni Affairs or immediate supervisor and proceed with an investigation. Divulge current privacy policy to all involved. If the request is approved, provide minimum amount of information needed to meet the request.

Red Flag 2: Reports or documents containing sensitive constituent data are discovered outside of a secure/locked location.

Response: Notify the Director of Alumni Affairs immediately and proceed with investigation.

Red Flag 3: Alum notifies university staff of identity theft and that he/she is receiving bills from unknown businesses using his/her name exactly as it appears on his/her alumni mail (including maiden name, if applicable).

Response: Notify the Director of Alumni affairs and proceed with investigation.

III. AUTHORITY FOR POLICY

Approved by the authority of the President's Cabinet on May 11, 2011.