Christopher Newport University

Policy: Red Flags Identity Theft Prevention Policy
Policy Number: 3030

Executive Oversight:	Vice President for Finance and Planning/CFO
Contact Office:	Business Office
Frequency of Review:	Biennially
Date of Last Review:	December 2022

A. PURPOSE

Christopher Newport University is committed to protecting the personal information entrusted to it by its students, faculty, staff and others in the course of financial transactions. This policy sets out the mechanisms by which the University will guard against identity theft in a manner that is consistent with federal regulation of creditors and covered accounts.

B. POLICY STATEMENT

The University shall adopt an Identity Theft and Prevention Program to prevent, detect, and mitigate identity theft. The program shall provide for active monitoring for "red flags" that may indicate a compromise of personal information, provide for reporting and responding to security incidents, and require training of employees in a position to identify red flags.

C. DEFINITIONS

Covered Account: A covered account is a consumer account designed to permit multiple payments or transactions, and any other account for which there is reasonably foreseeable risk of identity theft. These include student accounts established for the payment of tuition, fees, room, board, and other charges related to University activities, personal accounts through which employees receive wages or reimbursements, and accounts tied to the University identification card that allow students and employees to deposit personal funds for use at University locations and approved community vendors.

Creditor: A creditor is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit.

Identity Theft: Identity theft is a fraud committed or attempted using the identifying information of another person without his or her authority.

Red Flag: A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

Security Incident: A collection of related activities or events which provide evidence that personal identifying information may have been acquired by an unauthorized person.

D. PROCEDURES

1. Identity Theft Prevention Committee

The Vice President for Finance and Planning/CFO shall establish an Identity Theft Prevention Committee. The Committee shall be chaired by the Agency Risk Management and Internal Control Standards (ARMICS) Accountant and members of the Committee may include representatives from Admission, Advancement, Auxiliary Services, Student Accounts, Cashier Services, Financial Aid, Registrar, Human Resources, Information Technology Services, Payroll, and the Business Office. Other members may be appointed by the Vice President for Finance and Planning/CFO as needed.

The Committee is charged with reviewing existing University policies and procedures related to identity theft and incident reporting, and developing new standards and procedures as needed to ensure that the University maintains a high level of due diligence with respect to preventing, detecting and mitigating identity theft. The Committee is also responsible for establishing and maintaining routine training for staff in relevant positions, including training in how to identify a Red Flag, how to report a Red Flag, how to protect against identity theft in covered accounts and how to mitigate the impact of any incident that occurs.

2. The Identity Theft Prevention Program

The Identity Theft Prevention Program consists of this policy and procedures adopted by the Identity Theft Prevention Committee to identify, detect and respond to red flags, that include but are not limited to:

- Receipt of Notices of Dispute from a credit agency;
- Identification documents or cards that appear to be forged, altered or inauthentic;
- Identification documents or cards on which a person's photograph or physical description is not consistent with the person presenting the document;
- Inconsistencies in information among different documents presented;
- Presentation of identifying information that is inconsistent with other sources of information;
- Presentation of a social security number that is the same as one given by another student, employee or other individual; and
- Notice to the University of unauthorized activity on a student or employee account.

E. REFERENCES

Fair and Accurate Credit Transaction Act, 2003
Federal Trade Commission Regulation: Red Flags Rule, 2008

F. APPROVAL AND REVISIONS:

Approved By: Board of Visitors, Executive Vice President, April 7, 2009

Revision 1: Policy Committee, February 28, 2018
Revision 2: Policy Committee, November 11, 2020
Revision 3: Policy Committee, December 6, 2022

G. DATE OF NEXT REVIEW: Fall 2024