Western Carolina University - Identity Theft Prevention Program

I. PROGRAM ADOPTION

assurance levels (IALs):

IAL1 Requests for non-sensitive information, directory information or otherwise non-PII. IAL1 requests do not require further verification.

IAL2 Requests which require a moderate level of identity assurance may be satisfied by:

b. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent or that is consistent with fraudulent activity (e.g., an invalid phone number or fictitious billing address), and
c. Social Security number presented that is the same as one given by another individual or does not match the Social Security Administration database.

4. Suspicious Activity

a. Suspicious requests by an individual to change PII without supporting documentation,
b. Payments stop on an otherwise consistently up to date account,
c. Notice to the University that an account has unauthorized activity (e.g., credit card chargeback),
d. Suspicious use of University IT resources (e.g., logins from foreign countries), and
e. Identification or notification of unauthorized access to or use of individual account information.

5. Alerts from Others

a. Notice to the University from an individual, identity theft victim, law enforcement, other person or institution that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft.

D. Detection of Red Flags and Response to Red Flags

1. Student Enrollment

To detect any of the Red Flags identified above associated with the enrollment of a student, University personnel shall take the following steps to obtain and verify the identity of the person opening the account:

a. Verify the identification of individuals if they request information per the requirements in the Identity Proofing section above, and
b.

2. Existing Accounts

To detect any of the Red Flags identified above for existing covered accounts or records, University personnel shall take the following steps to monitor transactions on an account and requests to access or modify covered records:

a. Verify the identification of individuals if they request information per the requirements in the Identity Proofing section above,
b. Verify the validity of requests to change billing addresses by mail or email and provide the individual a reasonable means of promptly reporting incorrect billing address changes, and
c. Verify changes in banking information given for billing and payment purposes.

s4 i41 >BD3(ve)0 7 612 0 g 2399 r2 Tf1 0 0 1 8.224 1

a. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency, and
b. If a notice of an address discrepancy is received from a consumer reporting agency, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

4. Response to Red Flags

In the event University personnel detect any identified Red Flags, such personnel shall immediately notify their immediate supervisor and the CIO or CISO who may take or cause to be taken any one or more of the following steps, depending on their determination of the degree of risk posed by the Red Flag:

a. Complete or oversee additional authentication to determine whether the attempted transaction was fraudulent or authentic, and determine appropriate steps to take,
b. Continue to monitor a Covered Account for evidence of identity theft,
c. Notify the individual who is the subject of fraudulent account activity,
d. Change any passwords, security codes or other security devices that permit access to Covered Accounts,
e. Cancel the transaction,
f. Refuse to open a new Covered Account,
g. Close an existing Covered Account,
h. Provide the individual with a new individual identification number, if feasible,
i. Notify and cooperate with law enforcement as may be appropriate,
j. ement Network, United States Department of the Treasury,
k. Activate the Information Security Incident Response Plan, or
l. Determine that no response is warranted under the circumstances.

IV. PROGRAM ADMINISTRATION

A. Designation of Program Coordinators

The Program Coordinators are the Chief Information Security Officer (CISO), the Director of Student Financial Aid, the Associate Vice Chancellor of Human Resources, the Bursar and the Executive Director of Advancement Services (or their designees). These individuals are a subcommittee of the Information Security and Privacy Committee and are responsible for overseeing the implementation and oversight of this program.

B. Staff Training

The Program Coordinators will work with the Information Security and Privacy Committee and Human Resources to ensure that appropriate training is provided to all employees who have access to covered records. Training will include education on this plan and all other relevant information (T/F1 12gev)-7(a)4(nt i)-3(nfor)6(mation (