Western Carolina University - Identity Theft Prevention Program

I. PROGRAM ADOPTION

It is Western Carolina University (WCU) policy to ensure the integrity and confidentiality of personally identifiable information (PII) as required by implementing regulations of the FTC Red Flags Rule (Detection, Prevention, and Mitigation of Identity Theft) and the FTC Safeguards Rule related to the Gramm-Leach-Bliley Act (Standards for Safeguarding Customer Information). The purpose of this Identity Theft Prevention Program is to prevent, detect and mitigate identity theft in connection with any covered account or other University records containing PII.

II. DEFINITIONS

- **"Identity Theft"** means a fraud committed or attempted using the PII of another person without authority.
- **"PII"** means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to: name; address; telephone number; social security number; date of birth; government-issued driver's license or identification number; alien registration number; government passport number; employer or taxpayer identification number; or bank or other financial account routing code.
- **"Red Flag"** means a pattern, practice, alert or specific activity that indicates the possible existence of identity theft.
- **"Covered Account"** means (i) any account that constitutes a continuing financial relationship or is designed to permit multiple payments or transactions, including Perkins Loans, FFEL loans (Stafford loans and PLUS loans), student emergency loans, and any other student accounts and loans administered by the University; and (ii) any other account the University offers or maintains for which there is a reasonably foreseeable risk to holders of the account or to the safety and soundness of the University from identity theft.
- **"Covered records"** for purposes of this program includes student financial information, as defined below, required to be protected under Gramm-Leach-Bliley Act (GLBA). Additionally, WCU includes in this definition any credit card information received in the course of business by WCU, and all other records maintained by the University that contain PII. Covered records includes data maintained in any media.
- **"Student financial information"** is that information obtained by WCU from a student (sometimes also referred to as the "customer") in the process of offering a financial product or service, or such information provided to WCU by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services.
- **"Covered Office"** means any office that has access to covered records.
- **"Screen"** shall mean the display portion of any computing device.
- **"Public area"** shall mean a location outside of a departmental office where the general public has free and easy access to the area.
- **"Secured"** shall, at the very least, mean the locking of or otherwise preventing access to information, records, and/or physical space.

III. PROGRAM

A. Protecting PII

1. To prevent the likelihood of identity theft occurring, covered offices will take the following steps with respect to its internal operating procedures to protect individual identifying information:

a. Access to WCU information systems and covered records is limited to those employees who have a business reason to access these accounts. Covered records, specifically including account numbers, account balances, and transactional information, are available only to WCU employees in covered offices.
b. Collect and maintain only the types and amount of confidential identifying information necessary for University business purposes, consistent with University policies and directives. Avoid the collection and use of Social Security numbers, except as expressly permitted by the North Carolina Identity Theft Protection Act.
c. Ensure that transmission of information is limited and encrypted when required per the Data Handling Procedures,
d. Ensure complete and secure destruction of paper and electronic records containing confidential Identifying Information when such records no longer need to be maintained, subject to and in accordance with the UNC General Records Retention and Disposition Schedule (2018).

2. Each employee and contractor performing work for the University must utilize the following security measures:

a. Whenever unattended or not in use, all computing devices must be left logged off or protected with a screen or keyboard locking mechanism controlled by a password or similar user authentication mechanism (this includes laptops, tablets, smartphones, and desktops). The Mobile Computing Devices Standard gives more guidance on the protection of mobile computing devices,
b. When viewing sensitive information on a screen, users should be aware of their surroundings and should ensure that third parties are not permitted to view the sensitive information,
c. Sensitive or critical business information, e.g., on paper or on electronic storage media, must be secured when not required, especially when the office is vacated at the end of the workday. The Data Handling Procedures define data sensitivity levels. The Media Handling and Disposal Standard gives more guidance on the management of removable media,
d. Paper containing sensitive or classified information must be removed from printers and faxes immediately. Faxes and printers used to print sensitive information should not be in public areas. Any time a document containing sensitive information is being printed the user must make sure they know the proper printer is chosen and go directly to the printer to retrieve the document,
e. Sensitive information on paper or electronic storage media that is to be shredded must not be left in unattended boxes or bins to be handled later and must be secured until the time that they can be shredded.

B. Identity Proofing

Identity proofing details requirements for the evidence that will be presented by a customer to support their claim of identity. Identity proofing's sole objective is to ensure the customer is who they claim to be to an acceptable level of certitude through the presentation and verification of the required level of evidence.

The requirements for obtaining assurance in a customer's identity is described using one of three identity 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:

- Use of an active WCUid (i.e., a myWCU authenticated process or campus Email)
- Or the collection and verification of a minimum combination of PII such as Release of Student Information Security Code, 92#, name, DOB, a permanent address, personal Email address or phone number on file.

IAL3 – Requests that require a higher level of assurance which would include matching a photo ID to a person's face. This may be accomplished in person or electronically, or via a proxy such as a notary. Documents used for identity assurance need to be originals or a notarized copy.

- IAL3 Example – Send a video meeting request to an Email address that is on file. In the video meeting request the individual display a driver's license in front of the camera and verify it matches the face and other PII on file.

C. Identification of Red Flags

To identify relevant Red Flags, the University considers the types of covered accounts it offers and covered records it maintains, the methods it provides to open them, the methods it provides to access them, and its previous experiences with identity theft. Red Flags may be detected while implementing existing account opening and servicing procedures such as: individual identification, caller authentication, third party authorization, and address changes.

The University identifies the following Red Flags in each of the listed categories:

1. Notifications and Warnings from Consumer Reporting Agencies

a. Report of fraud accompanying a consumer report, including background checks, and
b. Receipt of a notice of address discrepancy in response to a consumer report request.

2. 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 individual information, and
d. Application for service that appears to have been altered or forged.

3. Suspicious Personal Identifying Information

a. Identifying information presented that is inconsistent with other information the individual provides or that is on file for the individual (e.g., inconsistent birth dates),
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. Verify the individual's identity at time of issuance of individual identification card.

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.

3. Consumer Report Requests

To detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, the University's Office of Human Resources personnel shall take the following steps to assist in identifying address discrepancies:

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. File or assist in filing a Suspicious Activity Report ("SAR") with the Financial Crimes Enforcement 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 Data Security and Stewardship 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 security policies and procedures.

C. Service Provider Arrangements

In the event the University engages a 3rd-party service provider to perform an activity in connection with covered records, the University will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

1. Require, by signed contract, that service providers have such policies and procedures in place, and
2. Require, by signed contract, that service providers review the University's Program and report any Red Flags to the Program Coordinator(s).