Augusta University
Policy Library

Identity Theft Policy

Policy Manager: Office of Audit, Compliance, Ethics and Risk Management

POLICY STATEMENT
This policy applies to any department or individual using or controlling personally identifiable information and/or information pertaining to a Covered Account on behalf of Augusta University.

The Office of Consumer Credit and various Federal Agencies have jointly issued final rules and guidelines implementing Section 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). This Program is developed pursuant to the Section 114 rules which require each financial institution or creditor to implement a written program that includes reasonable policies and procedures for implementing the guidelines, to address the risks to AU's account holders.

AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☐ Visitors
☐ Other:

DEFINITIONS
These definitions apply to these terms as they are used in this policy:

- **Identity Theft**: Fraud committed or attempted using the identifying information of another person without authority.

- **Creditor**: The Red flags Rule defines the terms "creditor" broadly, including any person who defers payment for services rendered, such as organization that bills at the end of the month for services rendered the previous month. In its July 2008 guidance, FTC stated, "where non-profit and government entities defer payment for goods or services, they too are to be considered creditors."

  Activities that could cause colleges and universities to be considered "creditors" under the Red Flag Rule may include:

  - Participating in the Federal Perkins Loan program
  - Participating as a school lender in the Federal Family Education Loan or Direct Lending Programs
  - Offering institutional loans to student, faculty, or staff (e.g. Augusta University's emergency loans for students)
  - Offering a plan for payment of tuition throughout the semester (disallowed by the Board of Regents)

- **Covered Accounts**: An account offered or maintained by Augusta University (i) is designated to allow multiple payments or transactions, such as a loan that is billed or payable monthly, and which includes certain types of arrangements in which an individual establishes a "continuing relationship" with the enterprise, including billing for previous services rendered. The rules specifically exclude “stored value cards” (prepaid cards), such as the “debit express” cards issued to students and employees for use on campus to purchase goods and services. Covered accounts at Augusta University would include student loans granted or administered by the University or, (II) any other type of account offered of maintained by Augusta University for which that is a reasonable foreseeable risk of Identify Theft that may have an impact on the holders of Covered Accounts or on the safety and soundness of the University as a vendor, including financial, operational, compliance, reputation, or litigation risks.

    - **Consumer Report**: Is any communication of information by a Consumer Reporting Agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, reputation, personal characteristics, or mode of living, which is used as a factor in establishing the consumer’s eligibility for (i) credit to be used primarily for personal, family, or household purposes, or (ii) employment purposes.
    - **Consumer Reporting Agency**: A person or entity that, for monetary fees or on a cooperative nonprofit basis, regularly collects, evaluates, and disseminates credit information about consumers to be used for credit evaluation and related purposes.
    - **Department**: A unit of the University that offers or maintains Covered Accounts, engages a vendor to offer or maintain Covered Accounts, or uses Consumer Reports IN CONNECTION WITH CREDIT TRANSACTION.
    - **Identifying Information**: Any name or number that may be used, alone or in conjunction with other information, to identify a specific person.

- **Red Flags**: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

- **Personal Identifying Information**: Any name or number used, alone or in conjunction with any other information, to identify a specific person including:
    i. Name
    ii. Address
    iii. telephone number
    iv. social security number
    v. date of birth
    vi. government issued driver's license
    vii. government issued identification number
    viii. alien registration number
    ix. government passport number
    x. employer or taxpayer identification number
    xi. student identification number

PROCESS & PROCEDURES

Identifying Red Flag

Augusta University units/departments will incorporate procedures to control foreseeable risks to its patients and students from identity theft by identifying relevant red flags.

Risk Factors: Each relevant AU department and unit shall consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

1. The types of covered accounts it offers or maintains;
2. The methods it provides to open its covered accounts;
3. The methods it provides to access its covered accounts; and
4. Its previous experiences with identity theft.

Source of Red Flags: AU departments and units shall incorporate relevant Red Flags from sources as:

1. Incidents of identity theft AU has experienced;
2. Methods of identity theft that the AU has identified that reflect changes in identity theft risk; and
3. Applicable supervisory guidance.

Categories of Red Flags: The Program shall include relevant Red Flags from the following categories, as appropriate:

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2. The presentation of suspicious documents;
3. The presentation of suspicious personal identifying information, such as a suspicious address change;
4. The unusual use of, or other suspicious activity related to, a covered account; and
5. Notice from customers, victims of identify theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

Detecting Red Flags

Departments shall develop procedures for detecting of Red Flags by implementing procedures to verify the identity of a patient, student, or customer opening an account, making transactions via an existing account, or pertaining to the use of personal information in the hiring process. These procedures may include but are not limited to, the following:

1. New Covered Accounts:
    a. Require relevant identifying information such as name, date of birth, home address and other necessary information; and
    b. In the case of student enrollment, verify the student's identity at the time of issuance of student identification card by review of driver's license or other government-issued photo identification.

2. Existing Covered Accounts:
    a. Verify identification of student or customer if they request information;
    b. Verify validity of requests to change billing addresses by mail or email and provide the student of reasonable means of promptly reporting incorrect billing address changes; and
    c. Verify changes in banking information given for billing and payment purposes.

3. Identifying Address Discrepancies in Consumer or Credit Report Requests
    a. Require written verification from any applicant that the address provided by the applicant is accurate at the time of the request for the credit report is made to the consumer reporting agency; and
    b. In the event that notice of an address discrepancy is received, 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.

Prevention, Response, and Mitigation of Detected Red Flags

When a Red Flag has been detected AU employee will consider several factors such as the type of transaction, relationship with the victim of the fraud, availability of contact information for the victim of the fraud, and other factors. After consideration one or more of the following actions will be taken:

1. Cancel the transaction.
2. Continue to monitor a covered account for evidence of ongoing actions associated with identity theft.
3. Contact affected student or customer.
4. Change any passwords or other security devices that permit access to the covered account(s).
5. Do not open additional covered account(s).
6. Provide student/customer with new student identification number and/or account number.
7. Notify **Program Administrator** for determination of the appropriate step(s) to take.
8. Notify law enforcement when applicable.
9. In appropriate situations, determine that no response is warranted under the specific circumstances.

Third Party Service Provider

Augusta University will gain assurances from vendors that engage with AU covered accounts that they are in compliance with the FTC Red Flags Rule, have policies that demonstrate compliance, are aware of AU's Identity Theft Program, and will report any Red Flags as soon as possible.

REFERENCES & SUPPORTING DOCUMENTS
Fair and Accurate Credit Transactions Act of 2003 (FACT Act)

RELATED POLICIES
Intentionally left blank.

APPROVED BY:
Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 8/19/2024

President, Augusta University Date: 8/24/2024