Augusta University
Policy Library

Identity Theft Policy

Policy Owner: VP for Finance

POLICY STATEMENT

This policy applies to any department or individual reviewing consumer credit or criminal background reports on employees, students or other customers.

This policy also applies to anyone on campus who may receive address, name or bank information change requests from such parties.

This Identity Theft Program (The Program) was developed under the oversight of Finance Administration based upon consideration of the nature and scope of the University's activities. On the recommendation of the Senior Vice President for Finance and Administration, this program has been duly approved by the President's Cabinet.

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 develop and implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts.

The section 114 rules require the assessment of the validity of notifications of changes of address under certain circumstances, and the section 315 rules provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy.

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

- **Red Flags Rule:** A regulation issued in 2007 by the Federal Trade Commission (FTC) and Federal banking agencies intended to reduce the risk of identity theft. Mandatory compliance with the Red Flags Rule for "creditors" or "financial institutions" that provide

"covered accounts" begins on January 1, 2011. The FTC has stated that nonprofit and government entities can be subject to parts of the rule.

The Red Flags Rule is actually three different but related rules, one or two of which apply to many colleges and universities. There are 26 detailed rules which fall under the three general categories and which are detailed below:

- Debit and credit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. (*This provision is likely not applicable to colleges and universities, because, as discussed in the preamble to the Red Flags Rule, the definition of "debit card" specifically does not include stored value cards. However, this provision could implicate student ID's that can also be used as part of a national debit card network, such as Visa or MasterCard.*)

  (2) Users of consumer reports must develop reasonable policies and procedures to apply when they receive notice of an address discrepancy from a consumer reporting agency. (This provision applies to colleges and universities when they use consumer reports to conduct credit or background checks on prospective employees or applicants for credit.)

  (3) Financial institutions and creditors holding "covered accounts" must develop and implement a written identity theft prevention program for both new and existing accounts. (This provision likely applies to many colleges and universities).

- **Identity Theft:** Fraud committed using the identifying information of another person.

- **Creditor:** The Red Flags Rule defines the terms "creditor" broadly, including any person who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month. In its July 2008 guidance, the 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 Flags 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 students, 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:** A consumer account that involves 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.

- **Address Rules:** Issued by the FTC at the same time as the “Red Flags Rule,” and effective November 1, 2008, the rules (16 C.F.R. §681.1) apply not only to financial institutions and creditors but potentially to all employers that use consumer reporting agencies to conduct background checks on applicants and employees.

  The Address Discrepancy rules provide specific guidelines to enable an employer to establish practices that will permit it to form a reasonable belief as to whether a consumer report relates to the person on whom the report was obtained. Those rules also provide criteria for when employers have an obligation to provide confirmed addresses to the nationwide CRA. In a nutshell, the Address Discrepancy rules require the nationwide consumer reporting agencies to provide users of consumer reports (including employers) with a notice of address discrepancy when there is a "substantial difference" between the address the agency has on file for a consumer and the address provided by the employer when requesting the report. The regulation also requires users of consumer reports (including employers doing background checks on applicants) to establish policies that permit them to form a reasonable belief as to whether addresses provided by applicants are correct and to notify the CRA when they have confirmed applicant addresses.

- **Red Flags:** A pattern, practice, or specific activity that indicates the possible existence of Identity Theft. These flags are circumstantial factors identified to indicate potential identity theft. While the majority of these flags pertain exclusively to a traditional creditor/customer or financial institution (banking)/customer relationship, many may still apply to the University in certain situations. The 26 flags identified are:

  Alerts, Notifications or Warnings from a Consumer Reporting Agency

  1. A fraud or active duty alert is included with a consumer report.

  2. A consumer reporting agency provides a notice of a credit freeze in response to a request for a consumer report.

  3. A consumer-reporting agency provides a notice of address discrepancy

  4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as
     - A recent and significant increase in the volume of inquiries;
     - An unusual number of recently established credit relationships;

- A material change in the use of credit, especially with respect to recently established credit relationships;
- An account closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example: The address does not match any address in the consumer report or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: The address on an application is the same as the address provided on a fraudulent application or the phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: The address on an

application is fictitious, a mail drop, or a prison or the phone number is invalid or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example: The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry) or the customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: Nonpayment when there is no history of late or missed payments; a material increase in the use of available credit; a material change in purchasing or spending patterns; a material change in electronic fund transfer patterns in connection with a deposit account; or a material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account (Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor).

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

PROCESS & PROCEDURES
Intentionally left blank.

REFERENCES & SUPPORTING DOCUMENTS
Intentionally left blank.

RELATED POLICIES
Intentionally left blank.

APPROVED BY:
President, Augusta University and CEO, AU Health System Date: 06/13/2017