Policy on Identity Theft Red Flag Rules

Responsible Departments: Determined by Responsible Administrator
Responsible Administrator: Dir. Institutional Compliance & Risk Mgmt. **Effective Date:** May 1, 2009
Reviewed/Updated Date: May 1, 2026
Date of Scheduled Review: May 1, 2027

I. PURPOSE

To implement and maintain an identity theft program in accordance with the Federal Trade Commission (FTC), Fair and Accurate Credit Transaction Act (FACTA), and other applicable federal and sate laws related to identity theft and data protection and using these guidelines to establish policies and procedures that meet the requirements of the final rules.

II. SCOPE

This policy applies to all departments that manage or process data related to covered accounts as defined below. In addition, this policy applies to all departments that manage or process personal identification data that could be used to access information from another department or other party related to covered accounts as defined below.

III. DEFINITIONS

Cardholder: means a consumer who has been issued a credit or debit card. This includes student identification cards, which may be used as debit cards. This does not include student identification cards that are stored-value cards.

Clear and conspicuous: means reasonably understandable and designed to call attention to the nature and significance of the information presented.

Covered accounts: Accounts that are used primarily for personal, family, household or business purposes that involve or are designed to permit multiple payments or transactions; any account for which there is a reasonably foreseeable risk to the Account Holder (e.g., student, employee, or other individual) or the safety and soundness of the university. Covered accounts include, but are not limited to, any accounts receivable from an employee or student, student loans, student accounts under tuition payment plans, online student portals, payment platforms, and third-party processors (Touchnet, Workday, etc.).

Identity theft: Fraud that is committed or attempted using a person's identifying information without authorization.

Account Holder: An individual for whom a covered account is maintained.

Red flag: An event or item that signals potential theft of personal information.

Relevant department: An ACU department assigned the responsibility for designing procedures to comply with this policy and the FACT Act Identity Theft Red Flag Rules.
Stored value cards: prepaid cards (such as laundry cards or dining hall cards) that do not require an electronic fund transfer from the cardholder's account held by ACU for the purpose of transferring money between accounts or in exchange for money, property, goods, services, or cash.

IV. RESPONSIBILITY AND OVERSIGHT

The Director of Institutional Compliance & Risk Management (ICRM) will oversee the further development, implementation, and administration; ensure staff are trained; and oversee service provider arrangements. Administration methods for the program will include:

- Assigning to relevant department directors the responsibility for designing procedures that comply with the requirements of the program and training staff on specific responsibilities for the program.
- Directors of relevant departments will deliver to the Director of ICRM an annual report regarding compliance with the red flag rules. This report should address matters such as the effectiveness of the policies and procedures that address the risk of identity theft in connection with the opening of covered accounts or existing covered accounts, service provider arrangements, significant incidents of identity theft and the relevant department's response to these incidents, and recommendations for material changes to the program.
- Providing guidance for the Board of Trustees Audit & Risk Management Committee or equivalent to approve material changes to the program.

V. REQUIREMENTS OF THE PROGRAM

1. Service Providers – If service providers are used in connection with covered accounts, the relevant departments must ensure service providers are contractually required to implement reasonable identity theft prevention measures, comply with applicable law, and notify the university of any security incidents involving covered accounts.

2. Procedures – Relevant departments must document written procedures to be implemented that will:

- Define potential red flags for covered accounts
- Communicate the definitions of red flags to relevant personnel
- Detect red flags in the normal course of operations
- Respond appropriately to red flags to prevent and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts
- Ensure procedures are updated periodically to reflect changes in risks to students and Abilene Christian University
- Be reviewed periodically by the Director of ICRM

3. Risk Assessment – For potential red flags identified, the relevant department should document a risk assessment that identifies risks in these areas: financial, operations, compliance, reputation, and litigation. The risk assessment should consider the

following:

- Types of covered accounts offered or maintained
- Methods provided to open accounts
- Methods provided to access accounts
- Previous experiences with identity theft
- Methods used to reflect changes in identity theft

4. Detection of Red Flags – Relevant departments must address the detection of red flags: (1) when opening new covered accounts by obtaining identifying information about and verifying the identity of a person opening a covered account, and (2) when authenticating identity, monitoring transactions, and verifying the validity of data change requests related to existing covered accounts. Possible sources used for detecting red flags may include:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services
- Presentation of suspicious or altered documents
- Presentation of suspicious, inconsistent, or altered personal identifying information, such as a suspicious address change
- Attempts to access an account by unauthorized users
- Unusual use of or other suspicious activity related to a covered account • Notice from students or victims, identity theft law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts
- Red flags may include indicators of cybersecurity incidents, including unauthorized system access, compromised credentials, or suspicious electronic activity.

5. Response Program – Relevant departments must initiate appropriate responses for preventing and mitigating identity theft. A response is required whenever a red flag event has been identified. These responses may include:

- Monitoring a covered account for evidence of identity theft
- Contacting the known owner of the covered account
- Changing any passwords, security codes, or other security device that permit access to a covered account
- Reopening a covered account with a new account number
- Not opening a new covered account
- Closing an existing account
- Not attempting to collect on a covered account or not selling a covered account to a debt collector
- Notifying law enforcement
- Determining that no response is warranted under the particular circumstances • Documenting the response and the basis for the response decision
- Significant incidents must be escalated to the Director of Institutional Compliance & Risk Management and, where appropriate, the Office of General Counsel, and senior leadership.

VI. STUDENT IDENTIFICATION CARDS AND RELATED CHANGE OF ADDRESS REQUESTS

This section applies to relevant departments that issue cards, such as student identification cards,

which may be used as debit or credit cards. This does not include student identification cards that are stored-value cards. This policy may also apply to ACU's service providers to the extent that they issue credit or debit cards on behalf of ACU. If a service provider of ACU does not have a stated policy that complies with FACTA, the service provider must comply with this policy.

1. **Required response –** Pursuant to its obligations under FACTA, the relevant department shall assess the validity of a request for a change of address if it receives notification of a change of address for a cardholder's account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the relevant department receives a request for an additional or replacement card for the same account.

   Under these circumstances, the relevant department shall not issue an additional or replacement card, until it assesses the validity of the change of address through the following steps:

   • The relevant department shall notify the cardholder of the request clearly and conspicuously, provided separately from its regular correspondence at the cardholder's former address or by any other means of communication that ACU and the cardholder have previously agreed to use;
   • Provide the cardholder a reasonable means of promptly reporting incorrect address changes; and
   • Documenting the results of the address verification process.

2. **Address Verification Alternative –** The relevant department may satisfy the requirements of this policy by validating an address pursuant to the method set forth above in Section VI.1 when it receives an address change notification before it receives a request for an additional or replacement card.

VII. UPDATES

This policy and related procedures must be reviewed periodically and, if necessary, updated to reflect changes in risks from identity theft to students and to the safety and soundness of Abilene Christian University, taking into consideration:

- Experiences with identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent, and mitigate identity theft
- Changes in the types of accounts that Abilene Christian University offers
- Changes in the business arrangements of Abilene Christian University including mergers, acquisitions, alliances, joint ventures, and service provider arrangements