**PURPOSE**

Under the Red Flags Rule ([16 CFR 681](https://www.ecfr.gov/cgi-bin/text-idx?SID=510c40578b4aebe619f067a363ae7257&mc=true&node=pt16.1.681&rgn=div5)), the University is required to establish and maintain an Identity Theft Prevention Program (“Program”) designed to detect, prevent, and respond to identity theft regarding certain *covered accounts* it offers, services, or maintains. This template may be used to assist units required to comply with documenting processes for identifying, detecting, and responding to red flags. If you have questions or need assistance with completing this form, please contact the [Compliance Office for Finance and Administration](http://uca.edu/compliance/).

**DEFINITION & EXAMPLES**

*Covered accounts* are accounts offered or maintained by UCA or third-party service providers primarily for personal, family, or household purposes that allow multiple payments or transactions **or** any other account for which there is a reasonably foreseeable risk (operational, compliance, legal, etc.) to customers or UCA from identity theft.

Examples include student loans, student accounts, payment plans, Bear Cards, and Pay Cards. Please note your area may be subject to the Red Flags Rule if you perform an activity related to a covered account; the rule is not limited to the primary office.

**COLLEGE/ADMINISTRATIVE UNIT:** (Enter unit name here)

|  |  |
| --- | --- |
| Contact Name: |  |
| Title: |  |
| Phone No: |  |
| E-Mail: |  |
| Date: |  |

**Step 1: Identify Red Flags**

The first step is to identify the red flags your unit may encounter that indicate that people who are trying to obtain or access products or services from you aren’t who they state they are. For instance, if you require photo ID, a red flag of identity theft is an inconsistency between the individual’s appearance and the information on the photo ID. Sometimes, the only red flag may be notice from another source that identity theft has been attempted or has occurred. Since that red flag applies to any unit, it is listed below.

**Below are the relevant red flags we have identified:** (add lines as needed)

1. *Example: Suspicious documentation (e.g., a photo ID is presented that does not resemble the individual).*
2. *Example: Notice from a customer, a victim of identity theft, a law enforcement agency, or someone else that an account has been opened or used fraudulently.*

Step 2: Detect Red Flags

The next step is to explain how your unit will detect the red flags you’ve identified. For example, perhaps in Step 1 you identified false IDs as a red flag. To detect a false ID, you may consider training staff to carefully review the ID to determine whether the individual’s appearance is consistent with the picture on the ID. What if somebody notifies you that an account has been opened or used fraudulently? To make sure those notices are properly recorded and followed up as necessary, you may decide to require staff to log that in a central location (see **Red Flags Rule Incident Log**) or to notify a supervisor and/or the Program Administrator or designee(s).

Below is how we detect the red flags our unit has identified: (add lines as needed)

1. *Example: Staff require identification (such as UCA ID) to verify identity.*

Step 3: Respond to Red Flags

The third step is to decide how you will respond to any red flags that arise. For example, you have identified the risk of false IDs as an indication of identity theft and noted that you will train staff to look for inconsistencies in identification. An employee has checked the ID and detected an inconsistency. What happens next? It may be asking for another form of ID – or not providing any information, products, or services until the inconsistency has been resolved. Or, if you’re trying to collect on a past due student account, and the individual you contact tells you her identity was stolen and she has not received any correspondence in quite some time because her address was changed without consent. Although it will depend on the circumstances, consider how you will respond. For exam­ple, you could ask for proof that an identity theft report has been filed with the appropriate law enforcement and/or government agencies (such as the Federal Trade Commission).

**Here is how our unit responds to the red flags identified:** (add lines as needed)

1. *Example: If identification presented does not match, we do not release any information.*
2. *Example: If we are notified by a student he/she has been a victim of identity theft, we record it in the Red Flags Rule Incident Log, notify other offices as appropriate, and make a note on the student’s account.*

Third-Party Service Providers

If and when third-party service providers are engaged to perform an activity in connection with a covered account(s), steps must be taken to ensure the service provider acts in compliance with the University’s Identity Theft Prevention Program. This might include reviewing the service provider’s Identity Theft Prevention Program or, more likely, including language in the contract to confirm compliance.

Here are the service providers we use and how we confirm compliance: (add lines as needed)

1. *Example: ABC Company – Student Accounts contracts with ABC Company as a servicer for student loans. The contract with ABC Company contains language as follows…*

**Describe how staff will be trained**

List the categories/types of employees who will be trained to detect red flags and how they will be trained – for example, during new employee orientation, monthly staff meetings, etc.

**Here is how staff are trained on identifying, detecting, and responding to red flags:** (add lines as needed)

1. *Example: Financial Aid staff are trained upon hire and at least annually thereafter by reviewing the Red Flags Rule Training presentation on the Compliance Office website. Staff are also trained on identity verification procedures (such as over the phone) to ensure confidential information is only released to authorized individuals.*
2. *Example: Student Accounts staff are required to review the Red Flags Rule Training presentation on the Compliance Office website at least annually. Staff are trained on office procedures to ensure sensitive information is provided only to the individual or those with a “need to know.”*

Program Review and Annual Certification

1. Please review and adjust your unit’s plan as needed but at least annually.
2. Please complete and submit the **Red Flags Rule Certification Form** located on the [Red Flags Rule Compliance](http://uca.edu/compliance/red-flags-rule-compliance/) page.