## Ouachita Baptist University

# Identity Theft Policy and Program

Under the Federal Trade Commission's "Red Flags Rule", Ouachita Baptist University is required to establish an Identity Theft Prevention Program ("the program") which contains reasonable policies and procedures to:

- Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the program;
- Detect Red Flags that have been incorporated into the program; and
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.

This policy and program were adopted effective May 1, 2009 to comply with the Red Flags Rule.

## Definitions

"Covered Account" – any consumer account that involves multiple payments or transactions. At Ouachita, this is interpreted to mean any student account or loan administered by the university, including:

- Student accounts
- Perkins loan accounts
- Institutional loan accounts
- Past due accounts assigned to collection agencies
- Student ID cards that include a debit card feature

"Identifying Information" – any name or number that may be used, alone or in conjunction with any other information, to identify a specific person. Identifying information may include name, address, phone numbers, social security number, student ID number, alien registration number, government passport number or computer Internet Protocol (IP) address.

"Identity Theft" – a fraud committed or attempted using the identifying information of another person without authority or permission.

"Red Flag" – a pattern, practice, or specific activity that indicates the possible existence of identity theft.

## Identification of Red Flags

The university considers the following risk factors in identifying relevant red flags:

- The types of accounts offered and maintained
- The methods used to open accounts
- The methods provided to access accounts.

- Previous experiences with identity theft

Based on those risk factors, we have identified the following red flags, listed by category:

Suspicious Documents

- An identification document or card that appears to be forged, altered or inauthentic
- An identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document
- Other documents with information that is not consistent with existing student information
- Any application that appears to have been altered or forged

Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the student provides (e.g. inconsistent birth dates)
- Identifying information presented that is inconsistent with other sources of information on file (e.g. an address on a loan application not matching an address on file)
- Identifying information presented that is the same as information presented on other documents that were found to be fraudulent
- Identifying information presented that is consistent with fraudulent activity (e.g. an invalid phone number or fictitious billing address)
- A social security number presented that is the same as that of another person
- An address or phone number presented that is the same as that of another person
- A person fails to provide complete identifying information on an application when reminded to do so

Suspicious Covered Account Activity or Unusual Use of Account

- A change of address on an account followed by a request to change the student's name
- An account used in a way that is not consistent with prior use
- Mail sent to the account is repeatedly returned as undeliverable
- Notice provided by a student that the student is not receiving mail from the university
- Notice to the university by a student or a third party that an account has unauthorized activity
- A breach in the university's computer system security
- Detection of unauthorized access to or use of student account information

Alerts from Others

- Notice from a student, law enforcement or other person that the university has opened or is maintaining a fraudulent account.
- Notice or report of fraud from a credit agency or credit report

**Detecting Red Flags**

To detect any of the red flags identified above when a new covered account is opened, university personnel will take the following actions to obtain and verify the identity of the person opening the account.

- Identifying information, including name, date of birth, home address and previous academic records, must be provided before a new covered account can be established.
- The student's identity must be verified, through examining the student's university ID card, before a new loan account is established. Verification will be completed by Student Financial Services staff prior to disbursing loan funds.
- Verifying SSN of new students

To detect any of the red flags identified above for an existing covered account, university personnel will take the following actions to monitor transactions.

- Verify the identity of a student requesting information by telephone, email or in person.
- Requests to change billing addresses received by mail or email will be verified by mailing a confirmation to both the old and new address.
- Students will be provided a method to report incorrect billing addresses.
- Any change in banking information used for refunds of credit balances will be verified in writing.

**Preventing and Mitigating Identity Theft**

To diminish the likelihood of identity theft occurring on a covered account, the university will take the following actions to protect student identifying information:

- Avoid the use of social security numbers to identify students or student information
- Ensure that any websites on which payments are accepted are secure
- Require only that student identifying information that is essential for university purposes
- Ensure complete destruction of paper documents and computer files containing student account information that is no longer needed
- Ensure that office computers and/or computer software applications with access to covered account information are password protected
- Ensure that virus protection software is current on all computers containing covered account information

If university personnel detect any identified red flags, the following actions may be taken to mitigate the risk of identity theft, depending on the type of red flag detected:

- Contact the student to notify him or her of the identified red flags
- Continue to monitor the covered account for additional red flags or other evidence of identity theft
- Not open a new covered account for which the information was provided
- Reopen a covered account with a new account number
- Change any passwords or other security features that permit access to the covered accounts
- Notify the Program Administrator to determine appropriate steps
- Notify law enforcement
- Take no action if the circumstances do not warrant

## Program Administration

Responsibility for developing, implementing and updating this Program lies with the Program Administrator. The Chief Financial Officer will serve as Program Administrator unless the President appoints another individual. The Program Administrator will be responsible for the following:

- Program administration
- Ensuring that appropriate university staff are trained on specific responsibilities for the program
- Reviewing any staff reports regarding the detection of red flags and the steps for preventing and mitigating identity theft
- Determining which steps of prevention and mitigation should be taken in particular circumstances
- Providing guidance to the Board of Trustees as to periodic changes to the program based on experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, or changes in types of accounts the university maintains.
- Preparing and delivering an annual report to the Board of Trustees regarding compliance with Red Flag Rules

### <u>Staff Training and Reporting</u>

University staff responsible for implementing the program will be trained by or under the direction of the Program Administrator in the detection, prevention, and mitigation of red flags.

University staff are expected to notify the Program Administrator once they become aware of an incident of identity theft or of any failure by the university to comply with the program. At least annually, staff will provide a report to the Program Administrator of all red flags detected, all incidents of suspected or confirmed identity theft, and any recommendations for changes to the program.

Service Providers

Any third party service agencies used in connection with covered accounts must provide annually an identity theft program which meets the requirements of the “Red Flags Rule”. Those agencies include:

- Delinquent account collection agencies
- Loan servicers
- Debit card providers linked to student IDs

Any contracts with such service providers will require the provider to have such policies and procedures in place. The service provider must report any detected red flags to the Program Administrator within 30 days of detection and provide an annual report of all red flags detected and all incidents of suspected or confirmed identity theft.