The University of Alabama
Red Flags Identification and Detection Grid

Note that these procedures are included here for basic guidance, based on the categories and examples provided by the FTC. They are not exhaustive, nor a mandatory checklist. Instead, they are provided to assist each area or department think through relevant red flags in the context of their operations. You can and should develop more detailed procedures for your area as necessary.

In general, the following should be done in all situations where Red Flags are suspected:

- Once potentially fraudulent activity is detected, an employee must act quickly as an appropriate rapid response can protect individuals and the University from damages and loss. At a minimum, any employee who knows or suspects that a security incident has occurred shall immediately notify their appropriate supervisor and the Identity Theft Prevention Officer, who will report to the Program Administrator as needed.
- Additional investigations will be conducted to determine whether the attempted transaction was fraudulent or authentic.
- Take appropriate actions immediately if a transaction is determined to be fraudulent. Actions may include:
  - Canceling the transaction;
  - Notifying and cooperating with appropriate law enforcement;
  - Determining the extent of liability of the University; and
  - Notifying the actual individual upon whom fraud has been attempted.

Red Flag	Detecting the Red Flag
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency	
1. Notice/report of fraud or active duty alert	• Verify activity reported with applicant/ customer. • If verified, review the notice, freeze, or degree of inconsistency with prior history, and proceed with the evaluation of applicant based on a consumer report received. • If unable to verify, do not use this report in evaluating applicant – no further action required.
2. Notice/report of a credit freeze on an applicant	
3. Indication of activity that is inconsistent with an applicant's usual pattern or activity history Examples: a large increase in the volume of inquiries or use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account closed because of an abuse of account privileges.	

4. Notice of address or another discrepancy	• Compare reported address (or other information) with that provided by the applicant and, if necessary, contact the applicant to verify. • If address (or other information) has been verified, report to credit report agency. • If unable to determine the relationship between the applicant and the notice, do not use the report to evaluate the applicant and notify the applicant. No further action required. *Also, see the* [FTC's Address Discrepancy Rule (16 CFR part 641.1)]().
Category: Suspicious Documents	
5. Identification presented looks altered, forged, or inauthentic.	• Retain and scrutinize identification or other document presented to ensure: o it is not altered, forged, or torn up and reassembled; o that the photograph and the physical description on the identification match the person presenting it; o that the identification and the statements of the person presenting it are consistent; and/or o that the identification presented and other information we have on file is consistent. • Notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
6. The person presenting identification does not look like the identification's photograph or physical description.	
7. The person presenting identification conveys information that differs from what is indicated on the identification.	
8. Information on the identification does not match other information on file for the customer (e.g., employee/student information in Banner).	
9. A request for information, application, or other document looks like it has been altered, forged, or torn up and reassembled.	
Category: Suspicious Personal Identifying Information	
10. Identifying information is inconsistent with other external information sources. Examples: an address that does not match the address printed on an FAFSA form, a Social Security Number (SSN) that has not been issued or is listed on the Social Security Administration's (SSA's) Master Death File.	• Inspect information and compare with other external information sources. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
11. Identifying information is inconsistent with other information provided by the customer Examples: inconsistent dates of birth, SSNs, or addresses on two forms received.	• Inspect information and ask the customer to validate which information is accurate. • Retain information and notify management for assistance if necessary. Do not provide services until

	correct identifying information is proven. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
12. Identifying information is associated with known fraudulent activity. Example: an address or phone number being used is also known to be associated with a fraudulent application.	• Inspect information and compare with documentation indicating fraudulent activity. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
13. Identifying information suggests fraud or is of the type commonly associated with fraudulent activity. Examples: an address that is obviously fictitious, an address that is a mail drop or a prison, a phone number is invalid.	• Inspect information and determine its validity. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
14. The SSN or CWID number is the same as that submitted by another customer.	• Inspect information and request to see the student's Social Security card, CWID, or driver's license. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • Place hold on the original customer who provided the duplicate ID number if identity is proven. Direct customer to the FTC Identity Theft website if necessary to learn what steps to take to recover from identity theft. If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
15. Address or phone number is the same as that presented by an unusually large number of other customers.	• Request and inspect information to determine its validity. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.

16. A customer omits required personal identifying information on an application or other form or does not provide it in response to notification that the application/form is incomplete.	• Do not provide services or award aid until application/form is complete. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
17. Identifying information is inconsistent with internal information sources on file.	• Inspect information and compare with information in Banner or other official University systems of record or data files. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
18. A person seeking access to systems or sensitive information cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.	• Do not provide services, reset passwords, or otherwise provide access until identity is proven. • Follow any protocols established to recover access to the system in question (e.g., by notifying the system administrator to send a password reset link to the person's email). • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
Category: Suspicious Account Activity	
19. Change of address request followed shortly by request for a name change.	• Request official documentation reflecting name change (court order, marriage certificate, etc.) and compare with photo identification. • Verify change of address previously submitted. • If the customer did not initiate the action(s) and identity theft of the customer's information is suspected, direct customer to the FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
20. An account is used in a manner inconsistent with established patterns of activity on that account. For example, payments are no longer made on an otherwise consistently up-to-date account.	• Banner automatically places a financial hold on overdue accounts and restricts certain services from being provided until Student Account Services has removed the hold. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.

21. Mail sent to a customer is repeatedly returned as undeliverable even though the account remains active.	• Attempt to contact the customer via the contact information on file. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
22. Customer notifies UA (via phone, email, or in-person) that the customer is not receiving mail.	• Verify address information with customer and ensure listed addresses are active. • If the address on file was not entered by the customer, notify management for assistance. If identity theft of the customer's information is suspected, direct customer to the FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
23. Customer notifies UA (via phone, email, or in-person) that an account with the University has unauthorized activity.	• Verify if the notification is legitimate and involves a UA account. Notify management for assistance to investigate the activity. • If customer's account does have unauthorized activity and identity theft of the customer's information is suspected, direct customer to the FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
24. Customer notifies UA (via phone, email, or in-person) that unauthorized access to a University account that uses myBama authentication has occurred. Example: Customer is automatically logged off during an online session due to multiple login attempts from an external site.	• Verify if the notification is legitimate and involves a UA account. Notify management for assistance to investigate the activity. • Instruct the customer to reset the account password immediately. • If unauthorized access did occur and identity theft of the customer's information is suspected, direct customer to the FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.
Category: Notice from Other Sources	

25. A customer, an identity theft victim, or a law enforcement agent notifies UA (via phone, email, or in-person) that an account has been opened or used fraudulently.	• Verify if the notification is legitimate and involves a UA account. Notify management for assistance to investigate the activity and determine if any actions are needed (e.g., inactivating direct deposit, placing a financial hold on the account). • Direct customer to the FTC Identity Theft website to learn what steps to take to recover from identity theft, if the customer has not already done so. • If the fraud occurred during the conduct of University business, report the incident to the area ITPO, UAPD and complete the Red Flag Detection Report.
26. We learn that unauthorized access to the customer’s personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	• Verify if the notification is legitimate and involves a UA account. Notify management for assistance to investigate the activity and determine if any actions are needed (e.g., inactivating direct deposit, placing a financial hold on the account). • If identity theft of customer’s information is suspected, direct customer to the FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to the area ITPO, UAPD and complete the Red Flag Detection Report.