



1  
2  
3  
4  
5

**POLICY STATEMENT 75  
IDENTITY THEFT PREVENTION PROGRAM**

6  
7

**POLICY DIGEST**

8  
9  
10  
11  
12

**Primary Monitoring Unit: Business Affairs**  
**Initially Issued: May 27, 2009**  
**Last Revised: None (format updated March 22, 2022)**

13

**I. PROGRAM ADOPTION**

14  
15  
16  
17  
18  
19  
20  
21

LSU Eunice (“University”) developed this Identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission’s Red Flags Rule (“Rule”), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the Vice Chancellor for Business Affairs and the Director of Information Technology. After consideration of the size and complexity of the University’s operations and account systems, and the nature and scope of the University’s activities, the Vice Chancellor for Business Affairs determined that this Program was appropriate for LSU Eunice.

22

**II. PROGRAM PURPOSE AND DEFINITIONS**

23

**A. Fulfilling requirements of the Red Flags Rule**

24  
25  
26

Under the Red Flag Rule, every financial institution and creditor is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

- 27  
28  
29  
30  
31  
32  
33
1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
  2. Detect Red Flags that have been incorporated into the Program;
  3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
  4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

34

**B. Red Flags Rule definitions used in this Program**

35  
36

The Red Flags Rule defines “Identity Theft” as “fraud committed using the identifying information of another person” and a “Red Flag” as a pattern, practice, or specific activity

37 that indicates the possible existence of Identity Theft.

38 The Rule defines creditors “to include finance companies, automobile dealers, mortgage  
39 brokers, utility companies, and telecommunications companies. Where non-profit and  
40 government entities defer payment for goods or services, they, too, are to be considered  
41 creditors.”

42 All the University accounts that are individual customer accounts of the University are  
43 covered by the Rule. Under the Rule, a “covered account” is:

- 44 1. Any account the University offers or maintains primarily for personal, family or  
45 household purposes, that involves multiple payments or transactions; and
- 46 2. Any other account the University offers or maintains for which there is a reasonably  
47 foreseeable risk to customers or to the safety and soundness of the University from  
48 Identity Theft.

49 “Identifying information” is defined under the Rule as “any name or number that may be  
50 used, alone or in conjunction with any other information, to identify a specific person,”  
51 including: name, address, telephone number, social security number, date of birth,  
52 government issued driver’s license or identification number, alien registration number,  
53 government passport number, employer or taxpayer identification number, unique  
54 electronic identification number, computer’s Internet Protocol address, or routing code.

### 55 **III. IDENTIFICATION OF RED FLAGS.**

56 In order to identify relevant Red Flags, the University considers the types of accounts that it  
57 offers and maintains, the methods it provides to open its accounts, the methods it provides to  
58 access its accounts, and its previous experiences with Identity Theft. The University identifies  
59 the following red flags, in each of the listed categories:

#### 60 **A. Notifications and Warnings from Credit Reporting Agencies**

##### 61 Red Flags

- 62 1. Report of fraud accompanying a credit report;
- 63 2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
- 64 3. Notice or report from a credit agency of an active duty alert for an applicant; and
- 65 4. Indication from a credit report of activity that is inconsistent with a customer’s usual  
66 pattern or activity.

#### 67 **B. Suspicious Documents**

##### 68 Red Flags

- 69 1. Identification document or card that appears to be forged, altered or inauthentic;
- 70 2. Identification document or card on which a person’s photograph or physical  
71 description is not consistent with the person presenting the document;

- 72 3. Other document with information that is not consistent with existing customer  
73 information (such as if a person's signature on a check appears forged)
- 74 C. Suspicious Personal Identifying Information
- 75 Red Flags
- 76 1. Identifying information presented that is inconsistent with other information the  
77 customer provides (example: inconsistent birth dates);
- 78 2. Identifying information presented that is inconsistent with other sources of  
79 information (for instance, an address not matching an address on a credit report);
- 80 3. Identifying information presented that is the same as information shown on other  
81 applications that were found to be fraudulent;
- 82 4. Identifying information presented that is consistent with fraudulent activity (such as  
83 an invalid phone number or fictitious billing address);
- 84 5. Social security number presented that is the same as one given by another  
85 customer;
- 86 6. An address or phone number presented that is the same as that of another person;
- 87 7. A person fails to provide complete personal identifying information on an application  
88 when reminded to do so (however, by law social security numbers must not be  
89 required); and
- 90 8. A person's identifying information is not consistent with the information that is on file  
91 for the customer.
- 92 D. Suspicious Covered Account Activity or Unusual Use of Account
- 93 Red Flags
- 94 1. Change of address for an account followed by a request to change the account  
95 holder's name;
- 96 2. Payments stop on an otherwise consistently up-to-date account;
- 97 3. Account used in a way that is not consistent with prior use (example: very high  
98 activity);
- 99 4. Mail sent to the account holder is repeatedly returned as undeliverable;
- 100 5. Notice to the University that a customer is not receiving mail sent by the University;
- 101 6. Notice to the University that an account has unauthorized activity;
- 102 7. Breach in the University's computer system security; and
- 103 8. Unauthorized access to or use of customer account information.

104 E. Alerts from Others

105 Red Flag

106 1. Notice to the University from a customer, identity theft victim, law enforcement or  
107 other person that it has opened or is maintaining a fraudulent account for a person  
108 engaged in Identity Theft.

#### 109 IV. DETECTING RED FLAGS.

110 A. New Accounts

111 To detect any of the Red Flags identified above associated with the opening of a **new**  
112 **account**, University personnel will take the following steps to obtain and verify the  
113 identity of the person opening the account:

114 Detect

115 1. Require certain identifying information such as name, date of birth, residential or  
116 business address, principal place of business for an entity, driver's license or other  
117 identification;

118 2. Verify the customer's identity (for instance, review a driver's license or other  
119 identification card);

120 3. Review documentation showing the existence of a business entity; and

121 4. Independently contact the customer.

122 B. Existing Accounts

123 To detect any of the Red Flags identified above for an **existing account**, University  
124 personnel will take the following steps to monitor transactions with an account:

125 Detect

126 1. Verify the identification of customers if they request information (in person, via  
127 telephone, via facsimile, via email);

128 2. Verify the validity of requests to change billing addresses; and

129 3. Verify changes in banking information given for billing and payment purposes.

#### 130 V. PREVENTING AND MITIGATING IDENTITY THEFT

131 In the event University personnel detect any identified Red Flags, such personnel shall take one  
132 or more of the following steps, depending on the degree of risk posed by the Red Flag:

##### 133 Prevent and Mitigate

134 A. Continue to monitor an account for evidence of Identity Theft;

- 135 B. Change any passwords or other security devices that permit access to Covered  
136 Accounts;
- 137 C. Not open a new Covered Account;
- 138 D. Provide the customer with a new identification number;
- 139 E. Notify law enforcement;
- 140 F. File or assist in filing a Suspicious Activities Report (“SAR”); or
- 141 G. Determine that no response is warranted under the particular circumstances.

142 **Protect Customer Identifying Information**

143 In order to further prevent the likelihood of identity theft occurring with respect to University  
144 accounts, the University will take the following steps with respect to its internal operating  
145 procedures to protect customer identifying information:

- 146 A. Ensure that its website is secure or provide clear notice that the website is not secure;
- 147 B. Ensure complete and secure destruction of paper documents and computer files  
148 containing customer information;
- 149 C. Ensure that office computers are password protected and that computer screens lock  
150 after a set period of time;
- 151 D. Keep offices clear of papers containing customer information;
- 152 E. Request only the last 4 digits of social security numbers (if any);
- 153 F. Ensure computer virus protection is up to date; and
- 154 G. Require and keep only the kinds of customer information that are necessary for  
155 University purposes.

156 **VI. PROGRAM UPDATES**

157 This Program will be periodically reviewed and updated to reflect changes in risks to customers  
158 and the soundness of the University from Identity Theft. At least each year the Director of  
159 Information Technology will consider the University’s experiences with Identity Theft situations,  
160 changes in Identity Theft methods, changes in Identity Theft detection and prevention methods,  
161 changes in types of accounts the University maintains and changes in the University’s business  
162 arrangements with other entities. After considering these factors, the Director of Information  
163 Technology will determine whether changes to the Program, including the listing of Red Flags,  
164 are warranted. If warranted, the Director of Information Technology will update the Program or  
165 present the Vice Chancellor for Business Affairs with his or her recommended changes and the  
166 Vice Chancellor for Business Affairs will make a determination of whether to accept, modify or  
167 reject those changes to the Program.

168 **VII. PROGRAM ADMINISTRATION.**

169 **A. Oversight**

170 Responsibility for developing, implementing and updating this Program lies with the Vice  
171 Chancellor for Business Affairs in coordination with the Director of Information Technology. The  
172 Director of Information Technology will be responsible for the Program administration, for  
173 ensuring appropriate training of University staff on the Program, for reviewing any staff reports  
174 regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft,  
175 determining which steps of prevention and mitigation should be taken in particular  
176 circumstances and considering periodic changes to the Program.

177 **B. Staff Training and Reports**

178 University personnel shall be trained at the new employee training workshop held each year in  
179 the fall. Additionally, each year all employees will be notified via email of this policy statement.  
180 University employees are expected to notify the Director of Information Technology once they  
181 become aware of an incident of Identity Theft.

182 **C. Service Provider Arrangements**

183 In the event the University engages a service provider to perform an activity in connection with  
184 one or more accounts, the University will take the following steps to ensure the service provider  
185 performs its activity in accordance with reasonable policies and procedures designed to detect,  
186 prevent, and mitigate the risk of Identity Theft.

- 187       A. Require, by contract, that service providers have such policies and procedures in place;  
188       and
- 189       B. Require, by contract, that service providers review the University's Program and report  
190       any Red Flags to the Director of Information Technology.

191 **D. Specific Program Elements and Confidentiality**

192 For the effectiveness of Identity Theft prevention Program, the Red Flag Rule envisions a  
193 degree of confidentiality regarding the University's specific practices relating to Identity Theft  
194 detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific  
195 practices is to be limited to those employees who need to know them for purposes of preventing  
196 Identity Theft. Because this Program is to be adopted by a public body and thus publicly  
197 available, it would be counterproductive to list these specific practices here. Therefore, only the  
198 Program's general red flag detection, implementation and prevention practices are listed in this  
199 document.