

The Southern Baptist Theological Seminary  
**IDENTITY THEFT “RED FLAGS” AND RESPONSE INSTRUCTIONS**  
 IDENTITY THEFT AND PREVENTION PROGRAM  
 As of June 2010

<i>RED FLAG</i>	<i>RESPONSE INSTRUCTIONS</i>
<b>Suspicious Documents</b>	
1. An identification document or card that appears to be forged, altered or inauthentic	1. (1) Ask for an alternative form of identification that would be sufficient to grant request. (2) If unable to adequately verify identity: <ul style="list-style-type: none"> <li>• Reject request.</li> <li>• If the Seminary is the issuer, contact supervisor to determine whether to confiscate, or only copy, the document/card in question.</li> <li>• If the Seminary is not the issuer, copy the document/card in question.</li> <li>• Notify Campus Security of the Red Flag (who will investigate the matter).</li> </ul>
2. An identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document	2. Same as no. 1 above.
3. An identification document containing information not consistent with existing individual information	3. Same as no.1 above.

*(The form, Report On An Identity Theft “Red Flag”, must be filed for each Red Flag observed...it is available at Inside Southern Seminary)*

The Southern Baptist Theological Seminary  
**IDENTITY THEFT “RED FLAGS” AND RESPONSE INSTRUCTIONS**  
 IDENTITY THEFT AND PREVENTION PROGRAM  
 As of May 2010

<i>RED FLAG</i>	<i>RESPONSE INSTRUCTIONS</i>
<b>Suspicious Personal Identifying Information</b>	
4. An application that appears to have been altered or forged	4. (1) Ask questions to determine authorship or better understand situation. (2) Compare to other information on file. (3) Consider contacting other offices for verifying information, as applicable. (4) If unable to verify authenticity of information on application, reject application.
5. Identifying Information is presented that is inconsistent with other information the individual provides, or with information from external sources	5. Same as no. 1 above.
6. Identifying Information is presented that is the same as information shown on other applications that were found to be fraudulent	6. (1) Notify Campus Security of Red Flag and to have them attempt to apprehend individual if still present. (2) Copy or confiscate identifying information. (3) Reject request.
7. Identifying Information is presented that is consistent with fraudulent activity	7. Same as no.6 above.

*(The form, Report On An Identity Theft “Red Flag”, must be filed for each Red Flag observed...it is available at Inside Southern Seminary)*

The Southern Baptist Theological Seminary  
**IDENTITY THEFT “RED FLAGS” AND RESPONSE INSTRUCTIONS**  
 IDENTITY THEFT AND PREVENTION PROGRAM  
 As of May 2010

<i>RED FLAG</i>	<i>RESPONSE INSTRUCTIONS</i>
<b>Suspicious Personal Identifying Information (continued)</b>	
8. A social security number presented is the same as one given by another individual	8. (1) Record SSN and obtain copy of document that contains SSN, if possible. (2) Attempt to reconcile SSN with existing records. (3) If unable to reconcile, contact local Social Security office. (4) Notify Campus Security of Red Flag.
9. An address or phone number is presented that is the same as that of another person	9. (1) Attempt to reconcile phone number. (2) If unable to reconcile, reject request until address and/or phone number information can be confirmed.
10. Identifying Information included in a person's file that is not consistent with the information that is on file for the individual	10. (1) Attempt to reconcile inconsistency in information. (2) If unable to reconcile, place any request associated with the information on hold pending further investigation by Campus Security. (3) Notify Campus Security of the Red Flag and request further investigation.
11. A person fails to provide complete personal Identifying Information on an application when reminded to do so	11. (1) Postpone action on the application until complete personal identifying information is provided. (2) Notify Campus Security of individual's name, address, phone number, and a brief description of incident.

*(The form, Report On An Identity Theft “Red Flag”, must be filed for each Red Flag observed...it is available at Inside Southern Seminary)*

The Southern Baptist Theological Seminary  
**IDENTITY THEFT “RED FLAGS” AND RESPONSE INSTRUCTIONS**  
 IDENTITY THEFT AND PREVENTION PROGRAM  
 As of May 2010

<i>RED FLAG</i>	<i>RESPONSE INSTRUCTIONS</i>
<b>Suspicious Covered Account Activity</b>	
12. Change of address for an account followed by a request to change the individual's name or for a replacement or additional card ( <i>applicable only to Campus Technology</i> )	<b>12. (Yet to be drafted)</b>
13. Payments stop on an otherwise consistently up-to-date account	13. (1) Contact individual (student, employee, or customer) as part of normal collection procedures. (2) Inquire about and document reasons given for stop in payments. (3) Notify Controller if additional direction is required for next actions to be taken.
14. Account used in a way that is not consistent with prior use	14. (1) Inform your department's director of the inconsistency and request direction as to actions to be taken. (2) Department director shall inform Chief of Campus Security if deemed appropriate for investigation.
15. Mail sent to the individual is repeatedly returned as undeliverable	15. (1) Contact individual by telephone or e-mail to obtain new address. (2) Enter corrected address information in ADDR and other required systems. (3) Document subsequent mailings until address is validated.

*(The form, Report On An Identity Theft “Red Flag”, must be filed for each Red Flag observed...it is available at Inside Southern Seminary)*

The Southern Baptist Theological Seminary  
**IDENTITY THEFT “RED FLAGS” AND RESPONSE INSTRUCTIONS**  
 IDENTITY THEFT AND PREVENTION PROGRAM  
 As of May 2010

<i>RED FLAG</i>	<i>RESPONSE INSTRUCTIONS</i>
<b>Suspicious Covered Account Activity (continued)</b>	
16. Notice to the Seminary that an individual is not receiving mail sent by the Seminary	16. (1) Contact individual by telephone or e-mail to obtain new address. (2) Enter corrected address information in ADDR and other required systems. (3) Document subsequent mailings until address is validated.
17. Notice to the Seminary that an account has unauthorized activity	17. (1) Notify and provide a summary of the notice received to <ul style="list-style-type: none"> <li>• Your department's director (who may elect to place a “freeze” on the account),</li> <li>• The Controller if a financial account is involved (who may elect to place a “freeze” on the account), and</li> <li>• The Chief of Campus Police.</li> </ul> (2) Request direction as to appropriate actions to be taken.
18. Breach in the Seminary's computer system security. (For purposes of this Red Flag, "computer system" includes servers, desktops, laptops, copiers, PDAs, USB disk drives, and similar devices that store or process data).	18. (1) Immediately report the breach to the VP for Campus Technology (or in his absence, either the Director of Network Services or the Director of Software Development). (2) The VP for Campus Technology (or his delegate) will notify the SVP for Institutional Administration, the Chief of Campus Police, and if appropriate, Seminary counsel, to determine the next steps to be taken, including following all federal and state regulations with regard to notification in the event identifying information has been disclosed.

*(The form, Report On An Identity Theft “Red Flag”, must be filed for each Red Flag observed...it is available at Inside Southern Seminary)*

The Southern Baptist Theological Seminary  
**IDENTITY THEFT “RED FLAGS” AND RESPONSE INSTRUCTIONS**  
 IDENTITY THEFT AND PREVENTION PROGRAM  
 As of May 2010

<i>RED FLAG</i>	<i>RESPONSE INSTRUCTIONS</i>
<b>Suspicious Covered Account Activity (continued)</b>	
19. Unauthorized access to or use of individual account information	19. (1) Contact Chief of Campus Police regarding incident. (2) Document facts and circumstances of the incident. (3) Notify the SVP for Institutional Administration, and if appropriate, Seminary counsel, to determine appropriate actions to advise and assist individual. (4) Consider placing a “freeze” on the account.
<b>Alerts from Others</b>	
20. Notice to the Seminary from an individual, Identity Theft victim, law enforcement, or other person that the Seminary has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.	20. (1) Notify and provide a summary of the notice received to <ul style="list-style-type: none"> <li>• Your department's director, and</li> <li>• The Chief of Campus Police and request direction as to appropriate actions to be taken.</li> </ul>

*(The form, Report On An Identity Theft “Red Flag”, must be filed for each Red Flag observed...it is available at Inside Southern Seminary)*

The Southern Baptist Theological Seminary  
**IDENTITY THEFT “RED FLAGS” AND RESPONSE INSTRUCTIONS**  
 IDENTITY THEFT AND PREVENTION PROGRAM  
 As of May 2010

<i>RED FLAG</i>	<i>RESPONSE INSTRUCTIONS</i>
<b>Notifications and Warnings from Consumer Reporting Agencies</b> <i>(applicable only to Security and Human Resources)</i>	
21. A fraud or active duty report accompanies a credit report	21. The Chief of Campus Police will initiate a joint evaluation of the red flag with the Director of Human Resources. They will mutually determine the severity of the Red Flag and the circumstances involved. The director of Human Resources will implement one of the following actions, as applicable: <ul style="list-style-type: none"> <li>• Achieve a satisfactory explanation or resolution</li> <li>• Withdraw the employment offer, or</li> <li>• Terminate the employee's employment.</li> </ul>
22. A notice from a credit agency of a credit freeze on an applicant.	22. See no. 21 above.
23. A notice of address discrepancy in response to a credit report request	23. See no. 21 above.
24. A credit report indicates a change in the applicant's usual pattern of activity	24. See no. 21 above.

*(The form, Report On An Identity Theft “Red Flag”, must be filed for each Red Flag observed...it is available at Inside Southern Seminary)*