

















9. Determine that no response is warranted under the particular circumstances.

### **Part 7. Staff Training and Reports**

System personnel responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. College, University, and Office of the Chancellor personnel are expected to notify their Program Administrator once they become aware of an incident of Identity Theft. At least annually or as otherwise requested by the Identify Theft Prevention Program Committee, Program Administrators shall report on compliance with the Program. The report will address such issues as effectiveness of the guidance in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft, and recommendations for changes to the Program.

### **Part 8. Service Provider Arrangements**

In the event the College, University or Office of the Chancellor engages a service provider to perform an activity in connection with one or more Covered Accounts, the College, University or Office of the Chancellor must take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

1. Require, by contract, that the service provider has such policies and procedures in place; and
2. Require, by contract, that the service provider review the System's Program and report any Red Flags to the responsible Program Administrator or the College, University or Office of the Chancellor employee with primary oversight of the service provider relationship.