Identity Theft - Red Flags - Checklist for Managers

1) Review internal processes where services or credit are provided to customers and implement the guidelines as necessary.

✓   Develop a compliance plan for your department to meet the requirements of the university red flags policy. Determine which of the 26 red flags apply to your business practices and which of the university red flag guidelines you should incorporate into your plan.

✓   Your compliance plan should begin with an assessment of your current business practices. Identify areas in your business processes where there is risk for identity theft to occur.

✓   Consider the types of accounts and the number of ways those accounts are created or assessed. Have you been defrauded before by someone using stolen information? How was it done?

✓   The compliance plan should include details such as roles and responsibilities of each staff member.

2) Update internal control structure or standard operating procedures as appropriate to reflect university guidelines.

✓   Determine the risk associated with each of your business processes.

✓   Determine whether you have proper controls in place or whether you should add some. Do gaps exist in your business procedures to identify individuals establishing university accounts? Do your procedures require a customer to present a photo identification to establish an account?

✓   Your compliance plan may incorporate documenting and reinforcing many of your existing controls.

3) Annually review internal processes, control structures and standard operating procedures for continued compliance with guidelines.

✓   The updates should document the action steps as defined in the Identity Theft Red Flags guidelines and how these guidelines will be applied within your unit.

✓   Don't forget to update any internal training manuals or other materials.

4) Identify employees who must complete training and ensure that training is completed.

✓   Ensure that your staff receives the necessary training. This includes training on the unit's internal processes as well as taking the online red flags training. Make sure that you and your staff are familiar with university policies related to protecting identifying information.

✓   New employees will need to complete this training within two weeks of their hire date.

Questions regarding the policy and training should be directed to George Bass, Director of Business Services, 507-537-7470 or George.Bass@smsu.edu.