

651 RED FLAGS POLICY

Policy 675 was approved by the ISU Board of Trustees on October 24, 2008.

651.1 Federal Requirements. The Federal Trade Commission (FTC) issued the “Red Flags Rule” under sections 114 and 315 of the Fair and Accurate Credit Transaction Act (FACT Act), which is intended to reduce the risk of identity theft. The National Association of College and University Business Officers (NACUBO) issue a statement in late September, 2008 that states that “parts of the rule likely cover many colleges and universities...”. NACUBO also stated that activities that could cause colleges and universities to be considered ‘creditors’ under the Red Flags Rule...” may include participation in the Federal Perkins Loan Program and/or offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester, among others. Since Indiana State University (ISU) regularly conducts several of the FTC example activities, we believe that ISU is required to be compliant by November 1, 2008.

651.2 Initial Program. The FTC has identified five categories of red flags that have been further defined into 26 examples that ISU will utilize as an initial written program, as they apply to us. The initial program will include red flags from the following categories:

1. Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2. The presentation of suspicious documents;
3. The presentation of suspicious personal identifying information, such as a suspicious address change;
4. The unusual use of, or other suspicious activity related to, a covered account; and
5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

651.3 Future Program Development. Further future program development will be the responsibility of University senior level management, who will ensure that the program designed will detect, prevent, and mitigate identity theft, and that the overall effectiveness of the program is appropriate to ISU’s size, complexity, and the nature and scope of its operations.

Last revised February 1, 2011