Attachment B

Possible Identified Red Flags

A. Alerts, notifications or warnings from a consumer reporting agency:

1. Receipt of a fraud or active duty alert accompanying a consumer credit report;
2. Receipt of a notice of credit freeze provided in response to a request for a consumer report;
3. Receipt of a notice of address discrepancy from a credit reporting agency; and
4. Receipt of a consumer report which indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of the account holder (e.g. recent and significant increase in number of inquiries; unusual number of recently established credit relationships; a material change in the use of credit).

B. Suspicious Documents

1. Documents presented for the purpose of personal identification are incomplete or appear to have been altered, forged or inauthentic;
2. The photographic and/or physical description on the personal identification is inconsistent with the appearance of the individual presenting the document;
3. Other information contained on the personal identification is inconsistent with information provided by the individual opening a new covered account or when presenting the personal identification for verification;
4. Other information contained on the personal identification is inconsistent with readily accessible information on file with the University; and
5. An application received by the University appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious Personal Identifying Information

1. Personal identifying information provided is inconsistent when compared against external information sources used by the University (e.g. discrepancies in addresses);

2. Personal identifying information provided is inconsistent when compared against internal information held by University, such as discrepancies in addresses, phone numbers, and other personal identifying information;
3. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University, such as fictitious and/or duplicated phone numbers, addresses or social security number;
4. Personal identifying information provided is fictitious and/or the same or very similar to that submitted by others opening an account or holding existing accounts, such as addresses, telephone numbers, bank accounts, and social security numbers;
5. The student or individual opening a covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete; and
6. Challenge questions, used by University to allow students and individuals to access their covered accounts, are answered incorrectly.

D. Unusual Use of, or Suspicious Activity Related to, the Covered Account

1. Shortly following a change of address to a covered account, or a request to change the address, University receives a request to change the account holder's name, a request for the addition of authorized users on the account, or other suspect request;
2. A covered account that has been inactive for a reasonably lengthy amount of time is used in an unusual manner;
3. Mail sent to the account holder is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account;
4. The University is notified that the student or individual is not receiving paper account statements and those statements are not being returned as undeliverable; and
5. The University is notified of unauthorized changes or transactions in connection with a student's or individual's covered account.

E. Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by University

1. University is notified by a student or individual account holder, a victim of Identity Theft, a law enforcement entity, or any other person that it has opened a fraudulent account for a person engaged in Identity Theft.