Identity Theft Prevention Program
Appendix: Red Flag Indicators

SUSPICIOUS DOCUMENTS

Documents provided for identification that appear to have been altered or forged.

The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

Other information on the identification is not consistent with readily accessible information that is on file with the University, such as information previously provided by a student in a loan entrance interview.

An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

SUSPICIOUS PERSONAL IDENTIFYING INFORMATION

Personal identifying information provided is inconsistent when compared against information sources used by the University, e.g.:

- The address does not match any address in the student record.
- The WSU ID number does not exist or is assigned to another student.
- Personal identifying information provided by the student is not consistent with other personal identifying information previously provided, e.g., date of birth.

Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University, e.g., University police reports.

The student opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

Personal identifying information provided is not consistent with personal identifying information that is on file with the University.

When using security questions (e.g., mother's maiden name, pet's name) the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Identity Theft Prevention Program
Appendix: Red Flag Indicators

UNUSUAL OR SUSPICIOUS ACTIVITY

Shortly following a notice of a change of address for a covered account, the University receives a request for new, additional, or replacement goods or services.

A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example, nonpayment when there is no history of late or missed payments.

Mail sent to the student is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the student's covered account.

The University is notified of unauthorized charges or transactions in connection with a customer's covered account.

The University receives notice from students, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University.

A student, a victim of identity theft, a law enforcement authority, or any other person that the University has opened a fraudulent account for a person engaged in identity theft notifies the University.