Ohio University Identity Theft Prevention Program:

Ohio University developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

The purpose of this Program is to document the protocol adopted by Ohio University in compliance with the Red Flags Rules. Many offices at the university maintain files on students, employees and patients, both in paper and electronic form with identity information. These files include, but are not limited to: admission information, financial aid information, billing information, employee personal information, academic and financial records, and patient records. In addition, the university hires outside service providers to perform institutional functions which may contain identity information.

This program will identify the areas of risk associated with identity theft on campus; will address the means whereby those risks will be identified; and will identify the methods of response to such Red Flags in order to mitigate the effects of identity theft.

Applying the Red Flags Rules to Ohio University

Per the Federal Trade Commission guidelines, the university would be a low risk entity for identity theft because:

1. The u

- Personal identifying information provided is associated with known fraudulent activity, such as addresses or phone numbers that have been previously submitted on fraudulent applications.
- Personal identifying information provided is of a type that is commonly associated with fraudulent activity. Examples are addresses submitted that are fictitious, a mail drop, or a prison, and phone numbers submitted that are invalid or are associated with a pager or answering service.
- The SSN provided is the same as that submitted by another person applying.
- The address or telephone number provided is the same or similar to the address or telephone number submitted by that of another person.
- The individual 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.
- When establishing security questions and answers, the person opening the covered account cannot provide authenticating information beyond that which would generally be available from a wallet or consumer report.

D. Suspicious covered account activity – Examples include bu1tatif7/MC i2 (ons)-1 ( )5Tn-1 (pp
Evi W2ngestablishm /LBoT (act)-1 (c)-2 (/6.2 (ato4 t)-a)-1a 1ise 12 a /LBoTj -LBoTd-13 (x(alcx

Step 2 – Detecting Red Flags (Current procedures designed to detect red flags in day to day operations)

A. Student Enrollment

- x Require specific identifying information such as name, date of birth, home address, or other identification; and
- x Verify the student's identity at the time of issuance of the student identification card by reviewing the student's driver license or other approved government issued photo identification.

B. Existing covered accounts

- x

x C C-2Ctl0-2013535-0C.3C35 0 C

Service Providers

In the event the