



# Identity Theft Red Flags

## Office of the Chief Information Officer

Applies to: University colleges/units, including the Medical Center, that collect and maintain personal information as it relates to the sale of goods or services on credit or extension of credit.

### POLICY

Issued: Target date: 5/1/2009  
Revised:

Federal regulations commonly known as Fair and Accurate Credit Transactions Act (FACTA) of 2003 Red Flags require that the university develop, implement and maintain a written identity theft program to detect, prevent and mitigate identity theft in conjunction with accounts that are opened and/or managed in relationship to the sale of goods or services on credit or the extension of credit.

### Table of Contents *(optional; suggested for documents 8-10 pages or longer, create links to sections if possible)*

### Definitions

Term	Definition
Account	A continuing relationship established by a person with the University to obtain a product or service for any purpose that involves or is designed to permit multiple payments or transactions. Account includes an extension of credit involving a deferred payment. Types of accounts include university based student loans, accounts receivable, patient financial accounts, medical records, gift shop credit accounts, tuition payment plans, etc. In addition, an account includes any type of account that the university offers or maintains for which there is a foreseeable risk to the customer of identity theft.
Identifying information	Any name, number or unique biometric data that may be used, alone or in conjunction with any other information, to identify a specific person. Examples of identifying information include but are not limited to name, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, fingerprint, voice print, retina or iris image or other unique physical representation or unique electronic identification number.
Identity theft	A fraud attempted or committed using the identifying information of another person without authority
Red flag	A pattern, practice or specific activity that indicates the possible existence of identity theft

### Policy Details

#### I Policy Intent

- A. The risk to the university and its students, faculty, staff and other customers from data loss and identity theft is of significant concern to the university and the university will make reasonable efforts to detect, prevent and mitigate identity theft associated with an Account.
- B. This policy is intended to work in conjunction with university and Medical Center policies such as Institutional Data, Health Insurance Privacy, Privacy and Release of Student Education Records as well as any other privacy and security standards and requirements, including Payment Card Industry (PCI).

#### II Identity Theft Red Flags Program

- A. The university will develop, implement and maintain an Identity Theft Red Flags program. At a minimum the program will include:



# Identity Theft Red Flags

## Office of the Chief Information Officer

1. Processes for identifying patterns, practices or specific activities that indicate the possible existence of an identity theft,
2. Identification of reasonable and appropriate action steps that will be taken when a pattern, practice or specific activity has been detected,
3. Processes for requiring that accounts accessed or managed by external vendors on behalf of the University have implemented an appropriate program,
4. Training to educate employees on the program,
5. Periodic review and updates to the program and,
6. Annual program reporting to appropriate university leadership.

### PROCEDURE

Issued: 5/1/2009  
Revised:

Business processes that involve the sale of goods or services or extension of credit will be continually reviewed and analyzed for compliance with the Identity Theft Red Flags program. Each process that is determined to be affected by the Identity Theft Red Flags will have appropriate action steps documented. The detailed documentation will be maintained at [buckeyesecure.osu.edu](http://buckeyesecure.osu.edu).

### Responsibilities

Position or Office	List of Responsibilities
Office of the CIO	Administer the Identity Theft Red Flags program, which includes the following: 1) facilitating the business process analysis and maintenance of documentation 2) ensuring that appropriate training is offered 3) ensuring that the program is periodically reviewed and updated 4) ensuring that an annual program report is provided to appropriate university leadership
Colleges/units	1) Implement processes to detect and mitigate identity theft as well as report identified red flag incidents; 2) Ensure employees complete necessary training 3) Update internal control structure or standard operating procedures as appropriate.
Employees involved in affected business processes	1) Follow the appropriate action steps as documented 2) Complete necessary training.

### Resources

Accounts Receivable Policy (<http://www.osu.edu/policies/home>)

Credit Card Policy (<http://www.osu.edu/policies/home>)

Credit Card Merchant Policy Credit Card Handling Responsibilities and Procedures (<http://www.treasurer.ohio-state.edu/PDFS/Merchant%20Policies%20and%20Procedures%202007.pdf>)

Fair and Accurate Credit Transactions Act of 2003 (<http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>)



# Identity Theft Red Flags

## Office of the Chief Information Officer

---

Health Insurance Privacy Policy (<http://www.osu.edu/policies/home>)

Identity Theft Red Flags Program details (<http://buckeyesecure.osu.edu>)

Institutional Data Policy (<http://www.osu.edu/policies/home>)

Privacy and Release of Student Education Records ([http://www.ureg.ohio-state.edu/ourweb/more/Content/ferpa\\_pg1.html](http://www.ureg.ohio-state.edu/ourweb/more/Content/ferpa_pg1.html))

### Contacts

---

Subject	Office	Telephone	E-mail/URL
Policy or procedure clarification	Office of the CIO	292-6553	<a href="http://cio.osu.edu/policies">http://cio.osu.edu/policies</a>
Identity Theft Red Flags program, processes or training	Office of the CIO	292-6553	<a href="http://buckeyesecure.osu.edu">http://buckeyesecure.osu.edu</a>

### History

---

Issued: