# Identity Theft Red Flags
# Policy 5.16
## Office of Business & Finance

**Applies to**: University colleges/units, including the health system, that collect and maintain personal information for the purpose of allowing their customers to obtain goods, services or credit.

## POLICY

Issued: 09/2009
Revised:

The Ohio State University recognizes that identity theft is a continuing and growing issue that can result in harm to its customers as well as the institution. The Fair and Accurate Credit Transactions Act (FACTA) of 2003 Section 114 Red Flag Regulations and Guidelines require that the university develop, implement and maintain a written identity theft program. The purpose of the program is to detect patterns, practices and specific forms of activity that indicate the existence of identity theft and prevent a customer from using false identifying information to obtain goods, services or credit. In addition, identifying information maintained by the University must be protected to the greatest possible extent.

### Definitions

| Term | Definition |
|---|---|
| Customer | Employees, students, patients or any other individual who obtains goods or services on credit. |
| 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. |
| University Account | A continuing relationship established with the University to obtain goods, services or credit for any purpose that involves or is designed to permit multiple payments or transactions, including those through payroll deduction. Types of accounts include university-based student loans, accounts receivable, patient financial accounts, medical records, gift shop credit accounts, tuition payment plans, parking permits, health insurance plans, memberships, 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. |

## Policy Details

I. Policy Intent

A. The university will make reasonable efforts to detect, prevent and mitigate identity theft associated with a university account. In support of this effort, the university will develop, implement and maintain an Identity Theft Red Flags program.

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:

1. Guidelines 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: 9/1/2009
Revised:

I. Prevention

A. University employees are responsible for safeguarding identifying information in order to prevent identify theft from occurring.

II. Detection

A. University Account Establishment

1. For university accounts established in-person, photo identification must be verified. Acceptable forms of photo identification are outlined in the University Account Establishment Red Flags Guidelines.

2. For university accounts initiated online, other safeguards must be documented and implemented to check identity.
3. University Account Establishment Red Flags Guidelines must be applied to standard operating procedures and/or internal control structures in all units that establish university accounts.

B. Billing and Account Payments

1. University Billing and Account Payments Red Flags Guidelines must be applied to standard operating procedures and/or internal control structures in all units that perform billing and processing of payments against university accounts.

III. Reporting Identity Theft

A. Employees are required to immediately notify their supervisor if identify theft is suspected.

B. Supervisors are required to immediately report suspected or actual incidents of identity theft to the University Police.

C. Supervisors are required to report financial fraud resulting from identity theft to the Department of Internal Audit by following the Reporting and Investigating Financial Fraud policy.

## Responsibilities

| Position or Office | List of Responsibilities |
|---|---|
| Office of Business & Finance | 1) Coordinate and administer the program<br>2) Develop and maintain guidelines on methods to detect identity theft and the associated action steps to prevent and mitigate the fraud<br>3) Develop and maintain employee training and associated reporting<br>4) Periodically review and update the program<br>5) Provide annual report on the program effectiveness |
| Colleges, Vice Presidential units and Regional Campuses | 1) Review internal processes where goods, services or credit are provided to customers and implement the guidelines as necessary<br>2) Update internal control structure or standard operating procedures as appropriate to reflect university guidelines<br>3) Annually review internal processes, control structures and standard operating procedures for continued compliance with guidelines<br>4) Identity employees who must complete training and ensure that training is completed<br>5) Protect identifying information collected in accordance with the Institutional Data, Health Insurance Privacy, Credit Card and Privacy and Release of Student Education Records policies as well as any other privacy and security standards and requirements, including Payment Card Industry standards. Report proven or suspected disclosure or exposure of personal information in |

| | |
|---|---|
| | accordance with the Disclosure or Exposure of Personal Information policy.<br>6) Report financial fraud resulting from an identity theft in accordance with the Reporting and Investigating Financial Fraud policy.<br>7) Report suspected or actual identity theft to the University Police Department as deemed appropriate based on the circumstances. |
| Employees involved in affected business processes | 1) Follow documented internal processes<br>2) Complete training.<br>3) Report proven or suspected disclosure or exposure of personal information, financial fraud, suspected or actual identity theft to supervisor immediately |

## Resources

Accounts Receivable Policy

Credit Card Policy

Credit Card Merchant Policy Credit Card Handling Responsibilities and Procedures

Disclosure or Exposure of Personal Information policy

Fair and Accurate Credit Transactions Act of 2003

Health Insurance Privacy Policy

Identity Theft Red Flags Guidelines

Institutional Data Policy

Privacy and Release of Student Education Records

Reporting and Investigating Financial Fraud Policy

## Contacts

| Subject | Office | Telephone | E-mail/URL |
|---|---|---|---|
| Policy or guideline clarification | Office of Business & Finance | 292-7970 | **http://www.busfin.ohio-state.edu/** |
| Identity Theft Red Flags training | Office of Business & Finance | 292-7970 | **http://buckeyesecure.osu.edu/Policy/RedFlagsTraining** |

## History

Issued: 9/1/2009