
Policy Objective:
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.

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.

Explicit Policy Requirements: (Items for which non-compliance will result in a policy Exception):
The following items are explicitly defined in the policy and should be considered as policy requirements; items which if not followed, will result in policy “exceptions.”

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1     | The University will develop, implement and maintain an Identity Theft Red Flags program. At a minimum, the program will include:  
- Guidelines for identifying patterns, practices or specific activities that indicate the possible existence of an identity theft.  
- Identification of reasonable and appropriate action steps that will be taken when a pattern, practice or specific activity has been detected.  
- Processes for requiring that accounts accessed or managed by external vendors on behalf of the university have implemented an appropriate program.  
- Training to educate employees on the program.  
- Periodic review and updates to the program.  
- Annual program reporting to appropriate university leadership. |
<p>| 2     | Prevention – University employees are responsible for safeguarding identifying information in order to prevent identity theft from occurring. |
| 3     | Detection – For university accounts established in-person, photo identification must be verified. |
| 4     | For university accounts initiated online, other safeguards must be documented and implemented to check identity. |
| 5     | 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. |
| 6     | 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 |</p>
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Description</th>
<th>Page</th>
<th>Para</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Employees are required to immediately notify their supervisor if identity theft is suspected.</td>
<td>3</td>
<td>III.A.</td>
</tr>
<tr>
<td>8</td>
<td>Supervisors are required to immediately report suspected or actual incidents of identity theft to University Police.</td>
<td>3</td>
<td>III.B.</td>
</tr>
<tr>
<td>9</td>
<td>Supervisors are required to report financial fraud resulting from identity theft to the Department of Internal Audit by following the <a href="#">Reporting and Investigating Financial Fraud</a> policy.</td>
<td>3</td>
<td>III.C.</td>
</tr>
</tbody>
</table>
| 10    | College/VP Units & Regional Campus Responsibilities (Any area that provides credit services should have management complete the following activities – i.e., Student Health Services, Rec Sports, Ohio Union & Student Activities, Housing, Regional Operations, etc.)  
  o Review internal processes where goods, services, or credit are provided to customers and implement the guidelines as necessary.  
  o Update internal control structure or standard operating procedures as appropriate to reflect university guidelines.  
  o Annually review internal processes, control structures, and standard operating procedures for continued compliance with guidelines.  
  o Identify employees who must complete training and ensure that training is completed.  
  o 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.  
  o Report financial fraud resulting from an identity theft in accordance with the [Reporting and Investigating Financial Fraud](#) policy.  
  o Report suspected or actual identity theft to the University Police Department as deemed appropriate based on the circumstances. | 3    | Responsibilities |
|       | Employees involved in affected business processes responsibilities (Any individuals directly involved in the processing of credit card transaction – i.e., cashiers, etc.)  
  o Follow documented internal processes.  
  o Complete training.  
  o Report proven or suspected disclosure or exposure of personal information, financial fraud, suspected or actual identity theft to supervisor immediately. | 3    | Responsibilities |
Notes:
Click the following link to review the document.
Reporting and Investigating Financial Fraud
Alternatively, it may be found at http://www.osu.edu/policies/.

Summary of Potential Policy Exceptions:

- Employees are not immediately notifying their supervisor when identity theft is suspected.
- Supervisors are not immediately reporting suspected or actual incidents of identity theft to University Police.
- Supervisors are not reporting financial fraud resulting from identity theft to the Department of Internal Audit.
- College/VP units do not complete the responsibilities listed above.
- Employees are not safeguarding identifying information in order to prevent identity theft from occurring.
- For university accounts established in-person, photo identifications are not being verified.
- For university accounts initiated online, other safeguards are not documented and implemented to check identity.
- University Account Establishment Red Flags Guidelines are not applied to standard operating procedures and/or internal control structures in all units that establish university accounts.
- University Billing and Account Payments Red Flags Guidelines are not applied to standard operating procedures and/or internal control structures in all units that perform billing and processing of payments against university accounts.
- Employees involved in affected business process do not complete the responsibilities listed above.

Policy Areas of Potential Student Life Interpretations and/or Follow-up with Business & Finance:
The following items are potential areas of policy interpretation, left to the discretion of Student Life:

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Description</th>
<th>Page</th>
<th>Para</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>● What makes one suspect identity theft? Red flags may be found in the following link. <a href="#">Red Flag Guidelines</a></td>
<td>3</td>
<td>III.A.</td>
</tr>
<tr>
<td>2</td>
<td>● What safeguards must be documented and implemented to check identity for accounts initiated online?</td>
<td>3</td>
<td>II.A.2.</td>
</tr>
</tbody>
</table>

Areas of Consideration for Defining as “Reasonable” in the ICS:
- Efforts taken to detect, prevent and mitigate identity theft
Potential Training Topics:

- Institutional Data Policy
- Understand & Prevent Fraud
- Internal Controls
- Accounts Receivable
- Identity Theft Red Flags
- HIPAA
- FERPA
- Credit Card Merchant Policy
- Credit Card Handling Responsibilities and Procedures