Identity Theft Red Flags

University Policy

Applies to: Units that collect and maintain personal information for the purpose of allowing their customers to obtain goods, services, or credit

Responsible Office
Office of Business and Finance

POLICY

Issued: 09/01/2009
Revised: 01/07/2021 (minor revision)

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

Purpose of the Policy

To advance the detection of patterns, practices, and specific forms of activity that indicate the existence of identity theft; the prevention of customers using false identifying information to obtain goods, services, or credit; and the protection of identifying information maintained by the university to the greatest possible extent.

Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td>Employees, students, patients, or any other individual who obtains goods or services on credit.</td>
</tr>
<tr>
<td>Exception</td>
<td>Any violation of or noncompliance with a university policy issued by the Office of Business and Finance (Business and Finance).</td>
</tr>
<tr>
<td>Identifying information</td>
<td>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 and 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, other unique physical representation, or unique electronic identification number.</td>
</tr>
<tr>
<td>Identity theft</td>
<td>A fraud attempted or committed using the identifying information of another person without authority.</td>
</tr>
<tr>
<td>Red flag</td>
<td>A pattern, practice, or specific activity that indicates the possible existence of identity theft.</td>
</tr>
<tr>
<td>Unit</td>
<td>College or administrative unit.</td>
</tr>
<tr>
<td>University account</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Waiver</td>
<td>Permission granted to a unit to operate differently than specified or required by a university policy issued by Business and Finance.</td>
</tr>
</tbody>
</table>

Policy Details

I. Identity Theft Red Flags Program
   A. The university maintains an Identity Theft Red Flags program that is coordinated and administered by the Office of Business and Finance, which includes:
      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;
Identity Theft Red Flags

University Policy

Applies to: Units that collect and maintain personal information for the purpose of allowing their customers to obtain goods, services, or credit

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: 09/01/2009
Revised: 01/07/2021 (minor revision)

I. Prevention

A. University employees are responsible for safeguarding identifying information to prevent identity theft from occurring.

B. Units must:
   1. Review internal processes, control structures, and standard operating procedures annually for continued compliance with University Account Establishment Red Flags Guidelines and University Billing and Account Payments Red Flags Guidelines.
   2. Review internal processes when goods, services, or credit are provided to customers and implement the University Billing and Account Payments Red Flags Guidelines, as necessary.
   3. Identify employees who must complete training and ensure that training is completed.
   4. Protect identifying information collected in accordance with the Institutional Data policy, Payment Card Compliance policy, and Privacy and Release of Student Education Records policy as well as any other privacy and security standards and requirements, including Payment Card Industry standards.

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.

III. Billing and Account Payments

A. 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.

IV. Reporting Identity Theft

A. Employees must immediately notify their supervisor if identify theft is suspected.
B. Supervisors must immediately report suspected or actual incidents of identity theft to the University Police.
C. Supervisors must report financial fraud resulting from identity theft to the Department of Internal Audit by following the Reporting and Investigating Financial Fraud policy.
D. Units must report proven or suspected disclosure or exposure of personal information in accordance with the Information Security Incident Response Management policy.

V. Waivers to this policy must be approved in advance and documented by the Office of Business and Finance, using the Business and Finance University Policy Waiver Request.
Applies to: Units that collect and maintain personal information for the purpose of allowing their customers to obtain goods, services, or credit

VI. Policy Violations
   A. All policy violations must be tracked as an exception in accordance with the Fiscal Stewardship policy.
   B. The university may require successful completion of training.
   C. The university may enforce corrective action, up to and including termination, in accordance with applicable policies or rules.
   D. The university may seek restitution, as appropriate.
   E. Criminal charges may be filed, as appropriate.

Responsibilities

<table>
<thead>
<tr>
<th>Position or Office</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees involved in business processes</td>
<td>1. Follow documented internal processes.</td>
</tr>
<tr>
<td></td>
<td>2. Complete training.</td>
</tr>
<tr>
<td></td>
<td>3. Report proven or suspected disclosure or exposure of personal information, financial fraud, and suspected or actual identity theft to supervisor immediately.</td>
</tr>
<tr>
<td>Office of Business and Finance</td>
<td>1. Coordinate and administer the program.</td>
</tr>
<tr>
<td></td>
<td>2. Develop and maintain guidelines on methods to detect identity theft and the associated action steps to prevent and mitigate the fraud.</td>
</tr>
<tr>
<td></td>
<td>3. Develop and maintain employee training and associated reporting.</td>
</tr>
<tr>
<td></td>
<td>4. Periodically review and update the program.</td>
</tr>
<tr>
<td></td>
<td>5. Provide annual report on the program effectiveness.</td>
</tr>
<tr>
<td>Units</td>
<td>1. Review internal processes when goods, services, or credit are provided to customers and implement the guidelines, as necessary.</td>
</tr>
<tr>
<td></td>
<td>2. Update internal control structure or standard operating procedures as appropriate to reflect university guidelines.</td>
</tr>
<tr>
<td></td>
<td>3. Review internal processes, control structures, and standard operating procedures annually for continued compliance with guidelines.</td>
</tr>
<tr>
<td></td>
<td>4. Identify employees who must complete training and ensure that training is completed.</td>
</tr>
<tr>
<td></td>
<td>5. Protect identifying information collected in accordance with the Institutional Data policy, Payment Card Compliance policy, and Privacy and Release of Student Education Records policy as well as any other privacy and security standards and requirements, including Payment Card Industry standards.</td>
</tr>
<tr>
<td></td>
<td>6. Report proven or suspected disclosure or exposure of personal information in accordance with the Information Security Incident Response Management policy.</td>
</tr>
<tr>
<td></td>
<td>7. Report financial fraud resulting from an identity theft in accordance with the Reporting and Investigating Financial Fraud policy.</td>
</tr>
<tr>
<td></td>
<td>8. Report suspected or actual identity theft to University Police immediately.</td>
</tr>
</tbody>
</table>

Resources

University Policies, policies.osu.edu
   Accounts Receivable, go.osu.edu/accounts-receivable-policy
   Fiscal Stewardship, go.osu.edu/fiscal-stewardship-policy
   Information Security Incident Response Management, go.osu.edu/infosec-irismp
   Institutional Data, go.osu.edu/idp
   Payment Card Compliance, go.osu.edu/payment-card-compliance-policy
   Privacy and Release of Student Education Records, go.osu.edu/prser-policy
   Reporting and Investigating Financial Fraud, go.osu.edu/financial-fraud-policy

Training
   Identity Theft Red Flags, busfin.osu.edu/financial-training

Additional Guidance
   Business and Finance University Policy Waiver Request,
   docs:sign.net/Member/PowerFormSigning.aspx?PowerFormId=fd68959a-4af8-48bb-a0ae-
   67521b9d821&env=na1&acct=387d1013-fb1c-4705-9bd9-7cf575f484ce&v=2
Applies to: Units that collect and maintain personal information for the purpose of allowing their customers to obtain goods, services, or credit

Identity Theft Red Flags Guidelines, busfin.osu.edu/bursar/more/compliance
PCI Compliance, busfin.osu.edu/treasurer/pci-compliance
University Account Establishment Red Flags Guidelines, busfin.osu.edu/bursar/more/compliance
University Billing and Account Payments Red Flags Guidelines, busfin.osu.edu/bursar/more/compliance

Contacts

<table>
<thead>
<tr>
<th>Subject</th>
<th>Office</th>
<th>Telephone</th>
<th>E-mail/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy questions</td>
<td>Financial Services, Office of Business and Finance</td>
<td>614-292-6261</td>
<td>busfin.osu.edu/bursar/identity-theft-red-flags</td>
</tr>
</tbody>
</table>

History

Issued: 09/01/2009
Edited: 09/04/2018
Edited: 06/01/2019 Number removed from title
Edited: 09/04/2019 Disclosure or Exposure of Personal Information policy title updated to Information Security Incident Response Management policy
Revised: 01/07/2021 Minor revision