Austin Peay State University

Identity Theft Prevention

POLICIES

Issued: March 25, 2017
Responsible Official: Vice President for Finance and Administration
Responsible Office: Information Technology

Policy Statement

It is the policy of Austin Peay State University to make reasonable efforts to detect, prevent, and mitigate identity theft.

Purpose

The purpose of this policy is to enact an effort to detect, prevent, and mitigate identify theft, and to help protect the University, faculty, staff, students, and other applicable constituents from damages related to loss or misuse of identifying information due to identity theft.

Contents

Definitions

Covered account Any account that involves or is designated to permit multiple payments or transactions; or any other account maintained by the

	University for which there is reasonably foreseeable risk of identity theft to students, faculty, staff or other applicable constituents, or for which there is a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.
Identifying Information	Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer Internet Protocol address or routing code, credit card number or other credit card information.
Identity Theft	A fraud committed or attempted using the identifying information of another person without authority.
Red Flag	Pattern, practice or specific activity that indicates the possible existence of identity theft.

Procedures

Background

A. The risk to the University, its faculty, staff, students, and other applicable constituents 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.

B. Under this policy the program will:
   1. Identify patterns, practices or specific activities ("red flags") that could indicate the existence of identity theft with regard to new or existing covered accounts (see Definitions);
   2. Detect red flags that are incorporated in the program;
   3. Respond appropriately to any red flags that are detected under this program to prevent and mitigate identity theft;
   4. Ensure periodic updating of the program, including reviewing the accounts that are covered and the identified red flags that are part of this program; and,
   5. Promote compliance with state and federal laws and regulations regarding identity theft protection.

C. The program shall, as appropriate incorporate existing University policies and guidelines such as anti-fraud programs and information security programs that establish controls for reasonably foreseeable risks.

Identification of Red Flags

A. The following examples of red flags are potential indicators of fraud or identity theft. The risk factors for identifying relevant red flags include the types of covered accounts offered or maintained; the methods provided to open or access covered accounts; and, previous experience with identity theft. Any time a red flag or a situation closely resembling a red flag is apparent, it should be investigated for verification.

B. Alerts, notifications or warnings from a credit or consumer reporting agency. Examples of these red flags include the following:
   1. A report of fraud or active duty alert in a credit or consumer report:
   2. A notice of credit freeze from a credit or consumer reporting agency in response to a request for a credit or consumer report;
   3. A notice of address discrepancy in response to a credit or consumer report request; and,
   4. A credit or consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant such as:
      a. A recent and significant increase in the volume of inquiries;
      b. An unusual number of recently established credit relationships;
      c. A material change in the use of credit, especially with respect to recently established credit relationships; or,
      d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

C. Suspicious documents. Examples of these red flags include the following:
   1. Documents provided for identification that appears to have been altered, forged or are inauthentic.
   2. The photograph or physical description on the identification document is not consistent with the appearance of the individual presenting the identification.
   3. Other information on the identification is not consistent with information provided by the person opening a new

covered account or individual presenting the identification.

4. Other information on the identification is not consistent with readily accessible information that is on file with the University, such as a signature card or a recent check.
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

D. Suspicious personal identifying information. Examples of these red flags include the following:
   1. Personal identifying information provided is inconsistent when compared against other sources of information used by the University. For example:
      a. The address does not match any address in the consumer report; or,
      b. The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.
   2. Personal identifying information provided by the individual is not consistent with other personal identifying information provided by that individual. For example:
      a. There is a lack of correlation between the SSN range and date of birth.
   3. Personal identifying information provided is associated with known fraudulent activity. For example:
      a. The address on an application is the same as the address provided on a fraudulent application; or,
      b. The phone number on an application is the same as the number provided on a fraudulent application.
   4. Personal identifying information provided is of a type commonly associated with fraudulent activity. For example:
      a. The address on an application is fictitious, a mail drop, or a prison; or
      b. The phone number is invalid or is associated with a pager or answering service.
   5. The social security number provided is the same as that submitted by another person opening an account.
   6. The address or telephone number provided is the same as or similar to the address or telephone number submitted by that of another person.
   7. 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.

8. Personal identifying information provided is not consistent with personal identifying information that is on file with the University.
9. When using security questions (mother's maiden name, pet's name, etc.), the person opening that covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

E. Unusual use of, or suspicious activity related to, the covered account. Examples of these red flags include the following:
   1. Shortly following the notice of a change of address for a covered account, the University receives a request for a new, additional, or replacement card, or for the addition of authorized users on the account.
   2. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
      a. Nonpayment when there is no history of late or missed payments;
      b. A material change in purchasing or usage patterns.
   3. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
   4. Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the individual's covered account.
   5. The University is notified that the individual is not receiving paper account statements.
   6. The University is notified of unauthorized charges or transactions in connection with an individual's covered account.
   7. The University receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the university.
   8. The University is notified by an employee or student, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
   9. A breach is the University's computer security system.

Detecting Red Flags

A. Student enrollment. In order to detect red flags associated with enrollment of a student, the University will take the

following steps to obtain and verify the identity of the individual opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and,
2. Verify the student's identity at the time of issuance of the student identification card through review of driver's license or other government-issued photo identification.

B. Existing accounts. In order to detect red flags associated with an existing account, the University will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information;
2. Verify the validity of requests to change billing addresses by mail or email, and provide the student a reasonable means of promptly reporting incorrect billing address changes; and,
3. Verify changes in banking information given for billing and payment purposes.

C. Consumer/Credit Report Requests. In order to detect red flags for an employment or volunteer position for which a credit or background report is sought, the University will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

Responding to Red Flags

A. Once a red flag or potential red flag is detected, the University must act quickly with consideration of the risk posed by the red flag.

B. The University should quickly gather all related documentation, write a description of the situation and present this information to the Program Administrator for determination.

C. The Program Administrator will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

D. The University may take the following steps as is deemed appropriate:
   1. Continue to monitor the covered account for evidence of identity theft;
   2. Contact the student or applicant for which a credit report was run:
   3. Change any passwords or other security devices that permit access to covered accounts;
   4. Close and reopen the account;
   5. Determine not to open a new covered account;
   6. Provide the student with a new student identification number;
   7. Notify law enforcement;
   8. Determine that ne response is warranted under the particular circumstances;
   9. Cancel the transaction.

Links

APSU Theft or Loss of Data http://www.apsu.edu/information-technology/theft-or-loss-data

Revision Dates

APSU Policy 4:031 (previously 4:034) – Rev.: March 25, 2017
APSU Policy 4:031 – Rev.: September 14, 2015
APSU Policy 4:031 – Rev.: January 28, 2011
APSU Policy 4:031 – Issued: December 1, 2005

Subject Areas:

Academic	Finance	General	Human Resources	Information Technology	Student Affairs
				☑	

Approved

President: signature on file