

IDENTITY THEFT PREVENTION PROGRAM

Purpose

In late 2007 the Federal Trade Commission implemented regulations requiring financial institutions and other creditors to develop policies and procedures to identify detect and respond appropriately to Red Flags of identity theft. The regulations also require users of consumer reports to develop policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report when the user receives a notice of address discrepancy. In addition, identity theft has become prevalent in today's society, and poses significant risk to consumers, including students of Fort Hays State University. Therefore, Fort Hays State University hereby implements this program in order to comply with applicable regulations, to protect students and other consumers of FHSU's services from identity theft, and to mitigate the effects of such when it does occur.

Policy and Procedures Regarding Identity Theft

Definitions

"Identity Theft" is a fraudulent or attempted use of identifying information of another person without such person's authority.

A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

"Covered Account" means all student accounts or loans administered by FHSU that involve or are designed to permit multiple payments or transactions, and accounts for business, personal, family and household purposes for which there is a reasonably foreseeable risk of identity theft. For purposes of this program, examples of covered accounts maintained or offered by FHSU include but are not limited to:

- Student tuition and fee payment plans;
- Housing payment plans (room and board, including meal plans);
- Financial Assistance programs and repayment plans associated therewith, when applicable;
- The Federal Perkins Loans;
- FHSU Institutional Loans, and;
- Student Health Center fees.

"Consumer" as used herein means the holder of a covered account or a person on whom a consumer report has been sought.

Identifying Red Flags

In identifying Red Flags on covered accounts, FHSU will take the following into consideration:

- The type of covered accounts it maintains as identified above and the nature of regular and ordinary transactions on those accounts;
- The level of access by the account holder to the account, and;
- Any specific reports of or recent history involving identify theft in connection with FHSU students, faculty, staff, or other consumers.

Examples of Red Flags

- Alerts, notifications or warnings from a consumer reporting agency including a fraud alert in connection with a consumer report;
- A notice of address discrepancy received from a consumer reporting agency;
- A consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity on that account;
- Suspicious documents including: documents used for identification that appear to have been altered or forged; and photographs or physical descriptions on an identification that are inconsistent with the appearance of the applicant or customer presenting the identification, or other inconsistent information on the identification;
- Suspicious personal identifying information including: personal identifying information provided by the customer not consistent with other personal identifying information; personal identifying information that is of the type commonly associated with fraudulent activity as indicated by internal or third-party sources, such as a fictitious address or a social security number that matches a social security number provided by another customer; and personal identifying information that is not consistent with other information on file with FHSU;
- Unusual or suspicious activity related to the covered account, including but not limited to notice to FHSU that a student is not receiving mail sent by FHSU, a breach of FHSU's computer system security, and unauthorized access to or use of student account information, and;
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identify theft in connection with covered accounts held by FHSU.

Detecting Red Flags

In order to attempt to detect Red Flags, FHSU will obtain identifying information about the person opening a covered account and attempt to verify such person's identity to the extent reasonable and possible, by comparing the information received with other information on the same person maintained by FHSU. In addition, FHSU may take one or more of the following actions to detect Red Flags:

- Require certain identifying information such as name, date of birth, academic records, home address or other identification, including verification of student's identity through photo identification for issuance of the student identification card (Tiger Card);
- Verify identification of students if they request information or changes in banking information given for billing and payment purposes;
- Require written verification that an address is accurate at the time the credit report request is made to the consumer reporting agency, and in the event there is an address discrepancy, verify that the report pertains to the applicant for whom the report was requested;
- Monitor account when specific activity on that activity occurs.

Responding to Red Flags

When FHSU has detected a possible Red Flag associated with a covered account, the administrator of the Program may take one or more of the following actions:

- Contact the customer to verify inconsistent information or to verify recent activity on the account;
- Monitor the covered account for unusual or suspicious activity;
- Change any password, security code or other security device that permit access to a covered account;
- Close an existing covered account;
- Notify law enforcement when circumstances indicate possible criminal activity;
- Determine that no particular response is warranted under the circumstances presented; and
- Post a notification to the campus community of the suspected incident involving identity theft on the University's Police Department website.

Updating the Program

FHSU will review the program periodically, and no less than once per year, to determine whether updates and modifications are needed based upon experience with identifying and responding to Red Flags. Also, the program will be reviewed and updated if FHSU becomes aware of changes in methods of committing, preventing and/or detecting identity theft. Finally, changes in the type or nature of accounts that FHSU maintains and particular business arrangements of FHSU may require an update to the program.

Administering the Program

This program has been approved by the President's Cabinet on the date indicated at the end of this document. Oversight for the program is delegated to the Vice President for Administration and Finance or designee. The Vice President for Administration and Finance or designee will review reports prepared by staff regarding any particular circumstances throughout the year when Red Flags were detected, and shall recommend and implement updates and changes to the program as needed.

Oversight of Service Provider Relationships

The Vice President for Administration and Finance or designee shall also be responsible for oversight of service provider arrangements, making sure that financial institutions or creditors engaged by FHSU to perform an activity in connection with one or more covered accounts are complying with applicable regulations relating to Red Flags for identity theft and address discrepancies (example: FHSU's vendor for student banking services). The person responsible for such oversight on FHSU's behalf will at a minimum contact the vendor to discuss the vendor's policies and practices pursuant to the Red Flags rules, and will periodically review the vendor's reports of detected Red Flags on accounts relating to the University, and will examine the vendor's response thereto.

Address Discrepancies

A notice of address discrepancy means a notice sent to FHSU by a consumer reporting agency, that informs FHSU of a substantial difference between the address provided to request a consumer report for the person for whom the consumer report was requested and the address in the vendor's file for such person.

Action Steps When a Notice of Address Discrepancy is Received

FHSU will take one or more of the following actions to enable it to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report when a notice of address discrepancy is received:

- Compare the information in the report with the information FHSU maintains in its own records;
- Verify the information in the report by contacting the person on whom the report was made.

Action Steps When an Address has been Found to be Accurate

When FHSU has reasonably confirmed an address for the consumer is accurate, FHSU will furnish such address to the consumer reporting agency as part of the information that FHSU regularly furnishes the next time it provides information. When FHSU has confirmed an address for a consumer after receiving a notice of an address discrepancy, it will provide the confirmed address to the vendor the next time FHSU provides information to the vendor.

Action Steps When an Address cannot be Verified

If FHSU receives notice of an address discrepancy in connection with one of its covered accounts as defined above, it will follow the policies and procedures relating to Red Flags for identity theft. FHSU will inform such person that the address provided by the consumer reporting agency is inconsistent with the address provided by the person or maintained by FHSU, and through this policy advises such persons to take appropriate steps to guard their identity and mitigate any possible harm that has been or could be caused as a result of identity theft.

Adopted by President's Cabinet 06/17/09