Procedures for Identifying and Responding to Red Flags for Identity Theft Prevention

The following general guidelines provide direction for identifying and responding to "Red Flags" in accordance with the SFASU Security and Identity Theft Prevention Program found in HOP 14.4.

All SFASU areas, departments, colleges and schools that hold personally identifiable student financial records and information and/or covered accounts (see HOP 14.4) must comply with the requirements of this procedure.

The detailed program, including specific responsibilities and procedures is found in HOP 14.4.

Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility that identity theft may occur. All SFASU departments must follow these guidelines and report their actions to the program officer if identity theft is suspected. Additionally, all SFASU departments must annually report their risk assessment via the linked form.

1. Alerts, notifications or warnings from consumer reporting agencies

Red Flag	Required Response/Action
A fraud or active duty alert accompanies a consumer report requested by SFASU.	1. Verify activity reported with applicant. 2. If verified, proceed with evaluation of applicant based on consumer report received. 3. If unable to verify, do not use this report in evaluating applicant.
A notice of a credit freeze is received in response to a request for a consumer report.	1. Verify activity reported with applicant. 2. If verified, proceed with evaluation of applicant based on consumer report received. 3. If unable to verify, do not use this report in evaluating applicant.
A notice of address discrepancy is received in response to a request for a consumer report.	1. Compare reported address with that provided by applicant and if necessary, contact the applicant to verify. 2. If address has been verified, report to consumer report agency. 3. If unable to determine relationship between the applicant and the notice, do not use the report to evaluate the applicant and notify the applicant.
Indication from a consumer report of a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or consumer.	1. Verify activity reported with applicant. 2. If verified, proceed with evaluation of applicant based on consumer report received.

	3. If unable to verify, do not use this report in evaluating applicant.

2. Suspicious documents

Red Flag	Required Response/Action
Identification documents or card provided appears to have been altered or forged.	1. Retain identification and notify management for assistance. 2. If identification appears fraudulent, report using the EthicsPoint reporting system.
Identification documents or card provided on which the photograph or physical description is not consistent with the appearance of the customer presenting the documents.	1. Retain identification, notify management for assistance. 2. If identification appears fraudulent, report using the EthicsPoint reporting system.
Identification documents or card provided on which other identifying information is not consistent with information provided by the customer or other readily accessible information that is on file. For example, a birth date doesn't match appearance of customer.	1. Retain identification, notify management for assistance. 2. If identification appears fraudulent, report using the EthicsPoint reporting system.
Request for information, applications, or other documents presented appear to have been altered or forged, or gives the appearance of having been destroyed and reassembled.	1. Retain documents, notify management for assistance. 2. If documents appear fraudulent, report using the EthicsPoint reporting system.

3. Suspicious personal identifying information

Red Flag	Required Response/Action
Identifying information is inconsistent with other external information sources. For example, an address that does not match the address printed on a loan application.	1. Inspect identification and compare with other external information sources. 2. Retain identification and notify management for assistance. 3. If information appears fraudulent, report using the EthicsPoint reporting system.
Identifying information is inconsistent with other information provided by the customer. For example, inconsistent birth dates.	1. Inspect identification and compare with Banner Student Identification forms, such as SPAPERS or SPAIDEN. 2. Retain identification and notify management for assistance. 3. If information appears fraudulent, report using the EthicsPoint reporting system.

Identifying information is associated with known fraudulent activity. For example, an address or phone number being used is also known to be associated with a fraudulent application.	1. Inspect identification and compare with documentation indicating fraudulent activity. 2. Retain identification and notify management for assistance. 3. If information appears fraudulent, report using the EthicsPoint reporting system.
Identifying information is of the type commonly associated with fraudulent activity. For example, an address is fictitious or the phone number is invalid.	1. Inspect identifying information. 2. Retain identifying information and notify management for assistance. 3. If information appears fraudulent, report using the EthicsPoint reporting system.
Social Security (SSN) or Banner ID number is the same as that submitted by another customer.	1. Inspect identifying information. 2. Retain document provided, request to see student's SSN card, Banner ID or driver's license card and retain a copy if discrepancy if not resolved. 3. Do not provide any services until identity proven. Place hold on original customer who provided the duplicate ID number if identity is proven. Notify management for assistance. 4. If information appears fraudulent, report using the EthicsPoint reporting system.
Address or phone number is the same as that presented by an unusually large number of other customers.	1. Request and inspect identifying documents to confirm information provided. 2. If information appears fraudulent, report using the EthicsPoint reporting system.
A customer fails to provide all of the required personal identifying information on an application or in response to notification that the application is incomplete.	1. Do not provide any services or award aid until application is complete. 2. If fraudulent, report using the EthicsPoint reporting system.
Identifying information is inconsistent with internal information sources on file.	1. Inspect identifying information. 2. Retain identifying information and notify management for assistance. 3. If information appears fraudulent, report using the EthicsPoint reporting system.
Customer cannot provide information in response to challenge questions beyond that which generally would be available from a wallet or consumer report.	1. Do not provide any services, do not reset PIN's. 2. If situation appears fraudulent, report using the EthicsPoint reporting system.

4. Unusual use of or suspicious activity related to covered accounts

Red Flag	Required Response/Action
Change of address for an account that is followed shortly by a request for a name change.	1. Request official documentation reflecting name change (court order, marriage certificate, etc.) and compare with photo identification. 2. Verify change of address previously submitted. 3. If situation appears fraudulent, report using the EthicsPoint reporting system.
An account is used in a manner inconsistent with established patterns of activity on that account. For example, payments are no longer made on an otherwise consistently up-to-date account.	1. Banner automatically places financial hold and restricts any services from being provided until the hold has been removed by the Student Business Services office. 2. If situation appears fraudulent, report using the EthicsPoint reporting system.
Mail sent to customer is returned repeatedly although transactions continue to be conducted.	1. Attempt to contact student by using: Contact information in Banner Student Identification screen (SPAIDEN); email address in Banner Email Address Form (GOAEMAL); phone number in Banner Telephone form (SPATELE). 2. If situation appears fraudulent, report using the EthicsPoint reporting system.
Customer notifies SFASU — via phone, e-mail or in-person — that the customer is not receiving mail.	1. Verify address information with customer and ensure listed addresses are active. 2. If address on file was not entered by customer, notify management for assistance. 3. If situation appears fraudulent, report using the EthicsPoint reporting system.
Customer notifies SFASU — via phone, e-mail or in-person — that an account has unauthorized activity.	1. Notify management for assistance and investigation. 2. If situation appears fraudulent, report using the EthicsPoint reporting system.
Customer notifies SFASU — via phone, e-mail or in-person — that unauthorized use of MySFA has occurred based on last logon date posted. For example, they did not attempt access during the time/date indicated on the date stamp.	1. Request photo identification from the customer to verify identity. 2. Reset MySFA password. 3. If situation appears fraudulent, report using the EthicsPoint reporting system .
Customer notifies SFASU — via phone, e-mail or in-person — that unauthorized use of	1. Request photo identification from the customer to verify identity.

MySFA has occurred. For example, the customer was automatically logged off during an online session due to multiple log on attempts.	2. Reset MySFA password. 3. If situation appears fraudulent, report using the EthicsPoint reporting system.

5. Notice from customers, victims of identity theft, law enforcement or others regarding possible identity theft

Red Flag	Required Response/Action
Customer notifies SFASU — via phone, e-mail or in-person — that an account has been opened fraudulently or is being maintained by SFASU for a person engaged in identity theft.	1. Notify management for assistance. 2. Place a financial hold on the account and contact UPD to request officer assistance. 3. If situation appears fraudulent, report using the EthicsPoint reporting system.
Customer reports — via phone, e-mail or in-person — receiving a bill for another individual or for a service that the customer denies receiving.	1. Notify management for assistance and investigation. 2. If situation appears fraudulent, report using the EthicsPoint reporting system.
Customer reports — via phone, e-mail or in-person — their personal information has been compromised.	1. Notify management for assistance and investigation. 2. Place a comment on appropriate Banner screen (TGACOMC, SPACMNT, RHACOMM, etc.). 3. If situation appears fraudulent, report using the EthicsPoint reporting system.

6. Other

Red Flag	Required Response/Action
Customer reports — via phone, e-mail or in-person — that an unauthorized change has occurred to direct deposit information stored on the Banner Direct Deposit screen (GXADIRD).	1. Notify management and inactivate direct deposit entry. 2. If situation appears fraudulent, report using the EthicsPoint reporting system.
Customer reports — via phone, e-mail or in-person — than an unauthorized change has occurred to the student address information on Banner Address screen (TUIADDR).	1. Notify management and inactivate address entry. 2. If situation appears fraudulent, report using the EthicsPoint reporting system.