# IDENTITY THEFT RED FLAGS GUIDELINES

| UNIVERSITY BILLING, ACCOUNT PAYMENTS & ACCOUNT CLOSURE | | | | |
|---|---|---|---|---|
| Payment on an account or closure of an account as defined in the Identity Theft Red Flags policy. Examples include missing account statements, unauthorized transactions, suspicious address or phone changes by the customer, etc. | | | | |
| Red Flag ID # | Description of Red Flag | Examples of Detection Mechanisms* | Employee Action Steps | Supervisor Action Steps |
| 1 | Fraud alert is included with a consumer report | | Not applicable | Not applicable |
| 2 | Notice of a credit freeze in response to a request for a consumer report | | Not applicable | Not applicable |
| 3 | Consumer reporting agency provides a notice of address discrepancy | | Not applicable | Not applicable |
| 4 | Unusual credit activity, such as an increased number of accounts or inquiries | | Not applicable | Not applicable |
| 5 | Document provided for identification appears to be altered or forged | | Not applicable | Not applicable |
| 6 | Photograph on identification is inconsistent with the appearance of the customer | | Not applicable | Not applicable |
| 7 | Information on identification is inconsistent with information provided by the person opening the account | | Not applicable | Not applicable |
| 8 | Information on identification (such as signature) is inconsistent with existing information on file | | Not applicable | Not applicable |
| 9 | Application appears to be forged, altered or destroyed and reassembled | | Not applicable | Not applicable |
| 10A | Information on identification does not match the address in a | | Not applicable | Not applicable |

| | | | | |
|---|---|---|---|---|
| | consumer report or existing system or application | | | |
| 10B | Social security number provided by customer has not been issued or appears on the Social Security Administrator's Death Master File | | Not applicable | Not applicable |
| 11 | Range in the social security number does not correlate to the date of birth | | Not applicable | Not applicable |
| 12 | Personal identifying information has been associated with known fraud activity | | Not applicable | Not applicable |
| 13 | Suspicious address is supplied, such as a mail drop or prison or phone numbers associated with pagers or answering service | • Payment sent by mail statement indicates suspicious change of address or phone number | 1) Call the customer to verify change<br>2) If the change is valid, proceed with change<br>3) If the change appears to be suspicious report the incident to supervisor | 1) Collect and retain any documents for potential evidence<br>2) Report the incident to University Police as appropriate<br>3) Report any financial fraud per the Financial Fraud Reporting Policy |
| 14 | Social security number provided matches that submitted by another person opening an account or other customers | | Not applicable | Not applicable |
| 15 | An address or phone number matching that supplied by a large number of applicants | | Not applicable | Not applicable |
| 16 | Person opening the account is unable to supply identifying information in response to notification that an application is incomplete | | Not applicable | Not applicable |
| 17 | Personal information is inconsistent with information already on file | | Not applicable | Not applicable |
| 18 | Person opening an account or customer is unable to correctly answer challenge questions | | Not applicable | Not applicable |

| | | | | |
|---|---|---|---|---|
| 19 | Shortly after change of address is received, receive request for additional users of the account | | Not applicable | Not applicable |
| 20 | Most of the available credit is used for cash advances, jewelry or electronics and/or customer fails to make first payment | • First payment is missed on account | 1) If first payment is missed, review the application to verify that the account is not fraudulent<br>2) If the application detects fraudulent activity and report the incident to supervisor | 1) Collect and retain any documents for potential evidence<br>2) Report the incident to University Police as appropriate<br>3) Report any financial fraud per the Financial Fraud Reporting Policy |
| 21 | Drastic changes in payment patterns, use of available credit or spending patterns | | Not applicable | Not applicable |
| 22 | An account that has been inactive for a lengthy time suddenly exhibits unusual activity | | Not applicable | Not applicable |
| 23 | Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account | | 1) Call the customer to verify address<br>2) If the change is valid, proceed with change<br>3) If the change appears to be suspicious report the incident to supervisor | 1) Collect and retain any documents for potential evidence<br>2) Report the incident to University Police as appropriate<br>3) Report any financial fraud per the Financial Fraud Reporting policy |
| 24 | Customer indicates that they are not receiving paper account statements | • Customer did not receive their statement | 1) Verify address with customer<br>2) If the customer states that the address on file is incorrect, then verify the customer's personal identification and obtain correct address from customer. If information cannot be verified report the incident to supervisor.<br>3) If the customer states that the address on file is correct refer the customer to the US Postal Service for further investigation | 1) Collect and retain any documents for potential evidence<br>2) If the customer cannot produce verifying information, report the incident to University Policy as appropriate<br>3) Report any financial fraud per the Financial Fraud Reporting policy |
| 25 | Customer notifies that there are unauthorized charges or transactions on customer's account | • Upon receiving their statement, the customer notices unauthorized charges or transactions | 1) Review statement transactions with customer in order to verify that the transactions were fraudulent<br>2) If the employee believes the | 1) Collect and retain any documents for potential evidence<br>2) Report the incident to University Police as appropriate<br>3) Report any financial fraud per the |

| | | | | |
|---|---|---|---|---|
| | | | transaction to be fraudulent, employee reports the incident to supervisor | Financial Fraud Reporting policy |
| 26 | Institution notified that it is has opened a fraudulent account for a person engaged in identity theft | | 1) Review statement transactions with customer in order to verify that the transactions were fraudulent<br>2) If the transaction appears to be fraudulent, report the incident to supervisor | 1) Collect and retain any documents for potential evidence<br>2) Report the incident to University Police as appropriate<br>3) Report any financial fraud per the Financial Fraud Reporting policy |
| 27 | Other | | 1) If the transaction appears to be fraudulent, report the incident to supervisor | 1) Collect and retain any documents for potential evidence<br>2) Report the incident to University Police as appropriate<br>3) Report any financial fraud per the Financial Fraud Reporting policy |