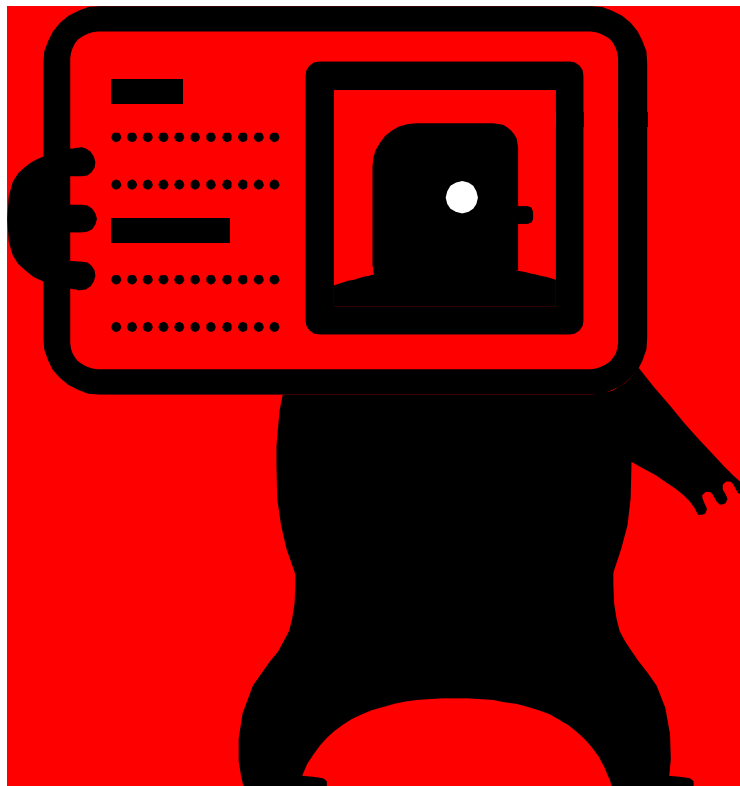




# RED FLAG TRAINING

IDENTITY THEFT PREVENTION PROGRAM



## Contents

Welcome .....	3
Overview .....	4
Definitions .....	5
Red Flags .....	6
Red Flag 1 – Alerts, Notifications or Warnings from a Consumer Reporting Agency .....	7
Red Flag 2 – Suspicious Documents .....	8
Red Flag 3 – Suspicious Personal Identifying Information .....	9
Red Flag 4 – Unusual Use of, or Suspicious Activity Related to, the Covered Account .....	10
Red Flag 5 – 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 Financial Institution or Creditor .....	11
Identity Theft Follow-up Procedures: .....	12
<b>Summary</b> .....	13

## Welcome

As many as nine million Americans have their identities stolen each year. Identity thieves may drain their accounts, damage their credit, and even endanger their medical treatment. The cost to businesses – left with unpaid bills racked up by scam artists – can be staggering, too.

The “Red Flags” Rule, in effect since January 1, 2008, requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate the damage it inflicts. By identifying red flags in advance, we will be better equipped to spot suspicious patterns when they arise and take steps to prevent a red flag from escalating into a costly episode of identity theft. The Red Flags Rule is enforced by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration.

This training program will grow and change as the University community share information with one another. The scenario used in the program is an exaggerated fabrication to allow multiple red flags to be identified. Not all of the red flags discussed in the training will be applicable to your department. Use the information contained in the training program to identify areas of concern that do relate to your department. Let us know of situations or specific challenges that your department faces so that we can address those issues in future publications and trainings.

## Overview

The Red Flags Rule sets out how we must develop, implement, and administer our Identity Theft Prevention Program. Our Program must include four basic elements, which together create a framework to address the threat of identity theft.

**First**, our Program must include reasonable policies and procedures to identify the “red flags” of identity theft we may run across in the day-to-day operation of the University. Red flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft. For example, if a customer has to provide some form of identification to open an account with the University, an ID that looks like it might be fake would be a “red flag”.

**Second**, our Program must be designed to detect the red flags we have identified. For example, if we have identified fake IDs as a red flag, we must have procedures in place to detect possible fake, forged, or altered identification.

**Third**, our Program must spell out appropriate actions you will take when you detect red flags.

**Fourth**, because identity theft is an ever-changing threat, the University must address how Finance and Administration will reevaluate our Program periodically to reflect new risks from this crime.

### **How does the Red Flags Rule fit in with the data security measures we are already taking?**

Preventing identity theft requires a 360° approach. Data security plays an essential role in keeping people’s sensitive information from falling into the wrong hands. Protect what you have a legitimate business reason to keep and securely dispose of what you no longer need. Even with appropriate data security measures in place, thieves are resourceful and still may find ways to steal information and use it to open or access accounts. That hurts individual identity theft victims, who may have to spend hundreds of dollars and many days, months or even years repairing damage to their good name and credit record. It also hurts our bottom line. Identity thieves run up huge bills with no intention of paying – leaving us with accounts receivable we will never be able to collect.

The Red Flag Rule picks up where data security leaves off. It seeks to prevent identity theft by ensuring that the University is on the lookout for the signs that a thief is using someone else’s information, typically to get products or services with no intention of paying. That is why it is important to fight the battle against identity theft on two fronts: First, by implementing data security practices that make it harder for thieves to get access to the personal information they use to open or access accounts, and second, by paying attention to the red flags that suggest that fraud may be afoot.

## Definitions

**Account** - a continuing relationship established by a person with the University to obtain a product or service for personal, family, household or business purposes. Account includes:

- A. An extension of credit, such as the purchase of property or services involving a deferred payment; and
- B. A deposit account.

**Card Issuer** – a financial institution or creditor that issues a debit or credit card.

**Consumer Reporting Agency** - are entities that collect and disseminate information about consumers to be used for credit evaluation and certain other purposes.

**Consumer Reports** – any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for—

- A. Credit or insurance to be used primarily for personal, family, or household purposes;
- B. Employment purposes; or
- C. Any other purpose authorized under US Code: Title 15, 1681b.

**Covered Accounts** -

- A. Any account the University offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions.
- B. Any other account the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from identity theft.

**Creditor** – an entity that regularly extends, renews, or continues credit.

**Customer** – person that has a covered account with the University.

**Mitigate** - to make something less harsh, severe, or violent.

**Notice of Address Discrepancy** - a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

**Identity Theft** - a fraud committed or attempted using the identifying information of another person without authority.

**Red Flag** - a pattern, practice, or specific activity that indicates the possible existence of identity theft.

**Service Provider** - a person that provides a service directly to the University.






## Red Flags

What are “red flags”? They are the potential patterns, practices, or specific activities indicating the possibility of identity theft. Although there is no one-size-fits-all approach, consider:

**Risk Factors** Different types of accounts pose different types of risk. For example, red flags for deposit accounts may differ from red flags for credit accounts. Similarly, the red flags for consumer accounts may not be the same as those for business accounts. Red flags for accounts opened or accessed online or by phone may differ from those involving face-to-face contact. Therefore, in identifying the relevant red flags, consider the types of accounts offered or maintained; the methods used to open covered accounts; methods used to access those accounts; and what you have learned about identity theft in the course of daily business.

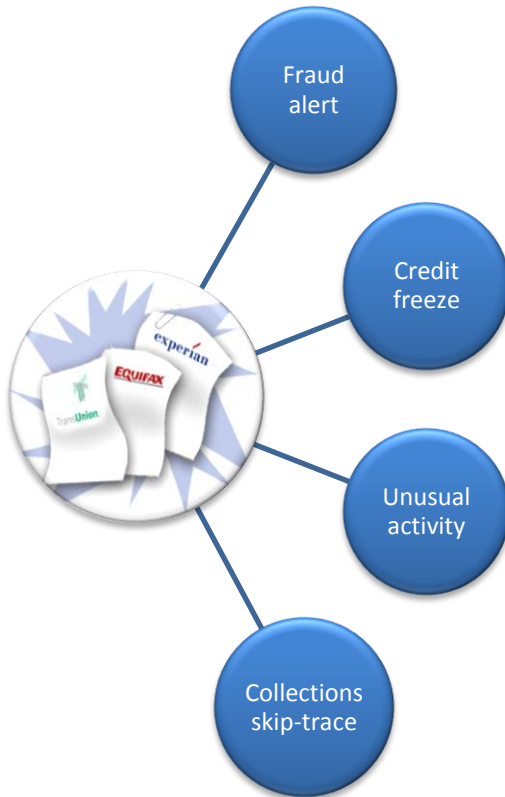
**Sources of Red Flags** Consider other sources of information, including how identity theft may have affected the University and the experience of other institutions. Because technology and criminal techniques change constantly, keep up-to-date on new threats.

**Categories of Common Red Flags** Supplement A to the Red Flags Rule lists five specific categories of warning signs to consider in our Program. Some examples may be relevant to the University. Some may be relevant only when combined or considered with other indicators of identity theft. The examples listed on the following pages are not an exhaustive compilation or a mandatory checklist, but rather a way to help think about relevant red flags in the context of your department.





-  Red Flag 1 – Alerts, Notifications or Warnings from a Consumer Reporting Agency
-  Red Flag 2 – Suspicious Documents
-  Red Flag 3 – Suspicious Personal Identifying Information
-  Red Flag 4 – Unusual Use of, or Suspicious Activity Related to, the Covered Account
-  Red Flag 5 – 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 Financial Institution or Creditor



## Red Flag 1 – Alerts, Notifications or Warnings from a Consumer Reporting Agency



Below are some examples of changes in a credit report or a consumer's credit activity that may signal identity theft:

-  A fraud or active duty alert is included with a consumer report.
-  A notice of a credit freeze in response to a request for a consumer report.
-  A notice of address discrepancy included with a consumer report.
-  A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
  - A recent and significant increase in the volume of inquiries;
  - An unusual number of recently established credit relationships;
  - A material change in the use of credit, especially with respect to recently established credit relationships; or
  - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

### Review

Which of the following might be red flags related to consumer reporting agencies? Indicate True or False next to each item.






True   False

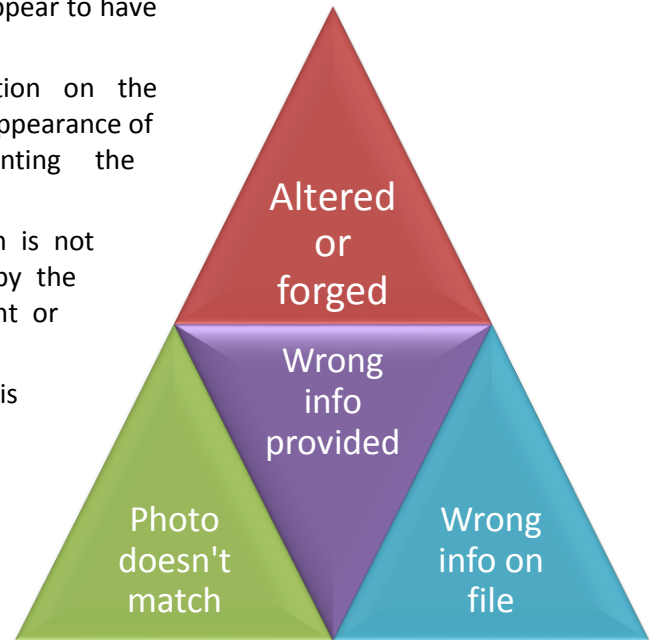
- |                          |                          |   |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | The consumer report indicates that the applicant has moved several times in the last year; however the address provided agrees to the last address on the report. |
| <input type="checkbox"/> | <input type="checkbox"/> | The credit report received by the University contains a notice of address discrepancy.  |
| <input type="checkbox"/> | <input type="checkbox"/> | The University receives notification from the collection agency that the address of record for the student differs from the address provided by the University.   |



## Red Flag 2 – Suspicious Documents

Many times paperwork has the telltale signs of identity theft. Here are examples of red flags involving documents:

-  Documents provided for identification appear to have been altered or forged.
-  The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
-  Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
-  Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
-  An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.



### Review

Which of the following might be red flags related to suspicious documents?

Indicate True or False next to each item.

True   False








- |                          |                          |  |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | You receive a direct deposit form that is wrinkled and has tape holding it together.   |
| <input type="checkbox"/> | <input type="checkbox"/> | The check presented for payment on a student's account does not have the same name as the student's.   |
| <input type="checkbox"/> | <input type="checkbox"/> | The transcript received from the student has an embossed seal and the letterhead matches similar transcripts you have received from high school attended.      |
| <input type="checkbox"/> | <input type="checkbox"/> | While processing a transcript request in person, you note that the person's height and weight doesn't appear to match the description on the driver's license. |





## Red Flag 3 – Suspicious Personal Identifying Information

Identity thieves may use personally identifying information that does not ring true. Below are some red flags involving identifying information:

-  Address does not match any address on file in consumer reports
-  Social Security Number comes back as unissued or deceased
-  Social Security Number is duplicate
-  Address or phone number is same or similar to other fraudulent applications
-  Address or phone number is fictitious, a mail drop, or a prison
-  Person fails to provide all required personal information on an application
-  Person cannot provide answers to personal security questions such as elementary school attended, pet's name, etc.



### Review

Which of the following might be red flags related to suspicious personal identifying information? Indicate True or False next to each item.

True   False

- |                          |                          |   |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | Student submits an application for admission containing a PO Box address.                             |
| <input type="checkbox"/> | <input type="checkbox"/> | The University does not find the address provided by the applicant on the background report received. |
| <input type="checkbox"/> | <input type="checkbox"/> | Banner indicates the SSN entered is a duplicate of an existing entry.                                 |
| <input type="checkbox"/> | <input type="checkbox"/> | The phone number listed on a housing application contains all 4's for the area code.                  |



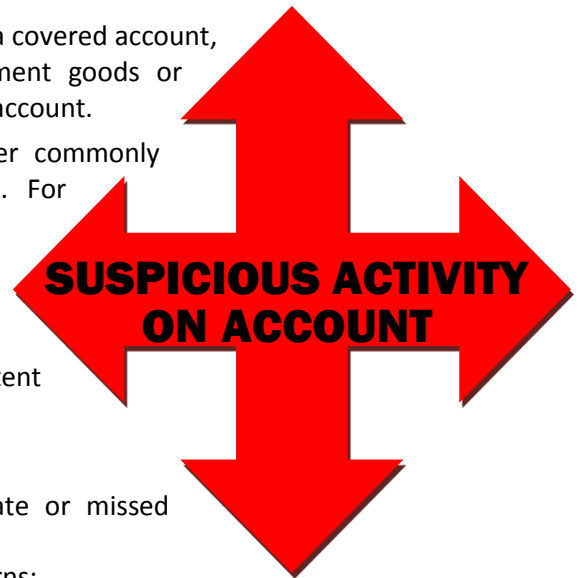
## Red Flag 4 – Unusual Use of, or Suspicious Activity Related to, the Covered Account

Many times the tip-off is how the account is being used. Below are some red flags related to account activity:

- ⊗ Shortly following the notice of a change of address for a covered account, receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.
- ⊗ A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
  - The customer fails to make the first payment, or
  - Makes an initial payment but no subsequent payments.
- ⊗ A covered account is used in a manner that is not consistent with established patterns of activity on the account.

There is, for example:

- Nonpayment when there is no history of late or missed payments;
- A material change in purchasing or usage patterns;
- ⊗ 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).
- ⊗ Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account.
- ⊗ The University is notified that the customer is not receiving documents.
- ⊗ The University is notified of unauthorized charges or transactions in connection with a covered account.



### Review

Which of the following might be red flags related to suspicious activity or use of an account? Indicate True or False next to each item.

True   False

☐   ☐   Letters sent regarding past due account balances are returned undeliverable.

☐   ☐   The University receives a dispute notice on a credit card payment.

☐   ☐   You receive mail back from the post office with a sticker indicating 'Forwarding Order Expired, Unable to Deliver'.



## Red Flag 5 – 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 Financial Institution or Creditor

Many times a red flag that an account has been opened or used fraudulently can come from a customer, a victim of identity theft, a law enforcement authority, or other source.

- When the University is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that the University has opened a fraudulent account for a person engaged in identity theft.



### Review

Which of the following might be red flags related to notice from other sources? Indicate True or False next to each item.

True   False

- |                          |                          |   |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | The University received notice from the FBI of potential ID theft related to a student.                 |
| <input type="checkbox"/> | <input type="checkbox"/> | A student contacts the University and informs them that their wallet was stolen.                        |
| <input type="checkbox"/> | <input type="checkbox"/> | A student contacts the University and indicates that they have been a victim of ID theft.               |
| <input type="checkbox"/> | <input type="checkbox"/> | You receive a call from a student indicating that they have moved and the address on file is incorrect. |

## Identity Theft Follow-up Procedures:

If a department supervisor is notified of red flags indicating possible identity theft, the supervisor needs to perform the following:

- Assess the situation that brought the red flag to the supervisor's attention.
- Verify that there are no other mitigating actions, such as those listed in this guide that can be taken to verify the documents or transactions are valid. These may be department actions not noted in this document. Please supply these mitigating actions to the contacts listed below for review and possible inclusion in future documentation and training.

If the supervisor cannot mitigate the red flag with the actions specified in this guide, they will contact the program administrator immediately and follow up by sending that person an e-mail that describes the red flag, the situation that resulted in the red flag, and any contact information available for parties involved in the transaction.

Upon receipt of a red flag situation, the University will determine the course of action and notify the department(s) responsible for follow up. These actions may include but are not limited to:

- Flag the student account with a red flag hold to notify faculty and staff accessing the account that possible identity theft has occurred.
- Attempt to contact the student in question to verify that an identity theft attempt has been made.
- Changing passwords, security codes, or other ways to access a covered account.
- Closing an existing account.
- Reopening an account with a new account number
- Not opening a new account.
- Not trying to collect on an account or not selling an account to a debt collector.
- Determining that no response is warranted under the particular circumstances.
- Attempt to identify the perpetrator if the student confirms that identity theft has been attempted.
- Refer to the University Police to conduct a criminal investigation if identity theft has occurred.

Once red flag hold has been placed on a covered account, University personnel should take extra care in handling the account including but not limited to:

1. Comparing ID to a recent book of each state's driver license details. Rules change often, so make sure the copy is up to date. Comparing the birth date against the driver's license number as many forgers forget to change this detail. Many states code the license number with the birth date and other identifying data.

2. Requesting additional identification for in-person transactions. Ask the person for a second or even third form of ID if you are still unsure. In the case of a borrowed driver's license where the person looks similar to the original owner of the ID, it is unlikely there will be multiple cards with the same name as the ID. Ask for credit cards<sup>1</sup>.
3. Requiring the student to perform certain transactions in-person, for example, obtaining a refund check, accounts payable check, payroll check, transcript, ID card, etc.
4. Confirming change / update of direct deposit information with the student.
5. Ask additional security questions. Talk to the person, and insert key questions which are not usually thought of. Ask for the person's zodiac sign or high school graduation year. When you believe it is a borrowed ID, ask what the middle initial stands for and see if there is a hesitation before the response.
6. Ask additional questions such as current address, UCard ID, birth date and/or last 4 SSN, when communicating via telephone. For example, when verifying account balances, obtaining SSN information, or verifying registration data.

## Summary

The University's Identity Theft Prevention Program is a result of the "Red Flags" Rule which became effective January 1, 2008. The policy and training program are designed to detect the warning signs – or "red flags" – of identity theft that employees may face in the day-to-day operations of their department and is designed to provide guidance on the steps to prevent the crime and ways to mitigate the damage identity theft inflicts. By identifying red flags in advance, we will be better equipped to spot suspicious patterns when they arise and take steps to prevent a red flag from escalating into a costly episode of identity theft.

This training program will grow and change as the University community share information with one another. Not all of the red flags will pertain to your department. Use the information contained in this training program to identify areas of concern that directly relate to your department. Let us know of situations or specific challenges that your department faces so that we can address those issues in future publications and trainings.