IDENTITY THEFT PROCEDURES

FREQUENTLY ASKED QUESTIONS ABOUT IDENTITY THEFT INCIDENTS AND RED FLAGS

Q1: How is a Red Flags incident different from a data security breach?
A1: A data security breach is the unintentional release of personal information. The Federal Trade Commission (FTC) strongly encourages reasonable data security practices, but the Red Flags Rule is not a data security regulation. Good data security practices, such as UCF Policy 4-008 – Data Classification and Protection, help ensure that personal information does not fall into the hands of identity thieves.

The Red Flags Rule picks up where data security leaves off. If identity thieves do get hold of someone's personal information, they typically use it to get goods or services from unsuspecting businesses and have no intention of paying the bill. By having companies set up procedures to look for and respond to the "Red Flags" that indicate an identity thief is trying to use someone else's information, the rule seeks to reduce the damage identity thieves can inflict on victims of identity theft and on businesses left with accounts receivable balances they'll never be able to collect. While data security practices are incorporated, the Red Flags program is a different kind of plan aimed at preventing a different kind of harm.

Q2: What are some examples of covered accounts that apply to universities?
A2: Examples of covered accounts that apply to universities are as follows:

- Federal Perkins Loan Program
- Student billing and receivables
- Accounts in collection
- UCF Card
- Restitution accounts with installment payments
- Credit bureau data
- Institutional loans
- Student refunds
- Short term loans/advances
- Payment plans, i.e. dining, parking, housing
- Student records
- Payroll advances

Q3: What are some of examples of red flags?
A3: Section II of UCF Policy 2-105.1 – Identity Theft Prevention (as reproduced below) identifies red flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies
1. Report of fraud accompanying a credit report.
2. Notice or report from a credit agency of a credit freeze on an applicant.
3. Notice or report from a credit agency of an active duty alert for an applicant.
4. Receipt of a notice of address discrepancy in response to a credit report request.
5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents
1. Identification document or card that appears to be forged, altered, or inauthentic.
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.

3. Other document with information that is not consistent with existing identifying information.
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information provided (example: inconsistent birth dates).
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application).
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).
5. Social security number presented that is the same as one given by another person.
6. An address or phone number presented that is the same as that of another person.
7. A person fails to provide complete personal identifying information on an application when reminded to do so.
8. A person's identifying information is not consistent with the information that is on file for that person.

D. Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the person's name.
2. Payments stop on an otherwise consistently up-to-date account.
3. Account used in a way that is not consistent with prior use.
4. Mail sent to the individual is repeatedly returned as undeliverable.
5. Notice to the university that a person is not receiving mail sent by the university.
6. Notice to the university that an account has unauthorized activity.
7. Breach in the university's computer system security.
8. Unauthorized access to or use of student account information.

E. Alerts from Others

1. Notice to the university from an individual, identity theft victim, law enforcement official, or other person that the university has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Q4: How are red flags typically detected?

A4: Section III of UCF Policy 2-105.1 – Identity Theft Prevention (as summarized below) identifies some methods for detecting red flags in each of the listed categories:

Enrollment

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

Existing Accounts

1. Verify the identification of the individual if they request information (in person, via telephone, via facsimile, via email).
2. Verify the validity of requests to change billing addresses by mail or email and provide the individual a reasonable means of promptly reporting incorrect billing address changes.
3. Verify changes in banking information given for billing and payment purposes.

Consumer (Credit) Report Requests

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.
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 to be accurate.

Q5: I may have detected a red flag. Now what do I do?
A5: Make sure you follow your department's Red Flags program in determining the appropriate response and steps for risk mitigation. Then, fill out the Red Flags Incident Report and e-mail it to report-fraud@ucf.edu. Depending on the degree of risk posed by the red flag, the following may be recommended, per Section IV of UCF Policy 2-105.1 – Identity Theft Prevention:

1. Continue to monitor a covered account for evidence of identity theft.
2. Contact the individual (for which a credit report was run).
3. Change any passwords or other security devices that permit access to covered accounts.
4. Do not open a new covered account.
5. Provide a new identification number.
6. Notify the program administrator for determination of the appropriate step(s) to take.
7. Notify law enforcement.
8. File or assist in filing a Suspicious Activities Report.
9. Determine that no response is warranted under the particular circumstances.

Q6: My office responded to a red flag incident and successfully prevented a potential case of identity theft. Am I still required to file an incident report?
A6: Yes, one of the many benefits the university will have by your filing an incident report will be the opportunity to review the incident and offer advice to other departments who may experience similar red flags.

Q7: What training is required?
A7: All personnel who play a role in the processing of transactions related to covered accounts are required to take the web course (FSC113 Red Flags-ID Theft Protection). This is a one-time training requirement. Department managers can request a list of active employees who have passed the course from the F&A Red Flags coordinator.

Q8: Is there an annual training requirement?
A8: The webcourse is a one-time requirement, but department managers with covered accounts are responsible for conducting training for their staff at least annually to reinforce knowledge, discuss changes to the program caused by changes in internal business processes or the identification of new red flags, and perform procedures to evaluate the effectiveness of the Red Flags program and implement changes if needed.

Q9: Who is responsible for oversight of the university's Red Flags program?
A9: The university controller or their designee is responsible for oversight of the program.

Q10: Who do I contact for more information or to find out if the Red Flags policy applies to my department?
A10: The Red Flags policy applies if your unit engages in any of the following activities:

A) Enters or alters personally identifying information in a university system or database.
B) Maintains systems that generate personally identifying information.
C) Offers goods or services that individuals can pay for later on an account administered by, or on behalf of, your office.
D) Administers billing, declining balance, debit, or other accounts whether on behalf of your own unit or another university unit/department.
E) Makes loans, such as short-term loans to students, faculty, or staff.
F) Administers student loans.
G) Issues cards to individuals that can be used to access accounts.
H) Uses consumer credit reports such as those issued by Experian, TransUnion, or Equifax.
I) Reports information to credit reporting agencies.
J) Bills for fines.
K) Pursues debt collection.
L) Offers leases to individuals for personal use/non-business purposes.
M) Sells or transfers debts to a third party.

However, please feel free to contact the program administrator's designee(s) listed in the contacts section of this website for more information.

Q11: What is the purpose of the Identity Theft Prevention Program Annual Assessment Worksheet?
A11: The purpose is to document compliance and provide the Red Flags committee with the ability to evaluate the effectiveness of the program.

Q12: Where do I turn if I have questions or need assistance with completing the annual assessment questionnaire?
A12: Feel free to contact the program administrator's designee(s) listed in the contacts section of this website.

Q13: After a Red Flags incident is reported, then what?
A13: Evaluate whether the program worked effectively and whether any changes are needed.

Q14: Do I need to worry about third-party service providers?
A14: If they process personal identifying information related to covered accounts, then we are responsible for making sure they are red flag compliant. Language regarding their compliance is included in purchasing agreements. It is important to list third-party service providers and document them on the Identity Theft Prevention Program Annual Assessment Worksheet so that the program administrator is aware of them.

Q15: What steps must be taken to protect personal identifying information?
A15: In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the university will take the following steps related to its internal operating procedures to protect identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure.
2. Subject to state record retention requirements, ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information.
3. Ensure that office computers with access to covered account information are password protected.
4. Avoid use of Social Security numbers.
5. Ensure that computer virus protection is up to date.
6. Require and keep only the kinds of individual information that are necessary for university purposes.

Q16: As a staff member, is it my responsibility to notify appropriate university personnel that a red flag has been detected?
A16: As a university employee, it is your duty to comply with university programs and policies. You must act if you observe a violation of the Red Flags Rule.

Q17: What are the consequences to UCF if it fails to comply with the Red Flags Rule?
A17: An incident of identity theft could be damaging to UCF and your department in significant ways. The FTC can seek both monetary civil penalties and injunctive relief for violations of the Red Flags Rule. Where the complaint seeks civil penalties, the U.S. Department of Justice typically files the lawsuit in federal court on behalf of the FTC. Each instance in which the company has violated the rule is a separate violation. Injunctive relief in cases like this often requires the parties being sued to comply with the law in the future and provide reports, retain documents, and take other steps to ensure compliance with both the rule and court order. Failure to comply with the court order could subject the parties to further penalties and injunctive relief.

An incident of identity theft could also be damaging to UCF and your department's reputation. It would be detrimental to have fraud attached to UCF in any way. A successful Red Flags program could help UCF guard against damage to the public perception of UCF.