Identity Theft Prevention Program

Use of Social Security Numbers and Financial Information

1. The University will make every reasonable attempt to protect the personal identification and personally identifiable financial information it creates, receives, maintains, and transmits, and to comply with current laws that provide for the protection of these types of information.

2. As allowed and/or required by law, the University of Florida will collect, maintain, use, and disclose Social Security Numbers and credit card or other financial information of employees, students, clients, patients, vendors, and others in the ordinary course of its business.

3. Each University entity with access to personal identification or personally identifiable financial information is responsible for developing and implementing procedures to comply with the Identity Theft Prevention Program.

DEFINITIONS

Account means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

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

Covered Account means:

- An account that the University of Florida offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, student account, or other financial accounts; and
- Any other account that the University offers or maintains for which there is a reasonably foreseeable risk to Customers (Consumers) or to the safety and soundness of the institution from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Credit means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

Credit Card Information includes:

- Credit card number (in part or whole) with or without its verification number
- Credit card expiration date
- Cardholder name
- Cardholder address
Identity Theft Prevention Program (continued)

_Creditor:_ "(A) means a creditor, as defined in section 702 of the Equal Credit Opportunity Act (15 U.S.C. 1691a), that regularly and in the ordinary course of business—

"(i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;

"(ii) furnishes information to consumer reporting agencies, as described in section 623, in connection with a credit transaction; or

"(iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person (i.e., financial aid or Gator1 debit cards);

"(B) does not include a creditor described in subparagraph (A)(iii) that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person (i.e., lawyers, doctors, accountants, dentists, orthodontists, pharmacists, veterinarians, nurse practitioners and social workers and other service providers); and

"(C) includes any other type of creditor, as defined in that section 702, as the agency described in paragraph (1) having authority over that creditor may determine appropriate by rule promulgated by that agency, based on a determination that such creditor offers or maintains accounts that are subject to a reasonably foreseeable risk of identity theft.”.

_Customer (Consumer) _means a person that has a Covered Account with the University of Florida.

_Identity Theft_ (16 CFR 603.2(a)) means a fraud committed or attempted using the identifying information of another person without authority. The term "identifying information" refers to any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any--

- Name, Social Security Number, date of birth, official state or government issued driver license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code; or
- Telecommunication identifying information or access device.

_Records:_ Any document, file, database, image, recording, or other means of expressing fixed information, made or received by an institution according to law or its particular mandate and preserved by it in any form as evidence or information.

_Record Systems:_ All mechanisms and media used for input, storage, organization, display, retrieval, and printing of records. Systems consist of components including, without limitation, computers, computer peripherals, wired and wireless networks used for voice and data, as well as fax machines, photo copiers or paper, and paper filing systems.

_Red Flag _means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
Identity Theft Prevention Program (continued)

Social Security Number: A unique nine-digit number assigned to individuals in the United States of America for the purpose of administering the Social Security laws. Truncated forms (last four digits, first three digits, etc.) of the number are also considered restricted data.

Telecommunication access device means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument). (18 U.S.C. 1029(e))

Telecommunication identifying information means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument. (18 U.S.C. 1029(e))

Workforce means all faculty, staff, students and volunteers, temporary and permanent, full-time and part-time, with access to personal identification and financial information who are employed by or otherwise associated with the University of Florida and their affiliated entities.

- PRIVACY REQUIREMENTS

1. Social Security Numbers
   a. Classification: Social Security Numbers obtained by the University are classified as restricted data and must be protected from unauthorized use or disclosure.
      1) Security protocols, including those for any hardware and software housing restricted data, will be subject to audit by the University’s internal audit office and information technology offices.
      2) In limited circumstances, with documented approval from the Chief Privacy Officer, individuals and entities may be allowed to use Social Security Numbers or truncated (last four digits) Social Security Numbers for certain specific purposes.
   b. Authorized Uses and Requests for Exemption:
      1) Individuals and units with a bona fide need to collect Social Security Numbers beyond those that are already authorized (listed below) must request an exemption by memorandum through the Privacy Office. The exemption request must:
         a) State the intended use of the number,
         b) Describe in detail the physical and technical security protocols that will protect the data from compromise, and
         c) State how written notice of the use of the number will be provided to the owner.
      2) Authorized uses of Social Security Numbers include:
Identity Theft Prevention Program (continued)

a) Tax Reporting – required as a taxpayer ID for all tax information reported to the IRS, including:
   i. Wage and withholding data for full-time and part-time employees,
   ii. Honoraria provided to guest lecturers,
   iii. Independent contractors working for the University,
   iv. Payments to research participants for 1099s.

b) Financial Aid – to obtain federal financial aid information and to identify and confirm the level of financial aid assistance.

c) Human Resource Services – approved for use on federal I-9 forms for hiring purposes, employment verification, and by certain benefit providers, such as insurance companies for verification of eligibility and coordination of benefits.

d) Law Enforcement – Federal and state agencies often rely upon SSN’s as the primary identifier for law enforcement and criminal information purposes. In the event such agencies request SSN information using proper procedures, it will be provided following review and approval through the Privacy Office in consultation with the Office of the General Counsel.

e) Business Imperatives of the University:
   i. Identity Management – to maintain the integrity of student records and verify the identities of students and workforce members.
   ii. External Reporting – to fulfill the University’s responsibility to provide transcripts and other information for which more universally known IDs are needed and approved.

c. Collection of Social Security Numbers:
   1) An entity of the University may not collect an individual’s Social Security Number unless the entity has stated in writing the purpose for its collection and unless it is:
      a) Specifically authorized by law to do so; or
      b) Imperative for the performance of that entity’s duties and responsibilities as prescribed by law.
   2) Social Security Numbers collected by an entity of the University may not be used by that entity for any purpose other than the purpose provided in the written statement.
   3) An entity of the University collecting an individual’s Social Security Number shall provide that individual with a copy of the written statement required above.

d. Training: Workforce members, including students and volunteers, who have access to Social Security Numbers must complete Social Security Number Privacy Training during their initial orientation and annually, thereafter.
   1) Self-directed training modules are available on the Privacy Office website. Classroom instruction is available by request through the UF Privacy Office.
   2) Unit supervisors/unit administrators are responsible for implementing appropriate unit training requirements based on the job duties of workforce members in the unit.
Identity Theft Prevention Program (continued)

e. Responding to a Privacy Breach: Promptly report loss or theft of Social Security Numbers from University records or record systems to the Privacy Office for immediate investigation.

2. Financial and Consumer Information: If a University organization is a Creditor and maintains Covered Accounts (see Definitions above), the organization must initiate and maintain Identity Theft Prevention Program procedures.

a. Program Administration
   1) The Identity Theft Prevention Program is the responsibility of the University of Florida’s Board of Trustees, which will approve the initial program, recertify the program annually, and maintain appropriate documentation of the program and its subsequent amendments.
   2) Operational responsibility of the program is delegated to the University’s Privacy Office.

b. Identifying Red Flags: A Red Flag, or any situation closely resembling a Red Flag, should be investigated for verification. The following Red Flags are potential indicators of fraud. More detailed examples of these indicators are included in the Exhibits at the end of this section.
   1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
   2) The presentation of suspicious documents;
   3) The presentation of suspicious personal identifying information, such as a suspicious address change;
   4) The unusual use of, or other suspicious activity related to, a Covered Account; and
   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.

c. Responding to Red Flags: Known and suspected fraudulent activity must be reported immediately to protect Customers and the University from damages and loss.
   1) Gather all related documentation and complete a Privacy Incident Report, available on the Privacy Office web site; provide a complete description of the situation. Send the report to the UF Privacy Office.
   2) If, after investigation, a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:
      a) Canceling the transaction;
      b) Notifying and cooperating with appropriate law enforcement;
      c) Determining the extent of liability of the University; and
      d) Notifying the Customer that fraud has been attempted.

d. Violations: Corrective action will be taken in the event of intentional violations of this policy. Such action may include:
   1) Modification of a process, practice, record or record system to better protect the confidentiality of Social Security Numbers, and/or
Identity Theft Prevention Program (continued)

2) Disciplinary action up to and including termination or expulsion in accordance with University disciplinary policies.

e. Training: University workforce members who have access to consumer reports and/or accounts must be trained concerning Red Flag Rules.

1) The Privacy Office is responsible for ensuring identity theft training for all requisite workforce members, at hire and annually thereafter.

2) Employees should receive notice when changes are made to the Identity Theft Prevention Program.

f. Updates to the Identity Theft Prevention Program: At regular intervals, as established in the program or as required, the program will be re-evaluated to include:

1) An overview of all aspects of the program to be sure they are up to date and applicable in the current business environment.

2) An assessment of which Accounts are covered by the program.

3) Revision, replacement or elimination of Red Flags, as well as definition of new Red Flags, as appropriate.

4) Review of corrective actions, sanctions, and mitigation plans.

g. Oversight Of Service Provider Arrangements

1) It is the responsibility of University entities that contract for services to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

2) A service provider that maintains its own Identity Theft Prevention Program, consistent with the guidance of the Red Flag rules, validated by appropriate due diligence, and included in the service agreement, may be considered to be meeting these requirements.

3) Any specific requirements should be specifically addressed in the appropriate contract arrangements.

3. Security: The University will implement every reasonable measure to protect restricted data provided to it by individuals, including, but not limited to, creating, maintaining, and using University records and record systems securely so that restricted data are only used and disclosed in accordance with state and federal regulations.

a. Prohibited Activities:

1) Public display of restricted data. (i.e., to exhibit, hold up, post, or make visible or set out for open view, including but not limited to, open view on a computer device, computer network, website, or other electronic medium or device, to members of the public or in a public manner.)

2) Using restricted data as the primary account number or identifier for an individual, except where existing University records or record systems require such use. Existing records or records systems, when retired, will be replaced with records or record systems that do not require or use Social Security Numbers or credit card numbers as the primary account number or identifier.
Identity Theft Prevention Program (continued)

3) Visibly printing restricted data on identification cards or badges.  (NOTE: This prohibition does not include student UFID’s; see the policy for Privacy of UFIDs in this manual.)

4) Using, transmitting by any means, including by email, downloading, or storing restricted data in or from records, record systems, or databases that are not encrypted or otherwise secured.

5) Requiring an individual to transmit his/her Social Security Number or credit card information over the Internet or a computer system or network, unless the connection is secure, or the transmission is encrypted.

6) Requiring an individual to use or transmit his/her Social Security Number to gain access to an Internet website or a computer system or network, unless the connection is secure, or the transmission is encrypted.

b. Limited Access: Access to records and record systems containing restricted data is limited to those who have an approved business reason to know this information.

1) The University limits access to restricted data to employees who have a legitimate University business reason to use or disclose such information or documents. (For more information see:  

2) Unit supervisors/unit administrators are responsible for implementing appropriate unit oversight procedures.

c. Record Disposal: Records containing restricted data must be disposed of in a manner that minimizes the risk of inappropriate access when those documents no longer need to be retained and pursuant to University document retention policies.

1) Paper documents containing restricted data should be shredded immediately, or placed in secure containers for later secure shredding and recycling.

2) Electronic documents containing restricted data should be destroyed in a manner consistent with the “best practices” guidance issued by the information technology offices.

 REFERENCES :
Florida Statutes 119.071(5), 817.568
16 CFR 603.2(a), 16 CFR 681: Identity Theft Rules (“Red Flag Rules”)
§ 334.82(b) Fairness and Accuracy in Credit Transactions Act
Red Flag Program Clarification Act of 2010
UF’s Media Reuse and Data Destruction Standard
UF’s Use Limitations of Personally Identifiable Information

 EXHIBITS :
Request to Use Social Security Numbers (form)
Red Flag Indicators (chart)