Information Technology Services Guidelines

User Guidelines for Identity Theft Prevention

Guidelines No.	ITS-1018-G	Rev:	--
Owner:	IT Security and Compliance		
Approved by:	Sheryl Okuno, Director IT Security and Compliance		
Issued:	8-26-09	Effective:	8-26-09

Table of Contents

1. Purpose

On October 31, 2007, the Federal Trade Commission and the federal financial institution regulatory agencies passed the final legislation to incorporate new sections 114 and 315 into the Fair and Accurate Credit Transactions Act of 2003 (FACTA). These new sections are referred to as the **Red Flag Rules**. Under the Red Flag Rules, every financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, is required to establish a documented Identity Theft Prevention program that provides for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft. Examples of red flag activities include unusual account activity, address discrepancies, fraud alerts on a constituent’s consumer report provided by a Credit Reporting Agency, or the attempted use of suspicious account applications.

Since the University provides student loans and collects payment for some services, it is considered a creditor and the FACTA Red Flag Rules apply. This guideline addresses procedures to:

- Identify relevant campus red flags that meet the FACTA Red Flag Rules definitions;
- Respond appropriately to any detected red flags to prevent and mitigate identity theft;
- Delineate affected University units’ responsibilities;
- Periodically update this guideline to reflect changes in identity theft risks to campus constituents and to the safety and soundness of the University and the CSU; and
- Encourage the ongoing participation of all University constituents to protect against identity theft.

2. Entities Affected by These Guidelines

These guidelines apply to all University departments and employees responsible for providing student loans and/or collecting payment for services.

These guidelines apply to all service providers contracted by the University to perform an activity in connection with one or more accounts or collect payment for services.

3. Definitions

a) Account: An "account" refers to a continuing relationship established by a person with a creditor [the University] to obtain a product or service for personal, family, household, or business purposes. It may also be referred to herein as a covered account.

b) Campus Constituent: Any person who has a covered account with the University.

c) Confidential Information: In addition to personal information (defined below), examples of confidential information include the following: financial records, student educational records, physical description, home address, home phone number, grades, ethnicity, gender, employment history, performance evaluations, disciplinary action plans, or NCAA standings. Confidential information must be interpreted in combination with all information contained on the computer to determine whether a violation has occurred.

d) Consumer Report: A report issued by a consumer reporting agency that is also known as a Notice of Address Discrepancy. For the purpose of this User Guideline, this report is a notice that informs the University of a substantial difference between the campus constituent's address that the University provided when requesting the consumer report and the address(es) in the agency's file for the campus constituent.

e) Covered Account: a) Any account the University offers or maintains primarily for personal, family, household, or business purposes that involves multiple payments or transactions; and/or b) any other account the University offers or maintains for which there is a reasonably foreseeable identity theft risk to campus constituents or to the safety and soundness of the University. Examples include collection accounts, student loans that are funded by the University such as the Perkins Loan program, or discipline-specific sponsored loans such as Nursing loans.

f) Credit: The right granted by a creditor to a debtor to defer payment of a debt or to incur debt and defer its payment or to purchase property or services and defer payment therefore.

g) Creditor: As defined in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a, a creditor is any person or entity that arranges for the extension, renewal, or continuation of credit.

h) Financial Institution: Any state or national bank; state or federal savings and loan association; mutual savings bank; state or federal credit union; or any other entity [the University] that holds a "transaction account" belonging to a constituent.

i) Identifying Information: Any name or number that may be used alone or in conjunction with any other information to identify a specific person. Identifying information generally includes name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or unique electronic identification number.

j) Identity Theft: The act of fraud committed using the identifying information of another person.

k) Identity Theft Department Administrator: The administrator, appointed in each University department determined to handle covered accounts within their business processes, responsible for detecting and logging red flags; preventing and managing red flag incidents; training department staff; and reporting identity theft occurrences to the Identity Theft Program Administrator.

l) Identity Theft Program Administrator: The campus administrator responsible for the annual review of campus identity theft occurrences; changes in identity theft methodology, detection, and prevention; changes of University accounts covered by this guideline; and changes in University business arrangements with other entities and service providers. The Director for IT Security and Compliance is the designated CSULA Identity Theft Program Administrator.

m) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Confidential data is information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of the University is governed by specific standards and controls designed to protect the information.

n) Level 2 Internal Use Data: Internal use information is information which must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights, or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

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

p) Personal Information: California Civil Code 1798.29 defines personal information as: An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security Number
- Driver's License or California Identification Card number
- Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Medical information
- Health insurance information

q) Red Flag: A pattern, practice, or specific activity that indicates the possible occurrence of identity theft.

r) Service Provider: A service provider is a person or business entity that provides a service directly to the University relating to or in connection with a covered account.

s) Transaction Account: A deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

4. Guidelines

4.1 Identification of Covered Accounts

Before identifying relevant red flags, all University departments must first determine whether there are covered accounts within the business processes of their respective units that meet the criteria of a covered account. Generally, covered accounts distribute reimbursable University funds; extend, renew, or continue credit; and allow the account owner to make multiple payments or transactions.

Covered accounts include:

- Student loans of University funds that are not funded by federal resources and are repaid by a payment schedule.
- Installment payments and short-term loans.
- Accounts that are created for ongoing services and allow students to reimburse when billed or over a period of time.
- Any type of collection account.

Covered accounts do not include:

- Student loans that are funded by federal resources and only disbursed by the University.
- Fee-for-service applications such as food services, parking passes, commuter services, one-time health services, and the like.
- Collection of fees such as Library fines or parking citations.
- Golden Eagle Card accounts.

4.2 Identification of Red Flags

In order to identify relevant red flags, University departments that offer and manage covered accounts must review and evaluate the methods utilized to open covered accounts, to allow access to covered accounts, and any previous known occurrences of identity theft.

As a guide, the following are potential red flags for each of the listed categories:

a) Notifications and Warnings from Credit Reporting Agencies.

- Report of fraud accompanying a credit report from a credit agency.
- Notice or report from a credit agency of a credit freeze on a customer or applicant.
- Notice or report from a credit agency of an active duty alert for an applicant.
- Indication from a credit report of activity that is inconsistent with a campus constituent’s usual pattern or activity.

b) Suspicious Documents.

- Identification document or card that appears to be forged, altered, or inauthentic.
- Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document.
- Other document with information that is not consistent with existing campus constituent’s information, such as a person’s signature on a check appears forged.
- Application for service that appears to have been altered or forged.

c) Suspicious Personal Identifying Information.

- Identifying information presented that is inconsistent with other information the campus constituent provided, such as inconsistent birth dates.
- Identifying information presented that is inconsistent with other sources of information, such as an address that does not match the address on a driver’s license.
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.

- Identifying information presented that is consistent with fraudulent activity, such as an invalid phone number or fictitious billing address.
- Social security number presented that is the same as one given by another campus constituent.
- An address or phone number presented that is the same as that of another person who is not a family member, spouse, or roommate.
- Failing to provide complete personal identifying information on an application when reminded to do so. However, as a reminder, by law social security numbers must not be required.
- Identifying information that is not consistent with the information on the official record for the campus constituent.

d) Suspicious Account Activity or Unusual Use of Account.

- Change of address for an account followed by a request to change the account holder's name.
- Payments stop on an otherwise consistently up-to-date account.
- Account used in a way that is not consistent with prior use, such as very high activity.
- Mail sent to the account holder is repeatedly returned as undeliverable.
- Notification to the University that a campus constituent is not receiving mail sent by the University.
- Notification to the University that an account has unauthorized activity.
- Breach in any University or department computer system security.
- Unauthorized access to or use of campus constituent's account information.

e) Alerts from Others.

- Notification to the University from a campus constituent, identity theft victim, or law enforcement authority that identity theft has occurred.
- Information from any person that they have opened or are maintaining a fraudulent account for a person engaged in identity theft or know of someone who has done so.

4.3 Detecting Red Flags and Preventing Identity Theft

Departments that offer and manage covered accounts are responsible for appointing an Identity Theft Department Administrator. This administrator is responsible for developing, documenting, monitoring, and updating internal processes and procedures that detect, prevent, and mitigate identity theft. These written procedures should also include employee training and steps to report identity theft incidents to the Identity Theft Program Administrator. Departments may be asked to produce their written procedures during future information security audits. Each department must do its part to ensure the University remains compliant with the legal requirements of the Red Flag Rules.

The following are guidelines to assist departments in developing these procedures.

4.3.1 New Covered Accounts

In order to detect any of the red flags identified above, University personnel must take the following steps to obtain and verify the identity of all campus constituents opening a new covered account:

- Require identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification.
- Verify the campus constituent's identity. For example, thoroughly review the driver's license or other identification card for authenticity and address accuracy.
- Review documentation showing the existence of a business entity.
- Independently contact the campus constituent using the official campus record information to ensure information accuracy.

4.3.2 Existing Covered Accounts

In order to detect any of the red flags identified above, University personnel must take the following steps to monitor transactions with an existing covered account:

- Request at least one verifiable identification information field of all constituents who request information whether in person or via telephone, facsimile, or e-mail.
- Verify the validity of requests to change billing addresses by checking with the holder of the official University record for a recent change-of-address transaction.
- Verify changes in banking information given for billing and payment purposes.

4.4 Mitigating Identity Theft

In the event a University employee detects any identified red flags, the following two steps should be taken immediately:

- Contact the appropriate Identity Theft Department Administrator. The administrator and/or designee must take one or more of the steps outlined in 4.4.1 below, depending upon the degree of risk posed by the red flag.
- Contact the Identity Theft Program Administrator for assistance with risk assessment and determination of the appropriate next steps to take. This is a critical step because if a crime was committed, electronic evidence may need to be collected and preserved.

4.4.1 Managing an Identity Theft incident

The following are guidelines to assist departments in identifying appropriate responses to a potential identity theft incident. Again, administrators may take one or more of the following actions:

- Notify other department employees about the event so everyone is alerted to the constituent's identity and the alleged identity thief's identity, if known.
- Closely review and continually monitor the covered account for any evidence of identity theft.
- Contact the campus constituent holder of the covered account.

- Change any passwords or other security codes and devices that permit electronic access to a covered account.
- Close the existing covered account.
- Not open a new covered account.
- Re-open a covered account with a new number after the campus constituent has been notified of the incident and his or her identity verified.
- Not attempt to collect payment on a covered account.
- Notify University Police.
- Determine that no response is warranted under the particular circumstances.

4.4.2 Preventing Future Identity Theft Incidents

To prevent the likelihood of future identity theft occurring in any manner, all University employees should take the following steps to protect campus constituent identifying information:

- Keep offices and unlocked file cabinets clear of documents containing campus constituent identifying information. Be sure file cabinets, cupboards, and closets containing confidential and personal information remain locked when unattended.
- Never leave documents containing confidential or personal information on printers or facsimile machines. Before faxing confidential or personal information, contact the recipient to be sure they are standing by their fax to immediately retrieve the document.
- Undertake complete and secure destruction of paper documents and computer files containing campus constituent information by using a confetti or pulp paper shredder.
- Ensure all computers are password protected and that computers are locked [*control/alt/delete*, then *enter*] every time a computer is left unattended.
- Maintain up-to-date computer anti-virus protection at all times.
- Promptly report the loss or theft of any device which grants physical access to a University facility (e.g., a card or token).
- Promptly report the loss or theft of any device that stores or transmits University data (e.g., computer, laptop, server, CD, DVD, electronic storage media, or smart phone) to University Police. Users must also promptly submit a *Lost/Stolen Computer/Electronic Storage Device Report* to IT Security and Compliance.
- Do not dispose, transfer, reassign, or donate any computers, laptops, electronic storage devices, or media, or return any smart phones to a service provider without first cleansing the equipment of any confidential, personal, or proprietary information.
- Departments and business units are responsible for ensuring that confidential information is encrypted on all electronic media.
- Do not send unencrypted protected University data over a public network.
- Do not remove constituent-identifying information from the campus without prior administrator authorization. If approved to do so, ensure that electronic files are encrypted, laptops are password protected, and documents and devices are secured and supervised at all times.

- If Social Security numbers (SSN) are required for financial reasons or verification of a campus constituent's identity, request only the last 4 digits. Whenever possible, use the campus identification number (CIN) instead of the SSN.
- Require and keep only campus constituent information that is necessary for University business purposes. University data must be retained, secured, and destroyed in compliance with all legal and regulatory requirements while implementing appropriate best practices.
- Ensure that all Web site requests for confidential information use encrypted transport methods by forcing users to a secured site (i.e., https) and if not available, provide clear notice that the Web site is not secured.

4.5 Responsibilities for University Departments

All University departments must determine whether there are covered accounts within the business processes of their respective units that meet the criteria of a covered account.

All University departments that offer and manage covered accounts are responsible for:

- Appointing an Identity Theft Department Administrator to oversee the department's red flag program;
- Reviewing and evaluating the methods utilized to open covered accounts, to allow access to covered accounts;
- Knowing about previous occurrences of identity theft;
- Ensuring staff are aware of all red flags for each occurrence category;
- Developing, documenting, monitoring, and updating internal business processes and procedures that detect, prevent, and mitigate identity theft;
- Training staff on the department's internal procedures; and
- Reporting red flag incidents to the appropriate Identity Theft Department Administrator.

4.6 Responsibilities for Service Providers

In the event the University engages a service provider to perform an activity in connection with one or more accounts, the University must take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

- Require, by contract, that service providers have such policies and procedures in place; and
- Require, by contract, that service providers review their service's program and report any red flags to the appropriate Identity Theft Department Administrator.

4.7 Identity Theft Program Administration

The Vice President for Information Technology Services/Chief Technology Officer is the oversight officer for the CSULA Identity Theft Prevention program. The Director for IT Security and Compliance acts as the Identity Theft Program Administrator responsible for managing the campus program and ensuring departmental compliance.

The Identity Theft Program Administrator is responsible for:

- Administering the Identity Theft Prevention program for Cal State L.A.;
- Ensuring appropriate training for Identity Theft Department Administrators;

- Determining which prevention and mitigation steps should be taken in particular circumstances, if requested to do so by the Identity Theft Department Administrator;
- Compiling a comprehensive log of all campus identity theft events;
- Monitoring changes in identity theft methods, detection and prevention as discovered through information security alerts, advisories, periodicals, journals, organization memberships, Web sites, and security vendors and consultants and providing this information to appropriate departments;
- Monitoring changes in the types of accounts the University maintains; and
- Monitoring changes in the University's business arrangements with other entities and service providers.

The Identity Theft Department Administrator is responsible for:

- Administering the Identity Theft Prevention program for their respective departments;
- Ensuring appropriate training for University staff;
- Reviewing any department reports regarding the detection of red flags;
- Determining which prevention and mitigation steps should be taken in particular circumstances or contacting the Identity Theft Program Administrator for risk assessment assistance;
- Contacting the Director of IT Security and Compliance if there are indications of a system breach or the collection of electronic evidence may be necessary;
- Compiling a log of all department identity theft events and submitting the log monthly to the Identity Theft Program Administrator;
- Ensuring department compliance with the CSULA Identity Theft Prevention program; and
- Monitoring changes in the department's business arrangements with other entities and service providers.

Every two years the Identity Theft Program Administrator will determine whether updates or changes to the CSULA Identity Theft Prevention program and this User Guideline are required. If warranted, the Identity Theft Program Administrator will update, circulate for approval, and Web-post a revised User Guidelines for Identity Theft Prevention.

5. Contacts and Resources

a) Questions regarding these guidelines should be directed to itsecurity@calstatela.edu.

b) Questions regarding whether a covered account meets the Red Flag Rules requirements should be directed to the Director, IT Security and Compliance, 323-343-2600, LIB PW 1070.

c) Questions regarding financial accounts, contracts, and student loans should be directed to the Associate Vice President for Administration and Finance, 323-343-3541, ADM 514.

f) Questions regarding student records management should be directed to the Admissions Director, 323-343-3863, ADM 246.

g) Questions regarding staff records should be directed to the Director of Human Resources Management, 323-343-3673, ADM 606.

h) Questions regarding faculty records should be directed to the Director of Faculty Affairs, 323-343-3810, ADM 706.

6. Applicable Federal and State Laws and Regulations

Federal	Title
Fair Credit Reporting Act (FCRA)	**Fair Credit Reporting Act (FCRA), U.S. Code, Title 15 § 1681 et seq.** For the complete text as amended October 2001, visit: http://www.ftc.gov/os/statutes/fcra.htm This is the federal law that protects consumer credit and credit reporting.
Fair and Accurate Credit Transactions Act of 2003 (FACTA)	**Fair and Accurate Credit Transactions Act of 2003 (FACTA), the Red Flag Rules** For the business alert summary, visit: http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm This is a federal law that requires financial institutions and creditors to develop and implement written identity theft prevention programs.
State	**Title**
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that provides information on safeguarding personal information.
SB 1386	**California Personal Information Privacy Act, SB 1386** http://www.info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb1386_bill_20020926_chaptered.html This bill modified Civil Code Section 1798.29 to require notification to individuals whose personal information is or is assumed to have been acquired by unauthorized individuals.

7. Related Documents

ID/Control #	Title
ITS-1005-G	User Guidelines for Portable Electronic Storage Media http://www.calstatela.edu/its/policies/ITS-1005-G_PortableElectronicStorageMedia.pdf These guidelines are intended to help students, faculty, and staff met the University's accepted standards for protecting confidential information that is copied, downloaded, or stored on portable electronic storage media.

ITS-1006-G	User Guidelines for Securing Offices, Workspaces, and Documents http://www.calstatela.edu/its/policies/ITS-1006-G_SecureDocs-OfficesGuidelines.pdf These guidelines are intended to help the campus community protect offices, machines, devices, and documents from unauthorized access to confidential, personal, and proprietary information.
ITS-1007-G	User Guidelines for Laptop Security http://www.calstatela.edu/its/policies/ITS-1007-G_LaptopSecurityGuidelines.pdf These guidelines outline the steps for securing laptops and the personal, confidential, and/or proprietary information contained on them.
ITS-1008-G	User Guidelines for Reporting a Lost or Stolen Computer or Electronic Storage Device http://www.calstatela.edu/its/policies/ITS-1008-G_Lost-StolenComputerGuidelines.pdf These guidelines outline the steps users must take to ensure the campus complies with all law and regulations regarding personal and confidential information when desktop or laptop computers and electronic storage devices are lost or stolen.
Are you Secure?	Identity Theft: Quick Tips for Victims http://www.calstatela.edu/its/itsecurity/tips/idtheft-victim.htm This Web site provides tips for victims of identity theft or fraud.
Are you Secure?	Quick ID Theft Reference Guide http://www.calstatela.edu/its/itsecurity/idtheft_quickrefguide.pdf This document is a quick identity theft reference guide.