IDentity Theft

QUICK REFERENCE GUIDE

A guide to protect you and the University

Campus Information Security Awareness
for Students, Faculty and Staff

Information Technology Services

Information Security Assurance Program

Director, IT Security and Compliance
323-343-2600
ITSecurity@calstatela.edu

ITS Help Desk
323-343-6170
LIB PW Lobby
helpdesk@calstatela.edu

Are You Secure? Website
www.calstatela.edu/its/itsecurity

ITS Alerts
www.calstatela.edu/its/alerts

Information Security Guidelines
www.calstatela.edu/its/itsecurity/guidelines

Information Security Awareness is among the most powerful tools in the fight against identity theft, and that's where you play an important role. The more you know how to protect your identity and that of our students, faculty and staff, and what to do if a problem occurs, the harder it is for identity thieves to commit their crimes.

Technology can help us safeguard our protected data but technology alone is not enough. Information security awareness uses a two-pronged approach: behavioral and technological, and the campus community should address both equally. Together, both approaches provide the necessary foundation for a safe, secure University environment.

Privacy and identity protection are possible only with an informed campus community. Please continue employing best practices and raising your information security awareness. Use this guide to help you protect information – yours and the University's – and to take action if personal or confidential information is at risk. The adjacent Information Security Assurance Program resources can provide additional information.

ITS Information Technology Services
Library Palmer Wing 1070
Phone: 323-343-2600 | Fax: 323-343-2602
http://www.calstatela.edu/its/

PREVENTING AND MANAGING IDENTITY THEFT

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name.

DETER

Deter identity thieves by safeguarding your information.

Shred financial documents and paperwork with personal information before you discard them.

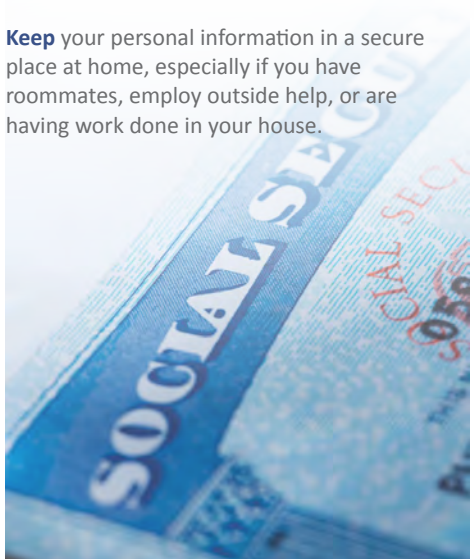
Protect your Social Security number. Don't carry your Social Security card in your wallet or write your SSN on a check. Give it out only if absolutely necessary or ask to use another identifier.

Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.

Never click on links sent in unsolicited e-mails: instead, type in the Web address you know. Use firewalls, anti-spyware and anti-virus software to protect your home computer; keep them up-to-date.

Don't use an obvious password like your birth date, your mother's maiden name, or the last four digits of your SSN or phone number.

Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.



DETECT

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Be alert to signs that require immediate attention:

- Bills that do not arrive as expected.
- Unexpected credit cards or account statements.
- Denials for credit for no apparent reason.
- Calls or letters about purchases you did not make.

Inspect:

- **Your credit report.** Credit reports contain information about you, including what accounts you have and your bill paying history.
  - The law requires the major nationwide consumer reporting companies – Equifax, Experian and TransUnion – to give you a free copy of your credit report each year if you ask for it.
- **Your financial statements.** Review financial accounts and billing statements regularly, looking for charges you did not make.

DEFEND

Defend against ID theft as soon as you suspect it.

- **Place a "Fraud Alert" on your credit reports,** and review the reports carefully.
- **Close accounts.** Close any accounts that have been tampered with or established fraudulently.
  - Call the security or fraud departments where an account was opened or changed without your okay. Follow up in writing.
  - Ask for written verification that the disputed account has been closed and the fraudulent debts discharged.
  - Keep copies of documents and records of conversations about the theft.
- **File a police report.** File a report with law enforcement officials to help you with creditors who may want proof of the crime.
- **Report the theft to the Federal Trade Commission.** Your report helps law enforcement officials across the country in their investigations.

To learn more about ID theft and how to deter, detect and defend against it, visit www.ftc.gov/idtheft.

REPORTING AGENCIES

Consumer Reporting Companies

- Equifax: www.equifax.com
  877-322-8228 - Order report
  888-766-0008 - Fraud alert
- Experian: www.experian.com
  888-397-3742- Order report
  888-EXPERIAN (397-3742) - Fraud alert
- TransUnion: www.transunion.com
  800-888-4213 - Order report
  800-680-7289 - Fraud alert

Free Annual Credit Report

- www.AnnualCreditReport.com
- 877-322-8228

Social Security Number Fraud

- oig.ssa.gov/report-fraud-waste-or-abuse
- 800-269-0271 - Fraud hotline
- U.S. Mail:
  Social Security Fraud Hotline
  P.O. Box 17785
  Baltimore, MD 21235

Social Security Annual Benefits Statement

- www.ssa.gov/mystatement
- 800-722-1213

Bank and Check Fraud

- Telecheck:
  www.firstdata.com/telecheck/telecheck-check-fraud.htm
- National Check and Fraud Center:
  www.ckfraud.org
  843-751-2143 - Fraud hotline

Federal Trade Commission

- www.ftc.gov/idtheft
- 877-ID-THEFT (438-4338)

INFORMATION SECURITY LEGISLATION

Family Educational Rights and Privacy Act (FERPA): Federal law that protects the privacy of student education records. Parents or eligible students (18 years of age) have the right to inspect education records and to request corrections if inaccurate or misleading. Generally schools cannot release any education record without written permission from the parent or eligible student. Under certain conditions some records can be disclosed without consent to or for accrediting organizations, schools to which a student is transferring, judicial orders or subpoenas, health and safety emergencies.If the parent or eligible student allows, schools may also disclose, without consent, directory information such as a student's name, address, e-mail address, phone number, date and place of birth, enrollment status, major field of study, participation in officially recognized activities and sports, weight and height of athletic team members, attendance dates, degrees and awards, most recent educational agency or institution attended by the student, and status as a student employee and department employed. **All requests for student directory information must be sent to Enrollment Services, ADM 146 or the Records Office, ADM 409.** www.calstatela.edu/**ferpa**.

Fair and Accurate Credit Transactions Act of 2003 (FACTA): Referred to as the **Red Flag** Rules, every institution 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. Since the University provides student loans and collects payment for some services, it is considered a creditor and the Red Flag Rules apply. See *ITS-1018-G User Guidelines for Identity Theft Prevention*: www.calstatela.edu/**its/itsecurity/guidelines**.

California Civil Code Sections 1798.29, 1798.80, 1798.82, 1798.84, and 1798.85 These state law sections outline requirements for safeguarding personal information. Among other things, it defines confidential information to include an individual's first name or initial and last name in combination with any one or more of the following: Social Security number, driver's license or CA ID card number; account, credit or debit card number in combination with any security code, access code or password; medical information; and health insurance information. The University is required to notify all affected individuals if their confidential information is acquired, or reasonably assumed to have been acquired, by unauthorized individuals.

California Civil Code Section 1798.81: This section requires businesses to take all reasonable steps to dispose, or arrange for disposal, of confidential records within its custody when the records are no longer needed by a) shredding, b) erasing or c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means. The University paper shredder standard is pulp or confetti shredder. For electronic media, see *ITS-1021-G User Guidelines for Data Sanitization*: www.calstatela.edu/**its/itsecurity/guidelines**.

Payment Card Industry Data Security Standard (PCI DSS): Developed in 2004 by the PCI Security Standards Council, PCI DSS is a set of comprehensive requirements for enhancing payment card data security. In 2009, it was recognized that universities collect credit card information and process credit card payment, and are thereby obligated to adhere to the PCI DSS rules and regulations. See *ITS-1025- User Guidelines for Collecting and Processing Credit Card Information*: www.calstatela.edu/**its/itsecurity/guidelines**.

Learn more about identity theft and fraud on the Department of Justice website: http://www.ojp.usdoj.gov/programs/identitytheft.htm

FIND ADDITIONAL SECURITY RESOURCES AT http://www.calstatela.edu/**its/itsecurity**