



RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

Los Angeles World Trade Center
350 South Figueroa Street, Suite 188
Los Angeles, CA 90071

Telephone: (213) 253-5600
Facsimile: (213) 633-4733

March 21, 2013

To: Audit Committee

From: Richard Sanchez
Chief Information Officer

REVIEW OF BOARD POLICY 7.100 – IDENTITY THEFT PREVENTION PROGRAM

The Chief Information Office, in conjunction with County Counsel, reviewed Board Policy 7.100 to ensure compliance with the new amended legislation and recommends the following revisions:

1. Purpose – made revisions to narrative to reflect the correct title Fair and Accurate Credit Transactions Act (FACTA).
2. Policy section – deleted checking accounts, and savings account. These would be considered a “transaction account” rather than a “covered account” under the revised Red Flag Rule.
3. Policy section – replaced “covered accounts” paragraph with advances funds to or on behalf of an individual or entity based upon an obligation to repay such funds.
4. Policy section – relocated definitions section to the end of the policy to be consistent with other policy formats.
5. Responsible Department – Chief Executive Office has been deleted. Chief Information Office will be the responsible department.
6. Date Issued/Sunset Date – added Review Date: March 28, 2013 and Sunset Review Date: March 31, 2017 (four years).

If you have any questions, please contact me or your staff may contact Peter Loo at 213-253-5627 or ploo@cio.lacounty.gov.

RS:pg

Attachment

c: Chief Executive Officer
Executive Officer, Board of Supervisors

“To Enrich Lives Through Effective And Caring Service”



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
7.100	Identity Theft Prevention Program	03/31/09
		03/31/13

PURPOSE

To comply with the Fair and Accurate Credit Transactions Act (FACTA) Act regulations by implementing a written Identity Theft Prevention Program (ITPP) and policy that identifies and detects the relevant warning signs, or “red flags,” of identity theft. The ITPP program shall be designed to identify, detect, and respond to patterns, practices, or specific activities that could indicate that identity theft has taken place against the County of Los Angeles (County) and/or a County customer.

REFERENCE

July 13, 2004, [Board Order No. 10](#) – Board of Supervisors – Information Technology and Security Policies

Board of Supervisors [Policy No. 6.100](#) – Information Technology and Security Policy

Board of Supervisors [Policy No. 6.103](#) – Countywide Computer Security Threat Responses

Board of Supervisors [Policy No. 6.109](#) – Security Incident Reporting

Board of Supervisors [Policy No. 6.111](#) – Information Security Awareness Training

Board of Supervisors [Policy No. 3.040](#) – General Records Retention and Protection of Records Containing Personal and Confidential Information

Fair and Accurate Credit Transactions (FACT) Act of 2003 [amended sections 114 and 315](#)

March 31, 2009 Board Letter from Chief Executive Officer, [Board Order No. 21](#)

POLICY

BACKGROUND

Pursuant to the Federal Trade Commission's Red Flags Rule, this policy implements Sections 114 and 315 of the ~~Fair and Accurate Credit Transactions Act (FACTA)~~ of 2003 (16 C.F.R. § 681.2). The FACTA is enacted to curtail the effects of identity theft. The FACTA has been amended to require that all creditors (including local government) establish policies and procedures to help prevent identity theft.

DEFINITIONS

-
- A. ~~Covered Account~~ — is an account used mostly for personal, family or household purposes, and that involves multiple payments or transactions, e.g. payments for water billing. ~~Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phones accounts, utility accounts, checking accounts, and savings accounts, and payment deferral accounts. A covered account also includes an account for which there is a foreseeable risk of identity theft.~~
-
- B. ~~Creditor~~ — an individual or entity subject to Fair Credit Report Act who provides covered accounts (i.e., allowing multiple payments or transactions), and defers payments for goods or services (e.g., payment plans for parking tickets).
-
- C. ~~Identifying Information~~ — any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: 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 identification number or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.
-
- D. ~~Identity Theft~~ — fraud committed using the identifying information of another person.
-
- E. ~~Payment Deferral~~ — postponing payments to a future date and/or installments payments on fines or costs.
-
- F. ~~Red Flag~~ — a pattern, practice, or specific activity that indicates the possible existence of identity theft.

GENERAL

This ITPP policy is applicable to all County departments that regularly obtains, uses, or furnishes information to or from consumer reporting agencies or that advances funds to or on behalf of an individual or entity based upon an obligation to repay such funds, except where the County department advances funds for expenses incidental to a service it provides to such individual or entity. ~~possess covered accounts involving creditors or that store identifying information.~~ County departments shall act to identify, detect, and respond to patterns, practices, or specific activities that indicate the possible

existence of identity theft and address discrepancies.

County departments shall:

- A. Each applicable County department shall inventory all applications, which offer or maintain covered accounts that have a reasonably foreseeable risk of identity theft.
- B. Each applicable County department is responsible for determining the appropriate methods of detection and response to Red Flags warnings or violations.
- C. Each applicable County department shall develop and maintain written ITPP programs that prevent, detect, mitigate and respond to identity theft on such applications. Such policies should include procedures to proactively identify County employees, contractors or agents who engage in accessing confidential customer information without authorization or purpose. ITPP policies shall be designed to identify actions that are indicative of snooping, identity theft, or other suspicious and risky behaviors.
- D. Each applicable County department shall identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into ITPP departmental procedures.
- E. Each applicable County department shall respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
- F. Each applicable County department shall ensure that County department ITPP procedures are updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft.
- G. Each applicable County department shall ensure periodic training of employees on the ITPP procedures and any related materials.
- H. Each applicable County department shall immediately report to the County's Chief Information Security Officer (CISO) ~~and the Office of County Investigation~~ any significant violations of the ITPP.

OVERSIGHT

Responsibility for developing, implementing and updating this Countywide ITPP policy lies with the Chief Information Officer (Policy Administrator). Responsibility for developing, implementing and updating departmental ITPP procedures lies with departmental management (e.g., business units) including the Departmental Information Security Officer (DISO), senior departmental staff. At

~~†The departmental management and their DISO is level, senior staff shall be~~ responsible for determining the best methods for detection and response to all Red Flag

type violations; for developing departmental ITPP policy and procedure administration; for ensuring appropriate training of staff on the ITPP policy and procedures; and for reviewing any staff reports regarding the detection of Red Flags.

~~In addition, senior staff~~ Departmental management and their DISO shall take steps for preventing and mitigating identity theft; determining which steps of prevention and mitigation should be taken in particular circumstances; and considering periodic revisions to the policy and procedure.

POLICY UPDATES

This ITPP policy shall be periodically reviewed by the Chief Information Officer (CIO) to review changes in identity theft risks. The CIO shall specifically review the circumstances of any identity theft incidents, reported changes in identity theft detection and prevention methods, as well as changes in the County's business arrangements with other entities. After considering these factors, the CIO shall determine whether changes to the County ITPP policy are warranted.

COMPLIANCE

County employees who violate this ITPP policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County information technology resources, and other actions as well as both civil and criminal penalties.

DEFINITIONS

- A. Covered Account – is an account used mostly for personal, family or household purposes, and that involves multiple payments or transactions, e.g. payments for water billing. Covered Accounts include ~~credit card accounts~~, mortgage loans, automobile loans, margin accounts, cell phones accounts, utility accounts, ~~checking accounts, and savings accounts~~, and payment deferral accounts. A covered account also includes any other account for which there is a reasonably foreseeable risk of identity theft.
- B. Creditor – an individual or entity subject to Fair Credit Report Act who extends, renews, or continues credit or regularly provide goods or services first to customers with ~~provides~~ covered accounts (i.e., allowing multiple payments or transactions), and defers payments for such goods or services (e.g., payment plans for parking tickets).
- C. Identifying Information – any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: 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 identification number or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

- D. Identity Theft – fraud committed using the identifying information of another person.
- E. Payment Deferral – postponing payments to a future date and/or installments payments on fines or costs.
- F. Red Flag – a pattern, practice, or specific activity that indicates the possible existence of identity theft.

POLICY EXEMPTIONS

Requests for exceptions to this Board of Supervisors policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and approved by the Board. County departments requesting exceptions should provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County department, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests, confer with the requesting County department, and place the matter on the Board's agenda along with a recommendation for Board action.

RESPONSIBLE DEPARTMENT

~~Chief Executive Office~~

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: March 31, 2009
Review Date: March 28, 2013

Sunset Date: March 31, 2013
Sunset Review Date: March 31, 2017