Chief Executive Office

21. Recommendation: Adopt the proposed Identity Theft Prevention Program (ITPP) as the County's Red Flag policy to comply with the recently amended Federal Fair and Accurate Credit Transaction Act of 2003; and approve the following related actions:

Instruct all Department/District Heads to determine if they have covered accounts as defined in the ITPP and a) immediately begin developing a policy to comply with the ITPP if a department's review identifies covered accounts; b) notify the Chief Information Officer (CIO) in writing of the results of their review including details on the methodology used to determine the results, if no covered accounts are discovered;

Instruct the Chief Executive Officer and the CIO to establish a taskforce that will develop an implementation plan and ensure that all program deliverables and objectives are met by September 2009;

Instruct all Department/District Heads to complete their review and establish a final, department specific policy by December 31, 2009;

Instruct the CIO to report back on the progress of implementation of the ITPP at the first Board of Supervisors meeting in September, 2009, and again in December, 2009; and

Instruct the CIO to report back annually on the status of the ITPP at the first Board of Supervisor's meeting in September commencing in 2010 to include evaluation of the effectiveness of the ITPP with respect to opening of covered accounts, existing covered accounts and service provider arrangements, identification of any significant incidents involving identity theft, responses to such incidents, notification to other departments of "lessons learned;" and any recommendations for changes to the ITPP. (09-0604)

On motion of Supervisor Ridley-Thomas, seconded by Supervisor Knabe, this item was approved.

Ayes: 5 - Supervisor Molina, Supervisor Ridley-Thomas, Supervisor Yaroslavsky, Supervisor Antonovich and Supervisor Knabe

Attachments: Board Letter
Report

County of Los Angeles
CHIEF EXECUTIVE OFFICE
Kenneth Hahn Hall of Administration
500 West Temple Street, Room 713, Los Angeles, California 90012
(213) 974-1101
http://ceo.lacounty.gov

WILLIAM T FUJIOKA
Chief Executive Officer

ADOPTED
BOARD OF SUPERVISORS
COUNTY OF LOS ANGELES

21 MARCH 31, 2009

SACHI A. HAMAI
EXECUTIVE OFFICER

Board of Supervisors
GLORIA MOLINA
First District
MARK RIDLEY-THOMAS
Second District
ZEV YAROSLAVSKY
Third District
DON KNABE
Fourth District
MICHAEL D. ANTONOVICH
Fifth District

March 31, 2009

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, CA 90012

Dear Supervisors:

RECOMMENDATION TO ADOPT COUNTY IDENTITY THEFT PREVENTION PROGRAM – "RED FLAGS" POLICY (ALL DISTRICTS - 3 VOTES)

SUBJECT

This letter seeks Board approval to adopt this Identity Theft Prevention Program (ITPP) as the County's Red Flag policy and instruct all departments to develop a written policy to address their unique business requirements under the Fair and Accurate Credit Transaction Act (FACTA).

IT IS RECOMMENDED THAT YOUR BOARD:

1. Adopt the attached proposed ITPP as the County's Red Flag policy to comply with the recently amended federal FACTA of 2003.

2. Instruct all departments to determine if they have covered accounts as defined in the ITPP and (a) immediately begin developing a policy to comply with the ITPP if a department's review identifies covered accounts; and (b) notify the Chief Information Office (CIO) in writing of the results of their review including details on the methodology used to determine the results, if no covered accounts are discovered.

3. Instruct the Chief Executive Officer (CEO) and the CIO to establish a task force that will develop an implementation plan and to ensure that all program deliverables and objectives are met by September 2009.

4. Instruct all departments to complete their review and establish a final, department specific policy by December 31, 2009.

5. Instruct the CIO to report back on the progress of implementation of the ITPP at the first Board of Supervisors meeting in September, 2009, and again in December, 2009.

6. Instruct the CIO to report back annually on the status of the ITPP at the first Board of Supervisor's meeting in September commencing in 2010. Each annual report should include: Evaluation of the effectiveness of the ITPP with respect to opening of covered accounts, existing covered accounts and service provider arrangements; identification of any significant incidents involving identity theft; responses to such incidents; notification to other departments of "lessons learned"; and any recommendations for changes to the ITPP.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The FACTA of 2003 requires creditors to develop and implement written identity theft prevention programs by May 1, 2009. Under FACTA, a "creditor" is identified as an entity that regularly extends, renews, or continues credit. Non-profit and government entities are included within this definition of "creditor". The County currently maintains covered accounts as defined by FACTA e.g. utility accounts; therefore, the County must comply with the Act's requirements.

Implementation of Strategic Plan Goals

The recommended actions are consistent with the principles of Countywide Strategic Plan Goal #1: Operational Effectiveness.

FISCAL IMPACT/FINANCING

There is no impact to net County cost.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

To meet the terms of FACTA, the Chief Executive Office convened a committee comprised of Department of Public Social Services, County Counsel, Auditor-Controller, Public Defender, Treasurer and Tax Collector, Sheriff and various other departments. The committee developed the attached policy for your Board's review and adoption. Under the proposed County ITPP, each department will develop a written policy to address their unique business requirements under FACTA. The CIO, as Program Administrator, will

assist departments in this effort. Each department must assign an employee at the senior management level to develop, implement, oversee and administer that department's ITPP, including oversight of any departmental service providers providing services relating to the Act. All departments must periodically review and update their policies to maintain compliance under FACTA.

The proposed ITPP has been approved as to form by County Counsel.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

The adoption of this policy will ensure that the County is in compliance with the FACTA.

CONCLUSION

Please return one adopted, stamped copy of this letter to the CEO, Operations Cluster.

Respectfully submitted,

WILLIAM T FUJIOKA
Chief Executive Officer

WTF: EFS:LS
SW:LR:ef

Attachment

c: Public Defender
Sheriff
Auditor Controller
Chief Information Office
County Counsel
Public Social Services
Treasurer and Tax Collector

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
3.2##	Identify Theft Prevention Program	XX/XX/09

PURPOSE

To comply with the Fair and Accurate Credit Transactions (FACT) 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

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 phone 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 installment 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 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 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 senior departmental staff. At the department 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 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.

Policy Exceptions

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: XXXXX XX, 2009

Sunset Date: XXXXX XX, 2009

Reissue Date:

Sunset Review Date: