2005-2006 Civil Grand Jury

City and County of San Francisco

IDENTITY THEFT:

HOW WELL IS THE CITY AND COUNTY COPING?

Purpose of the Civil Grand Jury

The purpose of the Civil Grand Jury is to investigate the operations of the various departments, agencies, and officers of the government of the City and County of San Francisco – to develop constructive recommendations for improving the operations of the City and County of San Francisco, as required by law.

Each Civil Grand Jury has the opportunity and responsibility to determine which officers, departments and agencies it will investigate during its one year term of office. To accomplish this task, the Civil Grand Jury divides into committees. Each committee researches in depth the departments or areas which are being investigated, by visiting government facilities, meeting with public officials, and reading appropriate documents.

The nineteen members of the Civil Grand Jury are selected at random from a pool of thirty prospective jurors. San Francisco residents are invited to apply. More information can be found at: http://www.sfgov.org/site/courts_page.asp?id=3680, or by contacting Civil Grand Jury, 400 McAllister Street, Room 008, San Francisco, CA 94102; (415) 551-3605.

State Law Requirement

Pursuant to state law, reports of the Civil Grand Jury do not identify the names or identifying information about individuals who provided information to the Civil Grand Jury.

Departments and agencies identified in the report must respond to the Presiding Judge of the Superior Court within the number of days specified, with a copy sent to the Board of Supervisors. As to each finding of the Civil Grand Jury, the response must either (1) agree with the finding, or (2) disagree with it, wholly or partially, and explain why. Further, as to each recommendation made by the Civil Grand Jury, the responding party must report either (1) that the recommendation has been implemented, with a summary explanation of how it was; (2) the recommendation has not been implemented, but will be implemented in the future, with a time frame for the implementation; (3) the recommendation requires further analysis, with an explanation of the scope of that analysis and a time frame for the officer or agency head to be prepared to discuss it (less than six months from the release of this report); or (4) that recommendation will not be implemented because it is not warranted or reasonable, with an explanation of why that is. (California Penal Code, secs. 933, 933.05).

Purpose of This Report

The intent of this report is to provide information to City departments and agencies, and more importantly, to San Francisco residents about how the City and County of San Francisco is coping with the problem of identity theft. It includes related findings and recommendations.

I. Summary

Identity theft costs more than $50 billion in the United States each year. California has the third highest rate of identity theft in the nation. The Federal Trade Commission, the national watchdog on identity theft, counted over 43,000 California victims in 2004 and over 1,100 within San Francisco.[1]

The City and County of San Francisco (City) collects citizens' data that can lead to identity theft: social security numbers, credit card numbers, bank account information, driver's license numbers, dates of birth, home addresses, phone numbers, and e-mail addresses. Identity theft occurs when personal information is stolen so criminals can impersonate the victim to obtain credit and/or drain money from the victim's financial accounts.

How well is the City and County of San Francisco coping with the identity theft problem?

II. Introduction

Identity theft made big news in 2005. Some of the institutions adversely affected in 2005 were Bank of America, ChoicePoint, Westlaw, LexisNexis, T. J. Maxx, University of California at Berkeley, CitiFinancial Mortgage, Motorola, Time Warner, General Motors, Ameritrade, and the Colorado State Health Department. How well did the City and County of San Francisco do? Is the City taking proper care of this personal information? Is the personal data collected necessary, and is the City properly safeguarding the information once collected?[2]

III. Methodology

The Civil Grand Jury investigated identity theft in the City and County of San Francisco. Although the theft of personal information needed to steal a person's identity can occur in a variety of ways including pick-pocketing, mail theft, false change of address notices, and/or trash rummaging, the Civil Grand Jury confined its investigation to credit card theft involving computers.

---

[1] http://www.consumer.gov/idtheft/pdf/CY2004/California%20CY2004.pdf Site address verified 12.31.2005.
[2] http://www.idtheftcenter.org/datadisclosure_2005.pdf Site address verified 12.31.2005.

IV. Resources

The Civil Grand Jury conducted interviews from October 28, 2005 through December 22, 2005 with a variety of City departments: Department of Telecommunications & Information Technology, Department of Public Health, Office of the Controller (Payroll Department), San Francisco Police Department (Fraud Division), Office of the City Treasurer & Tax Collector, Municipal Transportation Agency, and Department of Parking & Traffic.

The Civil Grand Jury also obtained primary source material from the Internet and *New York Times*: (Note: Web site addresses verified December 31, 2005.)

1. http://www.idtheftcenter.org/busrisktest.shtml Identity Theft Resource Center.

2. http://cmcWeb.ca/epic/internet/incmc-cmc.nsf/en/fe00095e.html Business Identity Theft Checklist.

3. http://www.consumer.gov/idtheft/ Federal Trade Commission Identity Theft site.

4. http://www.msnbc.msn.com/id/8359692/site/newsweek/ "Grand Theft Identity", *Newsweek*, July 4, 2005.

5. http://www.hipaadvisory.com/regs/securityoverview.htm HIPAA Security Rules Overview. (Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act)

6. http://www.idtheftcenter.org/aftermath2004.pdf Identity Theft: The Aftermath 2004.

7. "Identity Crises", *New York Times*, October 1, 2005, Western edition.

V. Conclusions: Findings & Recommendations

Finding #1 - Department of Public Health: San Francisco General Hospital is the Department of Public Health's largest cash operation. Cash and credit card operations are handled directly with the Bank of America. The Department of Public Health runs its own information technology operation with applications including patient registration, accounting, lifetime clinical services, laboratory work, and on-line eligibility. To facilitate billing with Medicare and Medi-Cal, it is necessary to keep patient social security numbers on file. Although the Department of Public Health has about 5,000 computer workstations at over 400 separate sites, no credit card data is kept on Department's computer files.

There is no clause protecting the confidentiality of data in the Department of Public Health's contract with Bank of America.

Finding #2 - Office of the Treasurer & Tax Collector: In 2004-2005 the treasurer took in over $2.3 billion in tax revenue. Of this total, $19 million was collected by processing 11,200 transactions over the World Wide Web. The treasurer contracted with VeriSign, a NASDAQ-listed corporation that processes over 14 billion Internet transactions daily[3], to handle their Web-related credit card operations. Another $8 million was collected by processing 2,700 transactions through Interactive Voice Response (IVR), an enhanced automated phone service for processing payments made with credit cards.

The City treasurer contracted with Official Payments Corporation for these IVR transactions. Official Payments Corporation has been processing government payments electronically since 1996. Official Payments Corporation also does processing for the United States Internal Revenue Service, 25 states, and more than 1,600 counties and municipalities. No credit card data for Web or IVR transactions are kept on City computer files. A clause protecting confidentiality of data is present in the Treasurer's contract with Official Payments Corporation. (Note: Mail and walk-in credit card numbers are kept on the Treasurer's cashiering system, and are available only to the vault teller on an audit report. This on-request audit report is produced only when there are cash balancing problems.)

Finding #3 – Department of Parking & Traffic: The Department of Parking & Traffic contracts out daily management responsibilities for City-owned parking garages to various parking firms. All credit card transactions with parking garages are handled by the parking firms. Once again, no credit card data or social security numbers are kept on City computer files.

Finding #4 - Parking Citations Division: The Municipal Transportation Agency's Citations Division receives approximately $14 million yearly from some 250,000 Web transactions. As with the Office of the Treasurer & Tax Collector, VeriSign handles its Web transactions. Approximately $4 million is collected annually through some 78,000 phone transactions. Again, Official Payments Corporation handles phone payment transactions. The Citations Division does not retain any credit card or social security numbers on their files.

Finding #5 - Payroll: The Controller's Office has processed City's payroll since 1985 on a heavily modified package application processor that is run on the City's mainframe computer system. Although the payroll system must retain social security numbers for tax reporting purposes and bank account numbers for direct deposits, computer access is limited exclusively to payroll and programming staff. Similar to credit card transactions in shops and restaurants, only the last four digits of social security numbers are printed on checks. No credit card data is kept on the payroll system.

Finding #6 - Police Department: Although our investigation of departments which process major credit card transactions revealed no evidence of City-caused identity theft, we conducted a final interview with the San Francisco Police Department's Fraud Detail to verify our findings. Through early December 2005, police statistics reflect 1,300 instances of all types of identity theft in San Francisco. The police have no records involving identity theft within City government. Statistics are not kept by location of theft because most victims of identity theft do

[3] http://www.verisign.com/verisign-inc/index.html

not know where or how their personal information was stolen.

Finding #7 - Conclusion: The Civil Grand Jury asked all departments listed above and the Department of Telecommunications & Information Services the direct question, "Are you aware of any instances of identity theft caused by the City and County of San Francisco?" All replied negatively to this question.

Recommendation #1: San Francisco's widely distributed information technology departments have wisely chosen to contract out credit card processing (and the identity theft risks inherent in this activity) to nationally recognized firms specializing in Web-based remittance processing. The Civil Grand Jury recommends the departments continue this policy.

Recommendation #2: In answer to the question posed by the title of this report, the City and County of San Francisco is thus far coping well with identity theft. The Civil Grand Jury recommends that the City continues to handle sensitive data with the care that is currently in practice.

Recommendation #3: A clause protecting confidentiality of the City's data should be included in the Department of Public Health's contract with Bank of America.

VI. Required Responses

Department of Public Health – 60 days
Office of the Mayor – 60 days
Board of Supervisors – 90 days