FEDERAL TRADE COMMISSION

OFFICE
OF
INSPECTOR GENERAL

SEMIANNUAL REPORT TO CONGRESS

APRIL 1, 2003 - SEPTEMBER 30, 2003

Report #29

The Honorable Timothy J. Muris
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Chairman Muris:

The attached report covers the Office of Inspector General's (OIG) activities for the second half of fiscal year 2003, and is submitted according to Section 5 of the Inspector General Act of 1978, as amended.

During the six-month period ending September 30, 2003, the OIG issued a report on the status of the FTC's compliance with the Federal Information Security Management Act. The OIG found that the FTC continues to make progress in developing a mature information security program and that the agency is more secure today than it was a year ago. The audit also found that not every major system was Certified and Accredited and that the agency's Plan of Action and Milestones did not reflect all security system vulnerabilities as mandated by OMB. Management, after reviewing the findings, agreed to move forward to correct these deficiencies.

The OIG also started field work on its fiscal year 2003 financial statement audit. Finally, the OIG closed four investigations during the period, referring selected findings of staff wrongdoing to management for appropriate action.

As in the past, management has been responsive to all OIG recommendations. I appreciate management's support, and I look forward to working with you in our ongoing efforts to promote economy and efficiency in agency programs.

Sincerely,

Frederick J. Zirkel
Inspector General

TABLE OF CONTENTS

INTRODUCTION

The Federal Trade Commission (FTC) seeks to assure that the nation's markets are competitive, efficient and free from undue restrictions. The FTC also seeks to improve the operation of the marketplace by ending unfair and deceptive practices, with emphasis on those practices that might unreasonably restrict or inhibit the free exercise of informed choice by consumers. The FTC relies on economic analysis to support its law enforcement efforts and to contribute to the economic policy deliberations of Congress, the Executive Branch, and the public.

To aid the FTC in accomplishing its consumer protection and antitrust missions, the Office of Inspector General (OIG) was provided five workyears and a budget of $747,200 for fiscal year 2003.

AUDIT ACTIVITIES

During this semiannual period, the OIG issued its annual report on computer and information security pursuant to the Federal Information Security Management Act (FISMA), and prepared, together with the agency's Chief Information Officer (CIO), an executive summary assessing how well the agency measured up to government-wide IT performance standards. The OIG also began fieldwork on its annual financial statement audit, and participated in a peer review of its audit quality control program. Details of these audits and reviews are provided below.

Completed Audits

Audit Report Number	Subject of Audits
AR 03-056	Review of the Federal Trade Commission Implementation of the Federal Information Security Management Act for Fiscal Year 2003
AR 03-056A	Federal Information Security Management Act – Executive Summary

Summary of Findings for Audits Issued During the Current Period

In AR 03-056 and AR 03-056A, *Review of the Federal Trade Commission Implementation of the Federal Information Security Management Act for Fiscal Year 2003*, the OIG performed an evaluation of information security at the FTC pursuant to requirements contained in the Federal Information Security Management Act (FISMA). This is the third annual evaluation

completed by the OIG in the area of information and computer security. This year's review objectives were to assess compliance with FISMA and related information security policies, procedures, standards and guidelines, and to test their effectiveness on a representative subset of the agency's information systems.

The FTC continued to make progress in developing a mature information security program, and has implemented or addressed OIG-identified security vulnerabilities discussed in the prior year evaluation. For example, the FTC developed (i) security plans for its major applications and general support system; (ii) policies and procedures that addressed various security issues, such as password management, incident response reporting, remote access, and certification and accreditation; (iii) a Disaster Recovery Plan; and (iv) a new IT security awareness program.

As a result of these and other actions, the OIG believes that the FTC is more secure today (from an information security perspective) than it was just one year ago.

For FY 2003, OMB identified a number of specific vulnerabilities that must be reported as "significant deficiencies." Using this OMB guidance, the OIG identified two significant deficiencies for FY 2003, along with other less significant security vulnerabilities that need to be addressed.

First, the OIG found that only one of seven systems was certified and accredited. OMB requires that all major applications and general support systems undergo a security certification and accreditation once every three years, or sooner if the system has undergone major modifications. By having its systems certified and accredited, the agency gains assurances that its security controls work as anticipated, and that the agency's computer security officer officially accepts the level of risk associated with operating the system.

Next, OMB requires agencies to identify vulnerabilities from all audits, studies and evaluations performed on IT systems on a single corrective action plan called a Plan of Action and Milestones (POA&M). A POA&M is a tool that identifies tasks that need to be accomplished, including required resources and scheduled completion dates. The OIG found that ITM was tracking only OIG-identified vulnerabilities from the annual independent evaluations, and had not been routinely tracking vulnerabilities flowing from other security program efforts, such as annual self assessments. Having a comprehensive list of vulnerabilities helps the agency to better assess its overall security posture and implement a coordinated approach to prioritizing and addressing its IT vulnerabilities.

The OIG also performed internal scans of the FTC network and an external penetration test to assess the effectiveness of security controls. While the outcome for the tests was generally favorable, the OIG noted that some of the same vulnerabilities identified in prior scans were identified again, but on different machines. Further, the external test identified other vulnerabilities on the FTC's web servers that caused them to provide more information about their configuration than is needed. Scan results were provided to the computer security officer for additional analysis and action.

In the Executive Summary to the FISMA security evaluation, the OIG assessed agency progress against OMB-identified computer security standards. This was a quantitative assessment of the extent to which the agency meets established IT security standards. For example, the OIG identified the frequency of self assessments and security reviews, how the agency documents and tracks its IT vulnerabilities, and the extent to which security is integrated into the planning and life cycle of the agency's major systems.

Audits in Which Field Work is in Progress

Audit Report Number	Subject of Audit
AR 04-XXX	**Audit of FTC Financial Statements for Fiscal Year 2003.** The Accountability of Tax Dollars Act requires the Commission, along with many other federal agencies, to submit audited financial statements to the Office of Management and Budget (OMB). Although not required to prior to this fiscal year, the FTC has, for the past six fiscal years, submitted audited financial statements to OMB as a foundation of its efforts to maintain sound financial management within the agency. As in past years, the objective of this year's financial audit is to determine whether the agency's financial statements present fairly the financial position of the agency. The statements to be audited are the Balance Sheet as of September 30, 2003, and the related Statement of Net Cost, Statement of Changes in Net Position, Statement of Budgetary Resources, Statement of Financing, and Statement of Custodial Activity for the year then ended. Audit fieldwork performed during this period included preliminary tests of internal and management controls over the accumulation and reporting of financial information, and compliance with laws and regulations that have a material effect on the financial statements. In addition to following up on audit findings identified in last year's management letter, the OIG will also continue to work with program staff to improve the accuracy, timeliness and usefulness of (i) the agency's performance measures and (ii) financial information submitted to the FTC by court-appointed receivers. The OIG also plans to conduct some additional tests to verify that companies seeking agency approval to merge with or acquire other

firms are paying filing fees in keeping with mandated thresholds and assessment formulas.

Planned Audits

Audit Report Number	Subject of Audit
AR 04-XXX	**Program Inspection: An Evaluation of Controls Over The Transit Subsidy Program.** The Federal Government encourages the use of public mass transportation by its employees. Executive Order 13150, "Federal Workforce Transportation," effective October, 2000, permits Federal agencies in the National Capital Region to provide employees with public transit subsidies approximating their commuting costs up to $100 per month (as of January 1, 2002). The FTC provides about $700,000 in benefits to between 650 and 700 employees annually. The Office of Executive Director has overall responsibility for program planning, implementation and evaluation of the effectiveness of the subsidy program in achieving policy objectives. The Department of Transportation manages the program government wide. To participate in the program, employees must complete an application form certifying the amount of their expected monthly transportation costs. Subsidies are provided in the form of Metrochek vouchers, which can be used as fare cards on Metrorail or to purchase bus or train tickets. The objectives of this program inspection are to determine whether (i) funds are being disbursed in accordance with agency policy; and, (ii) adequate controls are in place to prevent program abuse by employees and/or program administrators.
AR04-XXX	**Audit of the Use of Government Purchase and Travel Cards**. Recent reports by the General Accounting Office and Inspectors General, as well as congressional hearings and press reports, have raised serious concerns regarding the adequacy of internal control systems that monitor the use of the more than 2.5 million government-issued credit cards in circulation. To date, millions of dollars of fraudulent and unauthorized expenditures have been made using these cards. While the purchase and travel card programs have increased efficiency in the federal acquisition process, they have also created new opportunities for fraud and abuse.

The overall objective of this review will be to insure that the credit card programs have effective internal controls to prevent abuses. The OIG will also perform transaction tests to identify (i) potentially fraudulent, improper and abusive uses of purchase cards: and (ii) any long-standing patterns of purchases of prohibited items by travel cardholders.

AR 04-XXX

Audit Survey: Access by Businesses to Registration Instructions and Other Information About the Do Not Call Registry. Many consumers do not want to be called by telemarketers. Industry experts estimated that as of June, 2003, telemarketers attempted approximately 104 million calls to consumers and businesses every day. To help address the problem of unwelcomed calls, the FTC, on January 29, 2003, issued an amended Telemarketing Sales Rule (TSR).

The revised TSR establishes a national "Do Not Call" (DNC) registry for consumers that makes it illegal for for-profit telemarketers to call consumers who have placed their phone numbers on the national registry. To date, there are approximately 52 million numbers on the registry.

Under the rule, telemarketers are required to scrub their call lists against the national "do not call" registry at least once every 90 days. Businesses that fail to comply are subject to a fine of up to$11,000 per violation. Consequently, the timely access to information on how to register with the FTC and download numbers from the registry is critical if businesses are to comply with the TSR and avoid the potentially heavy fines associated with violating the rules.

The OIG has received comments from business organizations who are subject to the TSR rules saying registration information is not readily available or is difficult to locate on the FTC's web site.

Consequently, the OIG plans to review the DNC web site for ease of access along with agency's policies and procedures on staff responsiveness to businesses that have DNC related questions.

AR 04-XXX

Review of Quarterly Plan of Action and Milestones (POA&M) Reports. OMB requires agencies to prepare, on a quarterly basis, a plan that addresses all identified security vulnerabilities. These reports serve to hold agencies

accountable for addressing vulnerabilities in a timely manner In the past, the OIG reviewed the quarterly POA&M at year-end as part of its annual IT security review. To enhance accountability, the OIG will instead review agency quarterly submissions when the reports are issued. This will enable the OIG to provide more timely feedback to management on the results of its efforts to address identified weaknesses.

INVESTIGATIVE ACTIVITIES

The Inspector General is authorized by the IG Act to receive and investigate allegations of fraud, waste and abuse occurring within FTC programs and operations. Matters of possible wrongdoing are referred to the OIG in the form of allegations or complaints from a variety of sources, including FTC employees, other government agencies and the general public.

Reported incidents of possible fraud, waste and abuse can give rise to administrative, civil or criminal investigations. OIG investigations might also be initiated based on the possibility of wrongdoing by firms or individuals when there is an indication that they are or were involved in activities intended to improperly affect the outcome of particular agency enforcement actions. Because this kind of wrongdoing strikes at the integrity of the FTC's consumer protection and antitrust law enforcement missions, the OIG places a high priority on investigating it.

In conducting criminal investigations during the past several years, the OIG has sought assistance from, and worked jointly with, other law enforcement agencies, including other OIG's, the Federal Bureau of Investigation (FBI), the U.S. Postal Inspection Service, the U.S. Secret Service, the Internal Revenue Service, Capitol Hill Police, as well as state agencies and local police departments.

Investigative Summary

During this reporting period, the OIG received 68 complaints/allegations of possible wrongdoing. Of the 68 complaints, 34 involved issues that fall under the jurisdiction of FTC program components (identity theft, credit repair, etc.). Consequently, the OIG referred these matters to the appropriate FTC component for disposition. Another four complaints were referred to other government and/or law enforcement agencies for ultimate disposition.

Of the remaining 30 complaints, 24 were closed without action; two are being monitored during the pendency of an administrative adjudication at the FTC; and four are matters that are under investigation by the OIG.

Following is a summary of the OIG's investigative activities for the six-month period ending September 30, 2003.

Cases pending as of 03/31/03.....	**5**
Plus: New cases.....	**+4**
Less: Cases closed.....	**(4)**
Cases pending as of 9/30/03.....	**5**

The first closed investigation resulted from an allegation made by a credit reporting and collection agency that an individual had used mock-FTC letterhead to write two letters to the credit reporting and collection agency. The letters, which purportedly were sent by an FTC staff attorney in a non-existent FTC regional office, attempted to mislead the company into believing that the FTC not only supported the named individual debtor in her dispute with the credit reporting and collection agency, but also that the FTC was challenging the credit reporting and collection agency's debt collection and credit reporting practices. The purported author of the two bogus FTC letters was informed of the criminal sanctions associated with posing as a federal official, in particular using indicia of an official nature such as FTC letterhead. As no additional bogus correspondence was received by the credit reporting agency, the case was closed.

The OIG closed a second investigation that related to similar conduct. This investigation involved allegations that an individual sent a mock-FTC letter to a national credit bureau that was written to mislead the credit bureau into believing that the FTC supported the individual in the dispute with his creditor. The mock-FTC form letter was created using the letterhead from correspondence the person had received from the Consumer Response Center.

The OIG contacted the suspected author of the bogus letter informing him of the criminal sanctions associated with posing as a federal official, in particular using indicia of an official nature such as FTC letterhead. The OIG also informed the individual that if we learned of such conduct in the future, a referral to a prosecutor would be considered. Thereafter, we closed the case.

The third closed investigation involved OIG assistance to agents from the Department of Homeland Security (DHS) to investigate scam artists using the name of the Federal Trade Commission to legitimize their scam. Specifically, individuals who were targeted were provided a number to call to verify the authenticity of the "prize" they had just won. The person answering the phone claimed to be an employee of the FTC, who then proceeded to assure the consumer that the prize was real. To receive the prize, consumers were asked to pay a fee.

The OIG searched the agency's consumer complaint system for any prior complaints against these individuals, along with the agency's "final order" database to determine whether the individuals were already under FTC order to halt deceptive practices. Program staff were then provided with our findings. They proceed to assist the DHS agent by providing the names of prosecutors from the U.S. Attorney's Office. DHS agents working with a federal prosecutor in Florida continue to pursue the scammers. The OIG closed its investigation after making a referral to staff.

The OIG closed a fourth investigation that resulted from a complaint made by agency management concerning an FTC employee's alleged misuse of position for personal gain. The

OIG developed evidence that indicated that the employee in question misused his/her position and violated IT policy regarding unauthorized access to private information contained in agency systems. A final investigative report was submitted to management, and sanctions against the employee are being considered.

As part of this investigation, the OIG identified systemic weaknesses that allowed this abuse to occur unnoticed. The OIG made three recommendations for corrective action that would strengthen management's ability to monitor its data systems and identify violators. Management has informed the OIG that it has taken steps to implement the recommendations.

Matters Referred for Prosecution

During the current reporting period the OIG did not refer any cases to a federal prosecutor.

OTHER ACTIVITIES

PCIE/ECIE Activities

Peer Review Activities – Federal Offices of Inspector General are required by the IG Act to have a peer review performed of their organization once every three years. These reviews are to be performed only by federal auditors. A committee of the Executive Council on Integrity and Efficiency (ECIE) schedules the review to ensure that resources are available to perform them and that OIG's do not conduct reviews of one another.

Against this background, the FTC/OIG was reviewed by audit staff from the Federal Communications Commission. The objectives of a peer review are to determine for the audit function whether an effective internal quality control system has been established in the office and if policies, procedures and applicable government auditing standards are being followed.

The review team found that the system of quality control for the audit function of the FTC OIG in effect for the year ended May 31, 2003, was designed in accordance with the quality standards established by the PCIE and was being complied with for the year then ended to provide the OIG with reasonable assurance of material compliance with professional auditing standards in the conduct of its audits. Consequently, the FTC/OIG received an unqualified opinion on its system of audit quality control.

Significant Management Decisions

Section 5(a)(12) of the Inspector General Act requires that if the IG disagrees with any significant management decision, such disagreement must be reported in the semiannual report. Further, Section 5(a)(11) of the Act requires that any decision by management to change a significant resolved audit finding must also be disclosed in the semiannual report. For this

reporting period there were no significant final management decisions made on which the IG disagreed, and management did not revise any earlier decision on an OIG audit recommendation.

Access to Information

The IG is to be provided with ready access to all agency records, information, or assistance when conducting an investigation or audit. Section 6(b)(2) of the IG Act requires the IG to report to the agency head, without delay, if the IG believes that access to required information, records, or assistance has been unreasonably refused, or otherwise has not been provided. A summary of each report submitted to the agency head in compliance with Section 6(b)(2) must be provided in the semiannual report in accordance with Section 5(a)(5) of the Act.

During this reporting period, the OIG did not encounter any problems in obtaining assistance or access to agency records. Consequently, no report was issued by the IG to the agency head in accordance with Section 6(b)(2) of the IG Act.

Internet Access

The OIG can be accessed via the world wide web at: http://www.ftc.gov/oig. A visitor to the OIG home page can download recent 1996-2003 (first half) OIG semiannual reports to Congress, the FY 1998 - 2002 financial statement audits, and selected other program and performance audits issued beginning in FY 1999. A list of audit reports issued prior to FY 1999 can also be ordered via an e-mail link to the OIG. In addition to this information resource about the OIG, visitors are also provided a link to other federal organizations and offices of inspectors general.

Audit Resolution

As of the end of this reporting period, all OIG audit recommendations for reports issued in prior periods have been resolved. That is, management and the OIG have reached agreement on what actions need to be taken.

Review of Legislation

Section 4(a)(2) of the IG Act authorizes the IG to review and comment on proposed legislation or regulations relating to the agency or affecting the operations of the OIG. During this reporting period, the OIG provided comments to the PCIE legislative committee on a number of personnel proposals developed by the committee affecting the staff of all federal statutory inspectors general.

Contacting the Office of Inspector General

Employees and the public are encouraged to contact the OIG regarding any incidents of possible fraud, waste, or abuse occurring within FTC programs and operations. The OIG telephone number is **(202) 326-2800**. To report suspected wrongdoing, employees and the public should call the OIG's chief investigator directly on **(202) 326-2618**. A confidential or anonymous

message can be left 24 hours a day. Complaints of allegations of fraud, waste or abuse can also be emailed directly to chogue@ftc.gov.

The OIG is located in Suite 1110, 601 New Jersey Avenue, Washington, D.C. Office hours are from 8:30 a.m. to 5:00 p.m., Monday through Friday, except federal holidays. Mail should be addressed to:

Federal Trade Commission
Office of Inspector General
Room NJ-1110
600 Pennsylvania Avenue, NW
Washington, DC 20580

TABLE I
SUMMARY OF INSPECTOR GENERAL REPORTING REQUIREMENTS

IG Act Reference	Reporting Requirement	Page(s)
Section 4(a)(2)	Review of legislation and regulations	9
Section 5(a)(l)	Significant problems, abuses and deficiencies	1-3
Section 5(a)(2)	Recommendations with respect to significant problems, abuses and deficiencies	2
Section 5(a)(3)	Prior significant recommendations on which corrective actions have not been made	9
Section 5(a)(4)	Matters referred to prosecutive authorities	8
Section 5(a)(5)	Summary of instances where information was refused	9
Section 5(a)(6)	List of audit reports by subject matter, showing dollar value of questioned costs and funds put to better use	1
Section 5(a)(7)	Summary of each particularly significant report	1
Section 5(a)(8)	Statistical tables showing number of reports and dollar value of questioned costs	12
Section 5(a)(9)	Statistical tables showing number of reports and dollar value of recommendations that funds be put to better use	13
Section 5(a)(10)	Summary of each audit issued before this reporting period for which no management decision was made by the end of the reporting period	9
Section 5(a)(11)	Significant revised management decisions	8
Section 5(a)(12)	Significant management decisions with which the inspector general disagrees	8

TABLE II
INSPECTOR GENERAL ISSUED REPORTS
WITH QUESTIONED COSTS

	Number	Dollar Value	
		Questioned Costs	**Unsupported Costs**
A. For which no management decision has been made by the commencement of the reporting period	0	0	[0]
B. Which were issued during the reporting period	1	8,400	[0]
Subtotals (A + B)	1	8,400	[0]
C. For which a management decision was made during the reporting period	0	0	[0]
(i) dollar value of disallowed costs	0	0	[0]
(ii) dollar value of cost not disallowed	0	0	[0]
D. For which no management decision was made by the end of the reporting period	1	8,400	[0]
Reports for which no management decision was made within six months of issuance	0	0	[0]

TABLE III

INSPECTOR GENERAL ISSUED REPORTS WITH RECOMMENDATIONS THAT FUNDS BE PUT TO BETTER USE

	Number	Dollar Value
A. For which no management decision has been made by the commencement of the reporting period	0	0
B. Which were issued during this reporting period	0	0
C. For which a management decision was made during the reporting period	0	0
(i) dollar value of recommendations that were agreed to by management	0	0
- based on proposed management action	0	0
- based on proposed legislative action	0	0
(ii) dollar value of recommendations that were not agreed to by management	0	0
D. For which no management decision has been made by the end of the reporting period	0	0
Reports for which no management decision was made within six months of issuance	0	0