

FEDERAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL



SEMIANNUAL REPORT TO CONGRESS

April 1, 2005 - September 30, 2005

Report #33



OFFICE OF
INSPECTOR GENERAL

FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

The Honorable Deborah Majoras
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Chairman Majoras:

The attached report covers the Office of Inspector General's (OIG) activities for the second half of fiscal year 2005 and is submitted according to Section 5 of the Inspector General Act of 1978, as amended.

During the six-month reporting period ending September 30, 2005, the OIG reviewed vulnerabilities associated with FTC website linkages to external sites, performed an inspection of select aspects of the FTC's Travel and Purchase Cards management program, reviewed agency implementation of the Federal Information Security Management Act (FISMA) including agency activities to address vulnerabilities identified in prior year information technology reviews and closed an audit survey of the Do Not Call Registry. In addition, the OIG issued a management advisory regarding possible fraud in connection with an IT contract for risk management and redundancy assessments of the FTC technology infrastructure. The OIG also began fieldwork on audits of the FTC's FY 2005 financial statements and FTC's implementation of the Government Performance and Results Act.

In addition, the OIG processed 382 consumer inquiries and complaints/allegations of possible wrongdoing during the period, opened two new investigations into wrongdoing, and closed two investigations. The results of these closed investigations were reported to management for ultimate disposition.

As in the past, management has been responsive in attempting to implement 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,

A handwritten signature in black ink, appearing to read "Howard L. Sribnick".

Howard L. Sribnick
Inspector General

TABLE OF CONTENTS

| | |
|---|-----------|
| TRANSMITTAL | |
| INTRODUCTION | 1 |
| AUDIT ACTIVITIES | 1 |
| <i>Completed Audits</i> | <i>1</i> |
| <i>Summary of Findings for Reviews Issued During the Current Period</i> | <i>2</i> |
| <i>Audits in Which Field Work is In Progress</i> | <i>4</i> |
| <i>Planned Audits</i> | <i>5</i> |
| INVESTIGATIVE ACTIVITIES | 6 |
| <i>Investigative Summary</i> | <i>6</i> |
| <i>Investigations Closed</i> | <i>7</i> |
| <i>Matters Referred for Prosecution</i> | |
| OTHER ACTIVITIES | 8 |
| <i>Significant Management Decisions</i> | |
| <i>Access to Information</i> | <i>8</i> |
| <i>Audit Resolution</i> | <i>8</i> |
| <i>Review of Legislation</i> | <i>8</i> |
| <i>Contacting the Office of Inspector General</i> | <i>9</i> |
| TABLE I: SUMMARY OF INSPECTOR GENERAL REPORTING REQUIREMENTS | 10 |
| TABLE II: INSPECTOR GENERAL ISSUED REPORTS WITH QUESTIONED COSTS | 11 |
| TABLE III: INSPECTOR GENERAL ISSUED REPORTS WITH RECOMMENDATIONS THAT FUNDS BE PUT TO BETTER USE | 12 |



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 work years and a budget of \$905,700 for fiscal year 2005.

AUDIT ACTIVITIES

During this semiannual period, the OIG reviewed vulnerabilities associated with FTC website linkages to external web sites, performed an inspection on select aspects of the FTC's Travel and Purchase Cards management program, reviewed agency implementation of the Federal Information Security Management Act, including agency activities to address vulnerabilities identified in prior year information technology reviews and closed an audit survey of the Do Not Call Registry. The OIG also issued a management advisory regarding possible fraud in connection with an IT contract for risk management and redundancy assessments of the FTC technology infrastructure. In addition, the OIG began fieldwork on audits of the FTC's FY FY 2005 financial statements and its implementation of the Government Performance and Results Act. Detailed information regarding these audits and reviews is provided below.

Completed Audits

| <u>Audit Report Number</u> | <u>Subject of Audit</u> |
|----------------------------|---|
| AR 05-064 | Review of FTC Web Page Links |
| AR 05-065 | Review of FTC Purchase and Travel Card Active Account Lists |
| AR 05-066 | Review of Federal Information Security Management Act Corrective Actions for July 1, 2004 to March 31, 2005 |
| AR 05-067 | OIG Audit Survey of the Do Not Call Registry Scrubbing Process |
| AR 05-068 | Review of FTC Implementation of the Federal Information Security Management Act for FY 2005 |

Summary of Findings for Reviews Issued During the Current Period

In AR 05-064, *Review of FTC Web Page Links*, the OIG identified potential technical (IT) vulnerabilities that could impact consumers visiting the FTC web page and linking to other (non-FTC) sites from the web page. The OIG also highlighted the need to develop a linking policy, i.e., a notice to consumers that they are leaving the FTC's domain when clicking on select links.

Due to the sensitive nature of the information contained in our report, we have limited its distribution.

In AR 05-065, *Review of FTC Purchase and Travel Card Active Account Lists*, the OIG assessed agency policies and procedures to cancel the accounts of former employees. Active accounts, regardless of whether employees are in possession of cards, are a vulnerability that could allow credit card fraud to occur.

The OIG found that all purchase cards for employees separating in fiscal year 2004 and the first four months of FY 2005 were cancelled. On the other hand, the OIG identified 13 former employees who still had active travel accounts. The former employees left the agency between November, 2003 and January, 2005. The OIG determined that none of the accounts had any activity during the period of employee separation. The OIG provided the names to management to cancel the accounts.

The OIG concluded that controls to cancel travel card accounts need to be strengthened. As the names of separating employees were known to the program manager, it appears that the credit card vendor was simply not notified timely by this employee.

In AR 05-066, *Review of Federal Information Security Management Act Corrective Actions for July 1, 2004 to March 31, 2005*, the OIG evaluated Information & Technology Management's (ITM) progress in correcting weaknesses identified in previous Government Information Security Reform Act, Federal Information Security Management Act and agency-sponsored security reviews.

During the period of review, ITM identified 127 weaknesses. During the same period, ITM closed 36 weaknesses from this and prior periods. The OIG reviewed these closed items and the actions taken by ITM to close them. The OIG concurred with ITM's disposition of these 36 items based on information provided by ITM and independent verifications by OIG's IT auditors when applicable.

The OIG and ITM continued to work together to review completed corrective actions on a quarterly basis to confirm that remedial actions addressed the identified vulnerabilities.

In AR 05-067, *Audit Survey of the Do Not Call Registry Scrubbing Process*, the objective was to determine whether registered phone numbers were being improperly removed (scrubbed) from the registry. To complete this objective, the OIG (i) reviewed criteria used by the agency's

contractor to scrub the registry, (ii) defined the role played by local phone companies in the scrubbing process, (iii) documented the criteria for removing phone numbers from the registry, and (iv) determined whether the removals were made for reasons consistent with contractual agreements and program objectives.

The OIG reviewed the control environment related to the Registry to document any weaknesses or potential weaknesses in the scrubbing process that would result in consumer phone numbers being scrubbed from the Registry without the consumer's knowledge or consent (e.g., an erroneous scrub).

The OIG found that a formal and repetitive (monthly) process exists to review the Registry to identify the phone numbers which should be scrubbed. This process appears to be functioning as described by all parties involved, although the formal process is not documented to a level that would be considered acceptable in the context of an audit. The total numbers "scrubbed" since the inception of the Registry is less than two percent of the total numbers registered. Given that there are many reasons to scrub a number from the registry (people move, for example) and that the scrubbing process appears to target these numbers, we concluded that a systemic problem (causing numbers to be erroneously deleted from the Registry) does not exist.

In AR 05-068, *Review of FTC Implementation of the Federal Information Security Management Act for FY 2005*, the OIG evaluated the implementation of the FTC information security program, assessed agency progress towards correcting weaknesses addressed within the FY 2005 Plan of Action and Milestones (POA&M), verified and tested information security and access controls for the FTC Network and modem pool, verified staff compliance with the agency's wireless network policy, and evaluated the implementation of IT security policies and procedures at one FTC regional office. The review followed National Institute of Science and Technology guidance for information systems, OMB Memorandum M-05-15, *FY2005 Reporting Instructions for the Federal Information Security Management Act* (June 13, 2005) and best practices used in the IT security industry.

The OIG found that the FTC continues to make progress in developing a mature information security program, and has addressed many of the OIG-identified security vulnerabilities discussed in the prior year evaluation. For example, the FTC (i) tested its Major Applications and General Support Systems for security vulnerabilities; (ii) addressed 51 of 111 issues identified on its POA&M and developed time frames to address the remaining 60 issues; (iii) established new policies and procedures to keep abreast of emerging security vulnerabilities; (iv) implemented a scanning and remediation program for identifying and correcting system vulnerabilities; and (v) modified IT inventory to include interconnections to other systems.

The FTC has also taken steps to ensure privacy in accordance with M-99-05, *Instructions for Complying with the President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records."* The FTC established a Privacy Steering Committee to address and monitor security issues. The FTC posted its privacy policy on its website and runs scans to identify and correct privacy-related vulnerabilities associated with its website. The FTC has also

taken steps to ensure the security and privacy of data located on contractor-owned and/or managed systems.

The agency's firewall prevented the OIG's team of "ethical hackers" from penetrating the network, and the OIG, using sophisticated electronic tracking and detection instruments, did not identify any wireless networks at the headquarters or 601 NJ buildings. At the FTC's Southwest Regional Office the OIG observed physical and operational controls in place to safeguard data.

While the agency has made many needed changes and improvements in its IT security program, the OIG has identified some new vulnerabilities that could impact the overall effectiveness of the IT security program. The OIG identified a vulnerability in the agency's modem pool that enabled the OIG to breach the modem's security controls. This breach could enable a hacker to execute attacks on the FTC network. Additional details were provided to ITM managers, who took immediate steps to correct the vulnerability. This and other technical vulnerabilities that could compromise FTC IT security were provided to ITM in a separate (nonpublic) OIG report.

The OIG also identified weaknesses in the agency's background check process for IT employees. Approximately 30 percent of ITM full-time staff had outdated or no background investigation. Half of these individuals have significant data access and/or security responsibilities. We also identified a weaknesses in the assignment of "roles" to ITM personnel working with the agency's personnel database. This allowed liberal access to privacy data even though such access was not needed for job performance responsibilities.

Finally, at management's request, the OIG reviewed the performance of an IT contractor. The requester was concerned that the contractor may have engaged in fraudulent activity in its performance and billing under the contract. The OIG did not find any indication of fraud but did find that there had been mismanagement on the part of ITM arising from ITM's commitment in the contract to provide information to the contractor needed to complete performance and its inability to do so.

Audits in Which Field Work is In Progress

Audit Report Number

Subject of Review

AR06-069

Audit of the FTC's Financial Statements for Fiscal Year 2005 The purpose of the audit is to express an opinion on the financial statements of the Federal Trade Commission for the fiscal year ending September 30, 2005. The principal statements to be audited include the (a) Balance Sheet; (b) Statement of Net Cost; (c) Statement of Changes in Net Position; (d) Statement of Budgetary Resources; (e) Statement of Financing; (f) Statement of Custodial Activity, and notes to the financial statements. The OIG will also test the internal controls associated with the movement of transactions through the FTC's financial system and assess compliance with selected laws and regulations.

The OIG is using guidance contained in OMB Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements*, in performing this audit. The audited financial statements are required to be included in the financial section of the agency's Performance and Accountability Report to be issued on or before November 15, 2005.

AR05-XXX

Review of Annual Performance Measures Under the Government Performance and Results Act Under the Government Performance and Results Act of 1993 ("GPRA"), virtually every federal agency is required to develop a five-year strategic plan, an annual performance plan and performance measures to assess how well the agency is meeting its performance objectives. Like many other agencies, the FTC strives to capture all of the activities that FTC staff perform to achieve the agency's mission.

The overall objective of the review is to ensure that the agency has, uses and reports on performance data that is compliant with laws and regulations and effectively aligns to the agency's vision and performance budget. The OIG will (i) ensure that current performance activity effectively complies with GPRA and OMB requirements; (ii) determine the value and relationship of current performance information to the agency's mission; (iii) document best practices used by other agencies and their effectiveness; (iv) validate that the performance data currently reported by FTC properly focuses on the priorities of the agency and its senior executives and managers; (v) determine that the appropriate performance reporting mix of output, outcome and efficiency measures is used to report FTC performance; and (vi) evaluate the "feedback" loop in place and the extent to which program management/operations are modified to enhance performance.

Planned Audits

Audit Report Number

Subject of Review

AR06-XXX

Audit of Redress Administration Procedures at Analytics, Inc. Redress is the term applied to situations in which monetary judgments are awarded against a seller of goods or services found to have committed unfair or deceptive trade practices. The amounts assessed and collected are distributed to consumers found to have suffered harm. Redress distributions are almost always made by claims administration agents under contract to the FTC. The OIG has selected one redress contractor to audit.

This contractor, Analytics, Inc., located in Chanhassen, MN, distributed \$36.2 million in FY 2005 to consumers, and, as of 9/30/05, held \$38.5 million in redress funds in bank accounts.

The objectives of this financial-related audit are to document and assess internal controls that are in place to ensure (i) efficient and effective funds management, (ii) safeguarding of fund assets, (iii) accurate reporting of redress activity results, and (iv) compliance with contract regulations.

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 are also initiated when there is an indication that firms or individuals are 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 these investigations.

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, the U.S. Postal Inspection Service, the U.S. Secret Service, the U.S. Marshal's Service, the Internal Revenue Service, Capitol Hill Police, Federal Protective Service as well as state agencies and local police departments.

Investigative Summary

During this reporting period, the OIG received 382 consumer inquiries and of possible wrongdoing. This number reflects a nearly two hundred percent increase over the number of complaints received during the last semiannual reporting period.¹ Of the 382 complaints, 325 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 24 complaints were referred to other government and/or law enforcement agencies for ultimate disposition.

¹ The FTC is an independent agency with consumer protection law enforcement authority. Because the OIG contact information is prominent on the Agency's web site, consumers frequently misdirect their consumer protection complaints to the OIG, with the belief that the OIG has authority to investigate consumer fraud. The dramatic increase in the number of complaints received most likely stems from the addition of the OIG contact information to the OIG web site.

Of the remaining 33 complaints, OIG closed 32 without any action and one resulted in an investigation that remained ongoing at the end of this reporting period. The OIG opened another investigation as a result of an OIG audit undertaken during this semiannual reporting period.

Following is a summary of the OIG's investigative activities for the six-month period ending September 30, 2005:

| | |
|------------------------------------|------------|
| Cases pending as of 3/31/05 | 6 |
| PLUS: New cases | +2 |
| LESS: Cases closed | (2) |
| Cases pending as of 9/30/05 | 6 |

Investigations Closed

The OIG closed an investigation, opened in the prior reporting period, regarding allegations that an employee had visited pornographic websites and downloaded pornographic images onto his FTC Government computer, in violation of agency policy. Because some of the websites accessed by the employee (and some of the websites to which access was blocked) might contain images of minors, management referred the matter to the OIG. Management seized the employee's computer hard drive at the request of the OIG and transmitted the secured hard drive for OIG review. Using computer forensics analytical tools, the OIG reviewed the computer hard drive. The evidence did not support a referral to the Department of Justice for prosecution. We informed management of our investigative findings and closed the matter.

Another investigation that the OIG both opened and closed during this reporting period originated from an OIG audit. The OIG audit focused on the use of the Government issued travel credit card by employees within a specified agency organization. The audit disclosed that an employee in this organization had misused her Government-issued travel credit card by obtaining cash advances for personal use (unrelated to official Government travel). Credit card records indicated that the employee had paid the outstanding balances and related service fees in full (although such payments were typically delinquent). The OIG referred its investigative findings to management for further administrative action.

Matters Referred for Prosecution

During this reporting period the OIG referred one case to the Department of Justice for prosecution and throughout this reporting period, we have continued to assist the federal prosecutor in this ongoing prosecution. The OIG closed this investigation during the preceding reporting period.

OTHER ACTIVITIES

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 its response to 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.

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, upon request, affecting the operations of the OIG. During this reporting period, the OIG reviewed no legislation.

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 may also call the OIG's investigator directly on **(202) 326-2618**. A confidential or anonymous message can be left 24 hours a day. Complaints or allegations of fraud, waste or abuse can also be emailed directly to chogue@ftc.gov. OIG mail should be addressed to:

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

OIG reports can be obtained directly from the internet at: www.ftc.gov/oig. A visitor to the OIG home page can download recent (1996-2005) OIG semiannual reports to Congress, the FY 1998 - 2004 financial statement audits, and 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 Office of Inspectors General.

TABLE I: SUMMARY OF INSPECTOR GENERAL REPORTING REQUIREMENTS

| <u>IG Act Reference</u> | <u>Reporting Requirement</u> | <u>Page(s)</u> |
|--------------------------------|--|-----------------------|
| Section 4(a)(2) | Review of legislation and regulations | 9 |
| Section 5(a)(1) | Significant problems, abuses and deficiencies | 2-4 |
| Section 5(a)(2) | Recommendations with respect to significant problems, abuses and deficiencies | 2-4 |
| 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 | 8 |
| Section 5(a)(6) | List of audit reports by subject matter, showing dollar value of questioned costs and funds put to better use | 11, 12 |
| Section 5(a)(7) | Summary of each particularly significant report | 2-4 |
| Section 5(a)(8) | Statistical tables showing number of reports and dollar value of questioned costs | 11 |
| Section 5(a)(9) | Statistical tables showing number of reports and dollar value of recommendations that funds be put to better use | 12 |
| 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 | 11, 12 |
| 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

| | | <u>Dollar Value</u> | | |
|--------------------------|--|---------------------|-----------------------------|-----------------------------|
| | | <u>Number</u> | <u>Questioned Costs</u> | <u>Unsupported Cost</u> |
| A | For which no management decision has been made by the commencement of the reporting period | <u>0</u> | <u>0</u> | <u>(0)</u> |
| B | Which were issued during the reporting period | <u>0</u> | <u>0</u> | <u>(0)</u> |
| Subtotals (A + B) | | <u>0</u> | <u>0</u> | <u>(0)</u> |
| C | For which a management decision was made during the reporting period | <u>0</u> | <u>0</u> | <u>(0)</u> |
| | (i) dollar value of disallowed costs | <u>0</u> | <u>0</u> | <u>(0)</u> |
| D. | (ii) dollar value of cost not disallowed | <u>0</u> | <u>0</u> | <u>(0)</u> |
| | For which no management decision was made by the end of the reporting period | <u>0</u> | <u>0</u> | <u>(0)</u> |
| | Reports for which no management decision was made within six months of issuance | <u>0</u> | <u>0</u> | <u>(0)</u> |

**TABLE III: INSPECTOR GENERAL ISSUED REPORTS WITH
RECOMMENDATIONS THAT FUNDS BE PUT TO BETTER USE**

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