United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on Federal Services, Post Office and Civil Service, Committee on Governmental Affairs, U.S. Senate

May 1994

POSTAGE METERS

Risk of Significant Financial Loss But Controls Are Being Strengthened

GAO/GGD-94-148

GAO

United States
General Accounting Office
Washington, D.C. 20548

General Government Division

B-256737

May 26, 1994

The Honorable David Pryor
Chairman, Subcommittee on Federal
Services, Post Office and Civil Service
Committee on Governmental Affairs
United States Senate

Dear Mr. Chairman:

This report responds to your request that we review fraudulent postage meter activities. Your request followed the Postmaster General's public disclosure in 1993 that significant revenue losses had occurred as a result of meter fraud. You were interested in knowing (1) how long meter fraud had been occurring and whether it involved a specific type or brand of meter, (2) what conditions allowed the fraud to occur, and (3) what actions the Postal Service is taking to address the problem.

Results in Brief

Over the years, unscrupulous mailers have taken advantage of weaknesses in the metered mail program to avoid paying millions of dollars in postage. Since 1985, the Postal Inspection Service has closed more than 130 cases of meter fraud with documented losses totaling about $25 million. Another 28 cases were being investigated as of December 1993, potentially involving at least an additional $11 million. The variety of fraud schemes that have been successfully perpetrated in the meter program—which brought in about $21 billion of the $45.7 billion total postage revenue in 1993—and the significance of potential losses led the Postmaster General to state in September 1993 that revenue losses from fraud could be costing the Postal Service $100 million or more per year.[1]

Revenue losses stem from criminal tampering with postage meters, counterfeiting of meter indicia, and criminal use of lost or stolen meters to produce meter indicia for which postage was not paid. There have also been cases involving criminal use of malfunctioning meters to produce meter indicia for which postage was not paid. Of the 1.4 million postage meters in use as of November 1993, 636,000 meters (45 percent) made by Pitney Bowes and Ascom Hasler are vulnerable to tampering, according to the Postal Service.

[1]The Postal Service, in 1993, using available data on mail volume and revenue, estimated that its losses from meter fraud could be as high as $171 million annually. However, Postal officials have acknowledged that they do not have the data necessary to accurately determine total losses.

The risk of revenue losses from meter fraud are high because of weaknesses in meter design and ineffective program controls. The physical control devices built into meters—ascending and descending registers, lead seals, and key locks—have been circumvented. Also, ineffective program controls relating to meter licensing, inspections, and management information are not capable of preventing and/or identifying fraudulent postage meter activities.

Although the Postal Inspection Service initiated a number of meter fraud investigations on the basis of tips, and reported on problems in the late 1980s, Postal Service top management was slow in responding to the need for corrective actions. The responsible program office had not been adequately staffed, and postal officials said that top management, at the time, did not want to potentially hurt customer service by tightening controls over meters and metered mail. Postal officials also said that management did not feel a sense of urgency to make changes in the program because they believed the controls, at the time, were cost effective considering the few documented cases of meter fraud that involved significant losses.

The Postal Service has relied on meter manufacturers to help ensure that meters are properly designed and controlled to prevent fraud. However, through its testing program, the Postal Service has traditionally placed greater emphasis on meter durability than security. Therefore, the incentive for meter manufacturers to upgrade security was not as great as the incentive to ensure durability.

Recently, the Postal Service has undertaken a number of major initiatives, which, if properly implemented, have the potential to improve the meter program. For example, it established a high-level management team charged with cleaning up the meter program. That team has initiated a number of substantive changes and continues to develop other short- and long-term changes that will require management's attention and support for many years to correct the problem. These changes range from decertifying and/or retrofitting problem meters to developing technology that would allow the Postal Service to match postage received with the volume of mail processed. Until those changes are fully implemented and operating effectively, the Postal Service will not be able to substantially reduce the risk of losing revenue to meter fraud.

Background

Metered mail is the largest single source of revenue for the Postal Service—accounting for about $21 billion (46 percent) of the postage revenue in 1993 and 37 percent (55 billion pieces) of the total mail volume. When mailers purchase postage, meters with remote resetting capabilities are reset by the meter manufacturers, and meters without that capability are reset by postal clerks. Currently, four manufacturers lease Postal Service approved meters directly to mailers: (1) Pitney Bowes, (2) Ascom Hasler, (3) Friden Neopost, and (4) Postalia. Since the inception of the program in 1920, Pitney Bowes has been the dominant manufacturer, accounting for about 88 percent of the 1.4 million meters currently being used in the United States.

The nature of meters—i.e., the capability to print postage—has always made them targets of opportunity for fraud. For this reason, a number of device and program controls have been used to help ensure the integrity of the meters. Despite these controls, meter fraud has occurred over the years.

Additional background information on meters is presented in appendix I.

Objectives, Scope, and Methodology

Our objectives were to (1) determine how long meter fraud had been occurring and whether it involved a specific type or brand of meter, (2) examine the system of controls over meters that permitted the fraud to occur, and (3) identify management's ability to oversee the meter program in the past and identify recent management initiatives to address meter fraud problems.

To accomplish objectives one and two, we (1) researched the development of the postage meter program; (2) reviewed data from existing Postal Service audit and investigative reports, including automated files containing data on meter fraud investigations that have been closed since 1985; (3) reviewed the investigative folders for 11 of the most significant closed meter fraud cases; (4) interviewed cognizant Postal Service headquarters officials; (5) observed metered mail operations at a large Postal Service mail processing center; (6) interviewed representatives from Pitney Bowes—the dominant manufacturer of meters currently in use; (7) interviewed Postal Service managers who are responsible for approving meters for use; and (8) interviewed Inspection Service officials at the Postal Service crime laboratory who are responsible for examining meters when tampering is suspected. To identify the Postal Service's corrective actions, we documented, reviewed, and discussed with postal

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.