

POSTAL REGULATORY COMMISSION

OFFICE OF INSPECTOR GENERAL



FINAL EVALUATION REPORT

FOLLOW-UP REVIEW TO POSTAL REGULATORY COMMISSION'S HANDLING OF NONPUBLIC INFORMATION (REPORT #10-01-A01)

**Evaluation Report 16-01-A01
March 30, 2016**

Table of Contents

INTRODUCTION	1
BACKGROUND.....	1
OBJECTIVE, SCOPE AND METHODOLOGY	1
RESULTS	2

Introduction

Background

In fulfilling its role in regulating and overseeing the United States Postal Service, the Postal Regulatory Commission (PRC) requires the Postal Service to provide a wide range of information regarding its operations. Most filings with the PRC are a matter of public record, and are posted on the PRC's website (<http://www.prc.gov>). However, the Postal Accountability and Enhancement Act of 2006 allows the Postal Service to file certain types of information, including commercially sensitive information, under protective conditions.

Under 39 USC 504(g), the PRC is generally prohibited from disclosing this nonpublic information; however, outside parties in matters before the PRC may move for access to nonpublic information only for purposes of participating in the matter.

In 2010, the Postal Regulatory Commission Office of Inspector General (PRC-OIG) issued an inspection report entitled *Postal Regulatory Commission's Handling of Nonpublic Information (Report Number 10-01-A01)*. We identified two vulnerabilities which are noted below along with their corresponding recommendations:

1. The PRC provided no formal training to educate staff members on adequately safeguarding non-public information in their personal possession. Instead, Management provided an informal oral "overview" of adequate safeguarding and relied on the supervisors to enforce procedure for safeguarding nonpublic information filed with the PRC.

Recommendation 1: Develop a more comprehensive, formal training program in order to remind PRC staff of the security requirements for safeguarding nonpublic information.

2. The PRC did not have a formal procedure for reporting alleged compromises of nonpublic information.

Recommendation 2: Develop a method for reporting incidents where a possible compromise of nonpublic information occurs. In developing this plan, the PRC should consider provisions to ensure affected parties are notified, that the cause is determined, and that plans are made to prevent recurrence.

Objective, Scope and Methodology

The objective of this follow-up review was to determine if the recommendations made in our 2010 audit were implemented.

To accomplish our objectives, we reviewed available documentation, including

- PRC Standard Operating Procedures—Non-public Records Access
- Training Certification Form
- Procedures for Protected Material

We conducted this review between December 2015 and March 2016 in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspections and Evaluations*. We believe that the documentation obtained provides a reasonable basis for our conclusions based on our objectives.

Results

The follow-up review found that the PRC has effectively implemented all recommendations from our prior audit report.

The PRC has taken steps to educate and train staff, and have sent numerous e-mails to staff to stress the importance of protecting sensitive information.

The Commission's Standard Operating Procedures on protecting non-public information provide detailed guidance on controls for protecting this information and for notifying appropriate parties when a breach occurs. These procedures appear adequate.

The PRC informed us that in 2013 an incident occurred whereby nonpublic information may have been compromised. They also told us that they followed the incident report protocols that they implemented pursuant to our recommendations.

We do not offer any further recommendations.