



U.S. Securities and Exchange Commission
Office of Inspector General
Office of Audits

Improvements Needed in the Division of Enforcement's Oversight of Fund Administrators



September 30, 2015
Report No. 531

Executive Summary

Improvements Needed in the Division of Enforcement's Oversight of Fund Administrators Report No. 531 September 30, 2015

Why We Did This Audit

Protecting investors is a critical mission of the U.S. Securities and Exchange Commission (SEC, agency, or Commission). To meet this mission, the SEC collects disgorgement and penalty amounts from securities violators and returns monies to harmed investors. In some instances, the SEC uses third party fund administrators to distribute the monies collected. As of July 2015, 9 fund administrators were administering 77 distribution matters totaling over \$6.5 billion ordered. If internal controls over the collection and distribution processes are not designed or are not operating effectively, harmed investors may not receive the monies owed to them or receive them in a timely manner. Consequently, we assessed the Division of Enforcement's Office of Collections' (OC) and Office of Distributions' (OD) controls over collections and distributions to harmed investors, including oversight of fund administrators used in the distribution process.

What We Recommended

To improve oversight of fund administrators, comply with applicable laws and agency policy and requirements, and ensure that goals and objectives are met, we recommended that OD continue to assess the risks involved when using fund administrators and update its policies and procedures to document its responsibilities for oversight of fund administrators. We also recommended that OD work with the Office of Information Technology to review fund administrators' data security controls and complete the required security assessments and privacy impact assessments of fund administrators. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

What We Found

Consistent with the SEC's mission, the agency has established goals and objectives for collecting and distributing monies to harmed investors. The Government Accountability Office's *Standards for Internal Control in the Federal Government* provides a framework for using internal controls to meet such goals and objectives. Additionally, agency requirements and information security laws, such as the E-Government Act, which includes the Federal Information Security Management Act, apply to entities that act on behalf of the SEC, including third party fund administrators.

We did not identify concerns related to OC's controls over its collection efforts. In addition, we found that, in 2010, the SEC initiated a "Fund Administrator Project" to, among other things, improve processes for appointing fund administrators, resulting in the selection of nine fund administrators to implement SEC distributions for a period of 5 years. However, OD's oversight of fund administrators could be improved to more fully align with the *Standards for Internal Control in the Federal Government*. Specifically, we determined that some distribution plans required fund administrators to provide payment files to Commission staff for the staff's review and authorization or approval before distributing funds. In response to a draft of this report, Division of Enforcement officials stated that controls are in place to ensure that fund administrators have the responsibility to submit accurate payment files. However, OD did not clearly document in its policies and procedures (1) the steps it takes to review and accept payment files submitted by fund administrators, and (2) its responsibilities for fund administrator oversight generally. Policies and procedures should address risks identified and, based on those risks, establish controls designed to ensure Federal requirements and the goals and objectives of the agency are met. OD officials told us about a limited number of instances, some of which occurred before fiscal year 2010, in which fund administrators submitted and OD accepted inaccurate payment files and at least one case where a fund administrator made inaccurate payments to investors. According to OD officials, corrective payments were made to the underpaid investors in that case. However, the SEC's oversight of fund administrators could be improved by fully assessing and documenting the risks of relying on fund administrators and updating policies and procedures for fund administrator oversight to address risks.

Additionally, in some instances where the SEC designed internal controls for oversight of fund administrators, the SEC did not implement the internal controls. For example, fund administrators collect on the SEC's behalf harmed investors' personally identifiable information (PII), including investors' names, addresses, dates of birth, social security numbers, and bank information. Despite Federal and agency requirements to assess fund administrators' information security controls, the agency did not complete required assessments of fund administrators' information technology environments before relying on the fund administrators. As a result, the agency lacks assurance that fund administrators adequately protect investors' PII collected and maintained on behalf of the SEC. The Office of Information Technology plans to complete required assessments of all nine fund administrators by December 31, 2015.

For additional information, contact the Office of Inspector General at (202) 551-6061 or http://www.sec.gov/about/offices/inspector_general.shtml.

TABLE OF CONTENTS

Executive Summary i

Background and Objectives 1

 Background 1

 Objectives 8

Results 9

 Oversight of Fund Administrators Needs Improvement..... 9

 Recommendations, Management’s Response, and Evaluation of Management’s Response 17

Figures

 Figure 1. Amounts Ordered and Collected and the Number of Filed Enforcement Actions FY 2004 – FY 2014 2

 Figure 2. The SEC’s Mission, Strategic Goals, Strategic Objectives, and Performance Goals and Indicators Related to Collections and Distributions 4

 Figure 3. Achieving Objectives Through Internal Controls 10

 Figure 4. Source of Harmed Investor PII..... 16

Tables

 Table 1. History of the SEC’s Ability To Seek Disgorgements and Make Distributions to Harmed Investors 3

 Table 2. Examples of Remedies and Funds Available for SEC Violations 5

 Table 3. Fund Administrator Pool Activity as of July 2015..... 6

 Table 4. Summary of Sampled Enforcement Actions 22

Appendices

 Appendix I: Scope and Methodology 19

 Appendix II: Management Comments..... 24

 Appendix III: OIG’s Response to Management Comments 26

ABBREVIATIONS

C.F.R.	Code of Federal Regulations
Enforcement	Division of Enforcement
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Management Act
FY	fiscal year
GAO	Government Accountability Office
IDC	Independent Distribution Consultant
IT	information technology
OC	Division of Enforcement, Office of Collections
OD	Division of Enforcement, Office of Distributions
OIG	Office of Inspector General
OIT	Office of Information Technology
PII	personally identifiable information
SEC or agency	U.S. Securities and Exchange Commission
U.S.C.	United States Code
USPIS	U.S. Postal Inspection Service

Background and Objectives

Background

Every year, thousands of U.S. investors lose money to fraudulent investment schemes. The U.S. Securities and Exchange Commission (SEC, agency, or Commission) prosecutes violations of Federal securities laws and holds violators accountable through appropriate sanctions and remedies. When the SEC brings a successful action against an individual or entity, the individual or entity may be required to disgorge the funds (give up the ill-gotten gains) resulting from the illegal conduct.

The SEC's Division of Enforcement (Enforcement) is responsible for collecting disgorged funds and penalties and distributing them in a fair, reasonable, and cost-effective manner to investors who were harmed by securities violations. Between fiscal year (FY) 2004 and FY 2014, there have been 7,415 filed enforcement actions and more than \$31 billion of disgorgements and penalties ordered, including more than \$4 billion in FY 2014 alone.

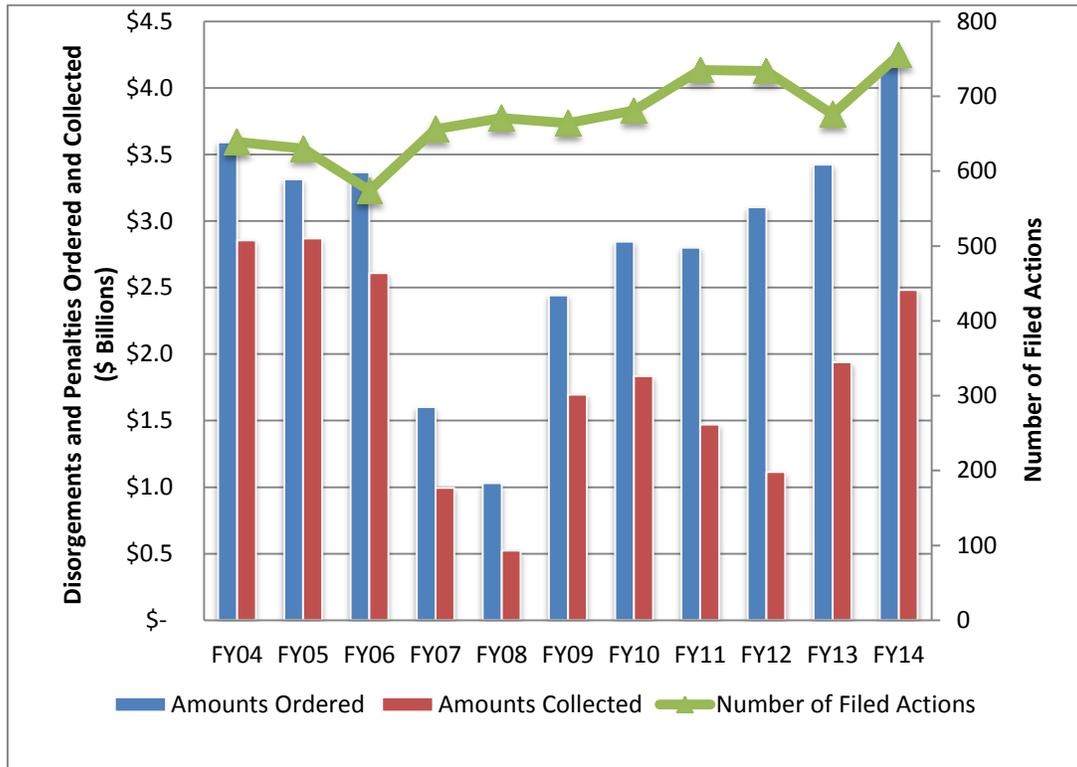
The SEC generally is authorized to bring its enforcement cases in either a civil action in Federal District Court or a Commission administrative proceeding before an administrative law judge. Depending on the type of action, the SEC appoints a third party fund administrator or recommends a distribution agent,¹ or a Federal District Court appoints a receiver to distribute disgorgements and penalties collected to harmed investors.² If internal controls over the collection and distribution process, including the oversight of fund administrators, are not designed or are not operating effectively, harmed investors may not receive the monies owed to them or receive them in a timely manner.

Figure 1 shows the number of filed enforcement actions and related amounts ordered and collected for actions between FY 2004 and FY 2014.

¹ A "fund administrator" is used in SEC administrative proceedings; "distribution agents" are used in District Court cases. The SEC may appoint a fund administrator in SEC administrative proceedings and may recommend for appointment a distribution agent in District Court cases. For the purposes of this report, unless otherwise noted, "fund administrator" refers to fund administrators and distribution agents.

² In some instances, SEC staff administers the distribution.

Figure 1. Amounts Ordered and Collected and the Number of Filed Enforcement Actions FY 2004 – FY 2014



Source: Office of Inspector General (OIG) analysis based on information from the SEC’s financial management system, Delphi, as of March 2015 and Select SEC and Market Data Reports FY 2004 – FY 2014.

Not all SEC enforcement actions result in a distribution to harmed investors. Between FY 2010 and FY 2014, the agency filed 3,581 enforcement actions. Approximately half of the filed actions, or 1,784, included ordered monetary relief. At the time of recommendation, the staff contemplated a possible distribution in 348 of these actions. Ultimately, 198 of these actions resulted in an actual distribution that was completed or is currently in progress. Furthermore, depending on the case, enforcement actions that result in the collection of disgorgements and penalties may be distributed to: (1) harmed investors, (2) the SEC’s Investor Protection Fund,³ or (3) the U.S. Treasury.

SEC’s Mission and History of Distributions to Harmed Investors. Congress established the SEC in 1934 to enforce Federal securities laws, promote stability in the markets and, most importantly, protect investors. The SEC’s authority to seek disgorgement in judicial actions was recognized in 1971 when the United States Court of Appeals for the Second Circuit, held that “the SEC may seek other than injunctive

³ Section 922 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, Title IX, § 922, 124 Stat. 1641 (2010) (codified as amended at 15 U.S.C. § 78u-6 (2012)), established the SEC Investor Protection Fund, which is funded through disgorgements and penalties that are not distributed to harmed investors. The SEC uses the Fund in certain circumstances to pay whistleblowers who give tips to aid the SEC’s enforcement efforts and to cover the expenses of the SEC OIG Employee Suggestion Program.

relief in order to effectuate the purposes of the [Securities Exchange Act of 1934], so long as such relief is remedial relief and is not a penalty assessment.”⁴ Thereafter, several Federal laws have reaffirmed and expanded the SEC’s authority to seek and distribute disgorgement and penalty amounts in both District Court cases and administrative proceedings. Table 1 provides additional details.

Table 1. History of the SEC's Ability to Seek Disgorgements and Make Distributions to Harmed Investors

Authority	Description
<i>Securities and Exchange Commission v. Texas Gulf Sulphur Co.</i> ⁵	Recognized the SEC’s ability to seek disgorgements in Federal District Courts for violations of the Securities Exchange Act of 1934.
Securities Enforcement Remedies and Penny Stock Reform Act of 1990 ⁶	Amended the (1) Securities Act of 1933, (2) Securities Exchange Act of 1934, (3) Investment Company Act of 1940, and (4) Investment Advisers Act of 1940. This law established the SEC’s authority to order disgorgement as a remedy in administrative proceedings and to distribute the disgorged funds to harmed investors. In addition, this law gave the SEC power to impose penalties against certain regulated entities and individuals through administrative proceedings and authorized the SEC to adopt rules and regulations for payments to harmed investors. ⁷
SEC’s Rules of Practice and Rules on Fair Fund and Disgorgement Plans ⁸	Among other things, these rules, as authorized by the Securities Enforcement Remedies and Penny Stock Reform Act of 1990, provide the procedures for payment of disgorgements and penalties to harmed investors.
Sarbanes-Oxley Act of 2002 ⁹	Section 308(a) of this law gave the SEC the power to distribute penalties to harmed investors by authorizing the creation of Fair Funds. Fair Funds allow penalties to be added to disgorgement funds for distribution to harmed investors.
Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ¹⁰	Section 929B of this law amended Section 308(a) of the Sarbanes-Oxley Act of 2002 and allows the SEC to distribute penalties to harmed investors; penalties no longer have to be included with disgorgements for distribution.

Source: OIG analysis of judicial decisions and Federal laws.

⁴ *Sec. & Exch. Comm’n v. Texas Gulf Sulphur Co.*, 446 F.2d 1301, 1308 (2d Cir. 1971).

⁵ *Id.*

⁶ Pub. L. 101-429, 104 Stat. 931 (1990) (codified as amended in scattered sections of 15 U.S.C.).

⁷ *Id.* at §§ 102(e), 202, 203, 301, and 401.

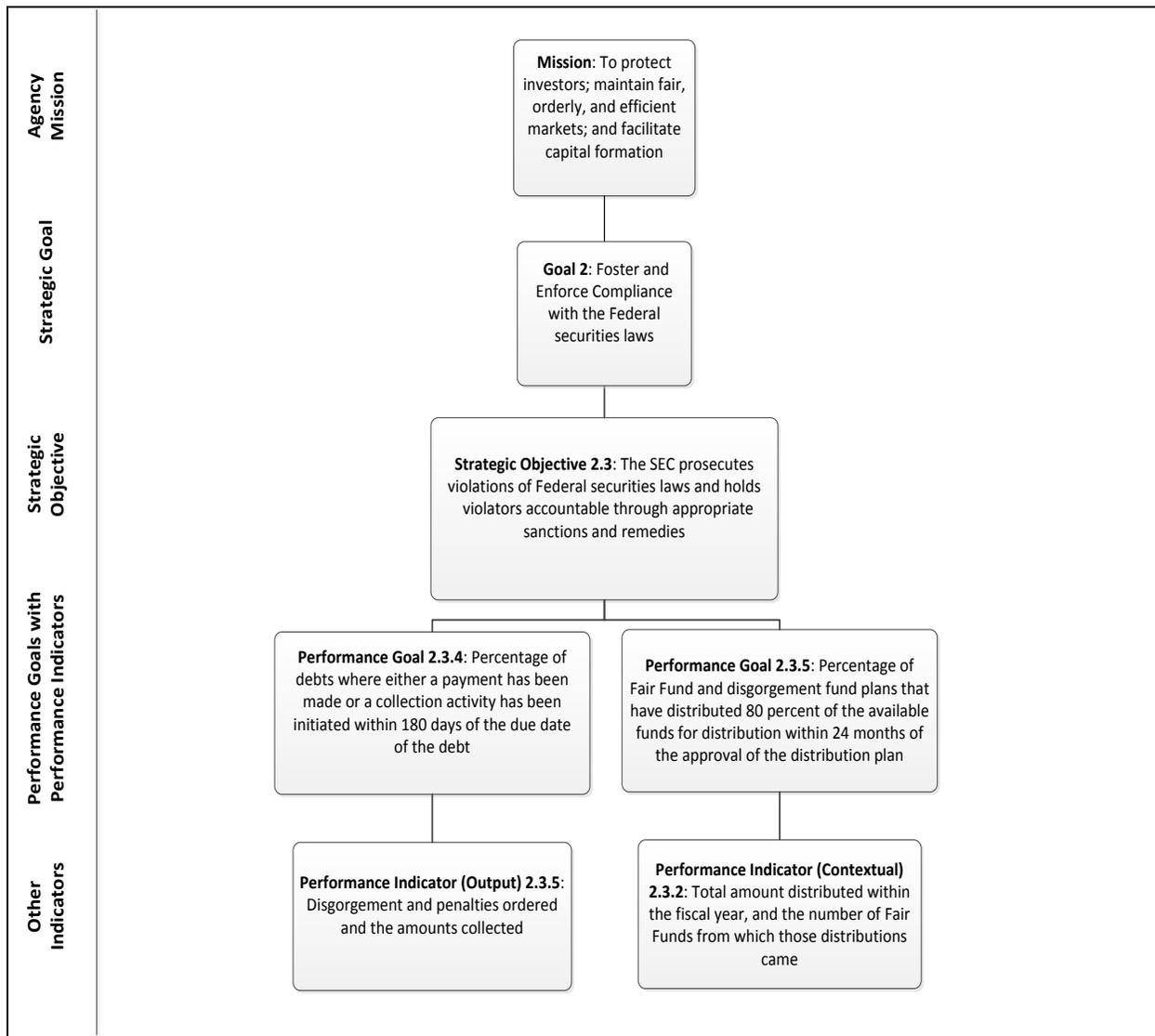
⁸ 17 C.F.R. Pt. 201, Subparts D and F (2015).

⁹ Sarbanes-Oxley Act of 2002 (Public Company Accounting Reform and Investor Protection Act) Pub. L. 107-204, 116 Stat. 745 (2002) (codified as amended in scattered sections of 15 U.S.C. and 18 U.S.C.).

¹⁰ Section 929B of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, Title IX, § 929B, 124 Stat. 1641 (2010) (codified as amended at 15 U.S.C. § 7246(a) (2012)).

To help fulfill its mission of protecting investors, the SEC established a strategic goal of fostering and enforcing compliance with Federal securities laws. As stated in the agency’s Annual Performance Reports and strategic plan for FY 2014 through FY 2018, the strategic objective to meet this goal is for the SEC to prosecute violations of Federal securities laws and hold violators accountable through appropriate sanctions and remedies. Figure 2 shows the relationship between the SEC’s mission, strategic goals, strategic objectives, and performance goals and indicators related to the collection and distribution of disgorgements and penalties.

Figure 2. The SEC’s Mission, Strategic Goals, Strategic Objectives, and Performance Goals and Indicators Related to Collections and Distributions



Source: OIG-generated based on the SEC’s FY 2014 Annual Performance Report and FY 2016 Annual Performance Plan.

On finding that a defendant has violated securities laws, the court or administrative law judge can issue a judgment ordering sanctions such as civil monetary penalties and disgorgement. Table 2 provides more information on some of the remedies available to a Federal District Court or an administrative law judge.

Table 2. Examples of Remedies and Funds Available for SEC Violations

Remedy / Fund	Description
Civil Monetary Penalty	A remedial measure aimed at deterring future misconduct.
Disgorgement	An equitable remedy aimed at preventing a wrongdoer from unjust enrichment from wrongdoing; deprives violators of “ill-gotten gains” linked to the wrongdoing. The SEC does not have to prove an exact amount but must show the estimate is reasonable.
Disgorgement Fund	A fund created for the benefit of harmed investors from the collection of a disgorgement order imposed on a securities law violator.
Fair Fund	A disgorgement fund that also includes a civil monetary penalty imposed on the securities law violator.

Source: OIG summary of the Government Accountability Office’s (GAO) report, GAO-05-670, *SEC and CFTC Penalties* (2005).

Evolution of the SEC’s Collection and Distribution Program. Since the SEC began distributing monies, the Commission has appointed fund administrators to develop, oversee, and/or implement distribution plans. During the 1990s, the SEC’s practice was to recommend only staff members to serve as fund administrators in administrative proceedings. Before a series of complex cases beginning in 2004, the Commission appointed few third parties as fund administrators. Between 2004 and 2010, the SEC used third party fund administrators¹¹ on a case-by-case basis. In 2010, the SEC initiated a “Fund Administrator Project” to:

- improve the efficiency and timeliness of the appointment of fund administrators;
- standardize the selection, oversight, and performance of fund administrators;
- improve staff’s ability to obtain and analyze distribution data; and
- forecast the feasibility and cost effectiveness of distributions generally.

In 2013, Enforcement selected a pool of nine fund administrators to implement SEC distributions for a period of 5 years. The agency may appoint or recommend that a

¹¹ Henceforth in this report, the term “fund administrators” refers to third party fund administrators.

court appoint one of the nine fund administrators in the pool to execute distributions related to filed enforcement actions. To set up its pool and select fund administrators, the agency used the Federal Acquisition Regulation (FAR) process for procuring goods and services as a best practice or comparable framework.¹² Because the monies involved in the distribution process are not appropriated funds, the agency is not required to follow the FAR when overseeing fund administrator performance.

Table 3 shows the number and ordered dollar amount of distributions that each fund administrator is administering as of July 2015.

Table 3. Fund Administrator Pool Activity as of July 2015

Fund Administrator	Number of Distribution Matters	Ordered Amount of Funds
1	10	\$1,248,865,822
2	4	\$1,873,000,000
3	3	\$105,368,414
4	4	\$17,082,089
5	23	\$2,168,473,243
6	4	\$20,094,938
7	17	\$689,258,183
8	8	\$396,368,932
9	4	\$56,601,466
Total	77	\$6,575,113,087

Source: OIG-generated based on information provided by Enforcement.

Organizational Roles and Responsibilities. On February 7, 2008, in response to the additional authority to distribute disgorgement and penalty amounts under the Sarbanes-Oxley Act of 2002, the then SEC Chairman appointed the leaders of a new Office of Collections and Distributions within Enforcement. The purpose of the Office of Collections and Distributions was to expedite the return of funds to harmed investors and to reduce the cost of distributions. During FY 2011, Enforcement separated the Office of Collections and Distributions into two offices: the Office of Collections (OC) and the Office of Distributions (OD). OC has specific responsibilities for collecting disgorgement and penalty amounts whereas OD has specific responsibilities for distributing disgorgement and penalty amounts.

Office of Collections. OC's responsibilities include collecting delinquent debts arising from actions to enforce the Federal securities laws, pursuing litigation to enforce judgments, and, in some instances, referring delinquent debt to the U.S. Treasury. OC

¹² The FAR applies only to the acquisition with appropriated funds of supplies and services for the use of the Federal Government. See FAR 2.101.

is composed of 11 employees, including trial attorneys and paralegals. OC's *Guidelines for the Collection of Delinquent Debt*, dated April 21, 2015, document OC's policies and procedures for its collection activities. This document includes OC's policies and procedures for enforcing judgments through litigating, searching for assets, and referring debt to the U.S. Treasury; the document also details OC's collection efforts in District Court actions and administrative proceedings.

Office of Distributions. OD handles all distributions in enforcement actions where a disgorgement or Fair Fund is created. Specific services OD provides include, but are not limited to:

- soliciting proposals and recommending fund administrators;
- reviewing and approving all invoices from fund administrators;
- drafting and submitting documents to the Commission or District Court for all distribution-related actions;
- facilitating final fund accountings and closing out funds;
- collecting and analyzing distribution-related metrics; and
- managing cost-effective, efficient, and fair and reasonable distributions of money to harmed investors.

OD also reviews and accepts payment files submitted by fund administrators. Before distributing money to harmed investors, a fund administrator prepares and submits to OD a list of payees and amounts to be distributed to those payees. The fund administrator provides OD a validation/reasonable assurances letter stating that the payment file was prepared in accordance with the Commission-approved distribution plan. In some cases the payment files are voluminous. Consequently, the agency determined that the payment files would not be easily examined or reviewed for accuracy and completeness by the Commission itself or by Commission staff without the aid of sampling techniques or technological assistance. Thus, OD relies on the fund administrator's validation/reasonable assurances letter for the completeness and accuracy of the payment file.

However, we identified language in distribution plans approved by order of District Courts and a Commission administrative proceeding that required the SEC to review and accept payment files before funds were distributed. For example, one such document stated, "The Distribution Agent shall provide the final payee list to the Commission staff, and upon **review**, [emphasis added] the Commission staff shall move the Court to transfer all funds. . ." Another distribution plan for a District Court case stated, "The Fund Administrator shall provide the Final Payee List to Commission staff for **review** [emphasis added]. The Fund Administrator shall distribute the Distribution Fund according to the Final Payee List once it receives written **authorization** [emphasis added] from Commission staff to do so." Finally, a distribution plan for an

administrative proceeding stated, “Upon receipt and **review** [emphasis added] of the validated list, and upon **approval** by the Commission [emphasis added], the Commission staff will direct the release of funds . . .” OD officials explained that OD’s review consists of identifying typos and duplicate entries and confirming the mathematical accuracy of the payment file. In distributions of more than \$25 million, OD may require an independent review of the claims process. Additionally, according to OD and as stated in Rule 1105 of the SEC’s Rules on Fair Funds and Disgorgement Plans, unless waived by the Commission, fund administrators in administrative proceedings are required to obtain a bond that covers errors, including errors resulting from fraud. Thus, the bond acts as a method to mitigate the financial consequences of errors within the distribution process, such as instances of inaccurate payments.

OD is composed of 11 employees including attorneys, paralegals, and management and program analysts. OD’s *Distributions Manual*, dated August 15, 2013, documents OD’s policies and procedures for distribution activities. Among other things, the manual provides the policies and processes for selecting fund administrators, processing and paying expenses related to administering distributions, monitoring distribution fund accounting, and evaluating and managing claims.

Objectives

Our objectives were to assess:

- the SEC’s policies, procedures, and efforts for collecting disgorgement and penalty funds and accurately and timely distributing those funds to harmed investors; and
- the SEC’s policies, procedures, and controls for overseeing the work of third party entities used in the distribution process.

We did not identify concerns with OC’s controls over the collections process. However, as this report describes, we determined that improvements are needed in OD’s oversight of fund administrators used in the distribution process.

Appendix I includes additional information on our scope and methodology, review of internal controls, prior coverage, applicable Federal laws and guidance, and SEC policies and procedures.

Results

Oversight of Fund Administrators Needs Improvement

Enforcement's OD is responsible for overseeing the distribution of disgorgement and penalty amounts to investors harmed by securities fraud or other securities law violations. One of OD's goals is to ensure distributions are made in a fair, reasonable, and cost-effective manner. In some instances, OD relies on fund administrators to return disgorgement and penalty amounts to harmed investors. Although the SEC initiated a "Fund Administrator Project" to improve distribution processes and established a pool of nine fund administrators to implement SEC distributions for a period of 5 years, OD's oversight of fund administrators could be improved to more fully align with the *Standards for Internal Control in the Federal Government*. Specifically, OD did not fully assess the risks resulting from its reliance on fund administrators and, based on that risk assessment, clearly document in its policies and procedures (1) the steps it takes to review and accept payment files submitted by fund administrators, and (2) its responsibilities for fund administrator oversight generally. Additionally, the agency did not complete required assessments of fund administrators' information security controls before using fund administrators to distribute monies to harmed investors. Therefore, the SEC lacks assurance that fund administrators are adequately protecting the confidentiality and integrity of investors' personally identifiable information (PII) collected and maintained on behalf of the agency in the course of the distribution process.

SEC Goals and Objectives and Applicable Laws and Requirements

Consistent with the agency's mission, the SEC has established goals and objectives for collecting and distributing monies to harmed investors. As described below, GAO's *Standards for Internal Control in the Federal Government* provides a framework for using internal controls to meet such goals and objectives.¹³ Additionally, certain information security laws and agency requirements apply to entities that act on behalf of the SEC, including fund administrators.

SEC Goals and Objectives. As previously discussed, the SEC has established specific strategic goals and performance objectives and indicators for collecting and distributing disgorgements and penalties to harmed investors. Consistent with the agency's mission and strategic plan, the Director of Enforcement recently reaffirmed

¹³ U.S. Government Accountability Office, GAO/AIMD-00-21.3.1, *Standards for Internal Control in the Federal Government* (1999). In September 2014, GAO revised the standards, issuing GAO-14-704G. The revised standards are not effective until FY 2016, although agency management may adopt them earlier.

Enforcement's commitment to these goals and objectives. On March 19, 2015, the Director stated in testimony before the U.S. House of Representatives Committee on Financial Services, Subcommittee on Capital Markets and Government Sponsored Enterprises, that "Enforcement is responsible for the collection of monies owed as a result of legal action brought by the Commission, as well as the distribution of monies to harmed parties whenever practicable in a fair, reasonable, and cost-effective, [sic] manner."¹⁴ As Figure 3 shows, GAO's *Standards for Internal Control in the Federal Government* provides the overall framework for establishing and maintaining an effective internal control system and specifies that agencies use internal controls to help achieve objectives like the ones established by the SEC.

Figure 3. Achieving Objectives Through Internal Controls



Source: U.S. Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (2014).

These Federal internal control standards include components and principles of internal control to implement Federal requirements, including the following aspects of assessing risk and designing control activities to respond to risks:

- **Risk Assessment:**
 - Management should define objectives clearly to enable the identification of risks and define risk tolerances.
 - Management should identify, analyze, and respond to risks related to achieving the defined objectives.
 - Management should consider the potential for fraud when identifying, analyzing, and responding to risks.
 - Management should identify, analyze, and respond to significant changes that could impact the internal control system.
- **Control Activities:**
 - Management should design control activities to achieve objectives and respond to risks.
 - Management should design the entity's information system and related

¹⁴ *Oversight of the SEC's Division of Enforcement: Hearing Before the H. Comm. on Financial Services, 114th Cong. (2015)* (statement of Andrew Ceresney, Director, Division of Enforcement, U.S. Securities & Exchange Commission).

control activities to achieve objectives and respond to risks.

- Management should implement control activities through policies.

The E-Government Act and FISMA. The E-Government Act of 2002, which includes the Federal Information Security Management Act (FISMA), amends Chapter 35 of Title 44 of the United States Code (U.S.C.) and provides a framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.¹⁵ Specifically, 44 U.S.C. § 3554 (2012) states that the head of each agency is:

responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or **on behalf of the agency** [emphasis added] and information systems used or operated by... [an] organization **on behalf of an agency** [emphasis added].

FISMA also requires each agency to develop, document, and implement an agency-wide information security program to provide information security over the information and information systems that support the operations and assets of the agency. This information security program includes periodic security assessments of the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, and modification or destruction of information and information systems that support the operations and assets of the agency. Such operations and assets include those provided or managed by another agency, contractor, or other source. Furthermore, Section 208 of the E-Government Act of 2002 states that each agency should conduct privacy impact assessments before initiating a new collection of information that will be collected, maintained, or disseminated using information technology (IT) including any information in an identifiable form.¹⁶

SEC OIT Security Policy. The SEC's Office of Information Technology (OIT) Security Policy Framework Manual 24-04-08-06-FM (Rev. 2), May 13, 2015, (SEC OIT Security Policy) also requires security assessments and an authorization process for fund administrators' IT environments.¹⁷ The authorization process requires OIT to assess the security controls in the fund administrator's information system and produce a report that documents the results of the assessment. The results are provided to a designated authorizing official, who is a senior-level executive or manager selected by the Chief

¹⁵ Pub. L. 107-347, Dec. 17, 2002, 116 Stat. 2899 (codified as amended in scattered sections of Titles 5, 10, 13, 31, 40, and 44 of U.S.C.). On December 18, 2014, FISMA was largely superseded by the Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073 (2014) (codified as amended at 44 U.S.C. §§ 101, 3531-38, 3541-49 and 3551-58).

¹⁶ Codified at 44 U.S.C. § 3501 note (2012).

¹⁷ When the fund administrator pool was established in 2013, the effective OIT policy, SEC OIT Security Policy Framework, August 7, 2012, also required security assessments and an authorization process.

Information Officer, to make a risk-based decision on whether to authorize use of the information system. The authorizing official for the SEC's fund administrator pool is Enforcement's Managing Director.

Additionally, to establish the pool, OD required fund administrators interested in supporting the SEC in the distribution process to respond to a statement of requirements document.¹⁸ The document required each fund administrator to submit several items that OD then used to select the pool. Section 6 of the document stated that each fund administrator selected for the pool would be required to protect the data it collects. OD's requirements document also required that each fund administrator demonstrate compliance with security and privacy regulations pertinent to the fund administrator's respective industry or profession by submitting a third party assessment of compliance.

Finally, when OD requested that the Commission approve the pool of fund administrators, it was agreed that OIT would (1) conduct periodic IT security evaluations to determine whether each fund administrator is compliant with FISMA (as required in the statement of requirements document), and (2) inform OD of substantial instances of noncompliance requiring suspension of distribution activity or removal from the pool.

Weaknesses in Oversight of Fund Administrators

OD's oversight of fund administrators was not consistent with the *Standards for Internal Control in the Federal Government* because the agency did not assess fully the risks resulting from its reliance on fund administrators and, based on that risk assessment, establish appropriate internal controls to respond to risks. Also, in some instances where the SEC designed internal controls for oversight of fund administrators' information security controls, the SEC did not implement the internal controls. We reviewed Enforcement's risk control matrix, which describes certain control activities that are designed to help ensure that physical documents containing PII are protected from unauthorized access. Additionally, the SEC addressed certain risks of using fund administrators by initiating a "Fund Administrator Project" in 2010, partially to improve performance and oversight of fund administrators. Notwithstanding the risks identified in Enforcement's risk control matrix, OD did not clearly document in its policies and procedures (1) the steps it takes to review and accept payment files submitted by fund administrators, and (2) its responsibilities for fund administrator oversight generally.

Policies and procedures should address risks identified and, based on those risks, establish controls designed to ensure the goals and objectives of the agency (for example, distribution of monies to harmed parties in a fair, reasonable, and cost-effective manner) and Federal requirements (for example, the E-Government Act of 2002) are met. OD officials told us about a limited number of instances, some of which

¹⁸ *Statement of Requirements, Distribution Fund Administration Services – Office of Collections and Distributions* (2011).

occurred before FY 2010, in which fund administrators submitted and OD accepted inaccurate payment files and at least one case where a fund administrator made inaccurate payments. According to OD officials, corrective payments were made to the underpaid investors in that case. However, the SEC's oversight of fund administrators could be improved by fully assessing and documenting the risks involved when using fund administrators and updating policies and procedures for fund administrator oversight.

Additionally, the agency did not ensure that fund administrators' information security controls were assessed, as required by the E-Government Act, including FISMA, and certain agency policies and requirements. Therefore, the SEC lacks assurance that fund administrators are adequately protecting the confidentiality and integrity of investors' PII collected and maintained on behalf of the agency in the course of the distribution process.

Fund Administrators Submitted and OD Accepted Inaccurate Payment Files. We reviewed a sample of 13 filed enforcement actions from FY 2010 through FY 2014 where distributions were made. In some cases, the SEC authorizes a payment to harmed investors in accordance with the payment file submitted by the fund administrator. In other cases, the SEC or the District Court transfers the funds to the fund administrator after reviewing the payment file. We tested the sample of actions to assess (1) the SEC's policies, procedures, and efforts for collecting disgorgement and penalty funds and accurately and timely distributing those funds to harmed investors; and (2) the SEC's policies, procedures, and controls for overseeing the work of third party entities used in the distribution process.

We did not identify any inaccurate payments specific to the cases in our sample. However, OD officials told us about a limited number of instances, some of which occurred before FY 2010, in which fund administrators submitted and OD accepted inaccurate payment files and at least one case where a fund administrator made inaccurate payments. These instances occurred after the fund administrators provided the SEC with assurances that payment files were accurate. Moreover, two of the instances involved payments of fraudulent claims. Nonetheless, the type of review performed of payment files is not documented in OD's policies and procedures. In addition, OD did not assess or change the steps OD performs to review payment files submitted by fund administrators as a result of the instances described below.

- In 2009, Fund Administrator 3's Independent Distribution Consultant (IDC)¹⁹ submitted an inaccurate payment file to OD. The payment file did not include six omnibus accounts eligible for \$5.5 million in distributions.²⁰ OD did not identify

¹⁹ According to OD officials, fund administrators can use an IDC to identify harmed investors when harmed investors are not easily identifiable, such as in market timing cases.

²⁰ An "omnibus account" is an account in which a financial institution serving as an intermediary is the shareholder of record and holds securities on behalf of the actual beneficial owners.

the error. Rather, the fund administrator's IDC informed SEC staff of the omission after OD accepted the file. Because the IDC identified the issue before the fund administrator made the payments, the Commission withdrew the order to distribute funds, and the fund administrator did not make any payments.

- In 2013, Fund Administrator 8 miscalculated the amount of money to be paid to harmed investors. The miscalculation occurred because the fund administrator treated blank cells in an electronic Microsoft Excel file submitted by an insurance company as "missing" information and filled in these perceived "gaps" with the previous year-end holdings data. This resulted in inaccurate payment amounts for about 76 percent of the claims in the payment file. Although OD reviewed and accepted Fund Administrator 8's payment file, OD did not identify the miscalculation. Rather, Fund Administrator 8 brought the issue to the SEC's attention after the staff's acceptance of the payment file but before distribution of payments. No inaccurate payments were made in the distribution, and the SEC received all funds (over \$20 million) from Fund Administrator 8. According to OD officials, Fund Administrator 8 will complete the distribution after an independent auditor validates Fund Administrator 8's revised calculations.
- In 2009, a subcontractor of an IDC used by Fund Administrator 5 programmed incomplete subaccount information that resulted in Fund Administrator 5 making inaccurate payments from a Fair Fund, which provided over \$220 million to more than 2 million harmed investors. After making the payments, Fund Administrator 5 received disputes from harmed investors about the amounts of settlement checks. Specifically, identical twins with the same investments received settlement checks for different amounts and, therefore, questioned the accuracy of the settlement. Fund Administrator 5's IDC and its subcontractor subsequently identified about 168,000 accounts that were overpaid by \$8.85 million and 157,000 accounts that were underpaid or not paid by \$8.44 million. Before Fund Administrator 5 distributed the money, OD had accepted the payment file.

SEC staff and the IDC believed that attempts to recover overpayments already in the hands of accountholders would pose significant problems. Although corrective payments were made to the underpaid investors, neither OD nor the fund administrator attempted to retrieve settlement checks already cashed by overpaid accountholders.

- *Fraudulent Claims.* Beginning in October 2002, an inmate at a Federal Correctional Institution began filing fraudulent proofs of claim in connection with at least five disgorgement funds established in enforcement actions brought by the Commission. The inmate submitted claims of about \$1 million. However, the fund administrator made only one payment in the amount of \$51,000 from a disgorgement fund to the inmate. The Federal Bureau of Investigation and SEC staff prevented payments to the inmate from two other SEC disgorgement funds and, in the remaining two SEC cases, the fund administrator denied the inmate's

claims due to inadequate documentation. To demonstrate that he had suffered a “loss” in connection with his claims, the inmate submitted falsified Schedule D forms purportedly from his income tax return for the relevant year(s). On the falsified Schedule D forms, the inmate represented that he had engaged in the purchase and sale of the securities at issue. A U.S. Attorney’s Office charged the inmate with mail fraud in connection with his fraudulent claims, including his successful claim in the SEC matter.

- In another case, neither a fund administrator nor the SEC identified three fraudulent claims submitted in 2008 resulting in the fund administrator distributing about \$227,000 to improper claimants. These payments, which were part of a larger distribution, were uncovered by the U.S. Postal Inspection Service (USPIS) during its investigation of a fraudulent check-cashing scheme. After USPIS investigated the issue, it determined that the fund administrator should not have made the distributions and that the applicable claims were part of a complex fraud scheme. In this distribution, the fund administrator required claimants to provide a proof of claim document evidencing the stock purchase. The claimants in question submitted proof of claim documents falsely stating that they were entitled to funds and attached fabricated records stating that the claimants had purchased the stock.

According to OD officials, in total, these instances resulted in approximately \$9,128,000 in misdirected or overpaid funds, which reduced the amount remitted to the U.S. Treasury. Further, OD officials told us this amount represents only about .09128 percent of the total funds returned to harmed investors during the period. However, OD’s processes did not identify these instances and OD did not change or further document its process for reviewing and accepting payment files submitted by fund administrators as a result of these instances. Additionally, OD did not perform a risk assessment of its reliance on fund administrators as a result of these instances. Therefore, additional instances of inaccurate payments could exist.

The Agency Did Not Ensure Fund Administrators’ Information Security Was Assessed. Another aspect of overseeing fund administrators is ensuring that sensitive, nonpublic information in the possession of fund administrators is adequately protected. Although the SEC had designed certain internal controls to meet this objective, the agency did not ensure that the controls were implemented and that fund administrators’ information security was assessed, as required by the E-Government Act, including FISMA, and certain agency policies and requirements.

As shown in Figure 4, the SEC provides, and fund administrators collect on the SEC’s behalf, harmed investors’ PII. Such PII includes investors’ names, addresses, dates of birth, social security numbers, and bank information. OD officials stated that, in the last 3 years, the agency provided PII directly to fund administrators in only five cases, but fund administrators regularly collect PII as part of administering the claims and distribution process. Despite Federal and agency requirements to assess fund administrators’ information security controls, the agency did not complete required

security assessments and privacy impact assessments of fund administrators’ IT environments or obtain approval from an authorizing official before using the fund administrators. OIT has developed a plan to complete required assessments of all nine fund administrators by December 31, 2015 – more than 2 years after the SEC selected the fund administrators for the SEC’s pool.

Figure 4. Source of Harmed Investor PII



Source: OIG-generated based on review of a memorandum to the Commission.

Moreover, the statement of requirements document required each fund administrator to demonstrate compliance with security and privacy regulations by providing an independent third party assessment of compliance. As of the date of this report, the SEC has third party assessments of all fund administrators’ data security controls. However, the SEC did not receive or thoroughly review the assessments before allowing the fund administrators into the pool or relying on them to perform distributions. Additionally, the assessment provided by Fund Administrator 7 on August 1, 2014, identified data security control deficiencies; however, the agency did not act on the information provided by Fund Administrator 7 or request additional information to thoroughly review the issue. Despite this issue, the agency recommended Fund Administrator 7 for the pool, used the fund administrator throughout our audit period of FY 2010 through FY 2014, and continues to use the fund administrator as of the date of this report.

Because the SEC did not complete required IT security assessments and privacy impact assessments of fund administrators, the agency did not comply with applicable sections of the E-Government Act, including FISMA. In addition, because the SEC did not obtain approval from an authorizing official before using fund administrators in the distribution process, the agency did not comply with its own OIT Security Policy. Finally, because the agency did not receive or thoroughly review third party assessments of fund administrators’ data security controls before allowing fund administrators into the pool, it did not ensure that fund administrators complied with OD’s statement of requirements document and other internal guidance for establishing the fund administrator pool. As a result, the SEC lacks assurance that fund administrators are adequately protecting the confidentiality, integrity, and availability of investors’ PII collected and maintained on behalf of the agency in the course of the distribution process.

Conclusion

According to OD and as stated in Rule 1105 of the SEC's Rules on Fair Fund and Disgorgement Plans, unless waived by the Commission, fund administrators are required to obtain a bond that covers errors and fraud in administrative proceedings. Thus, the bond acts as a method to mitigate the financial consequences of errors or fraud within the distribution process, including instances of inaccurate payments. In addition, the fund administrators provide statements of assurance that payment files are complete and accurate. Yet, in certain instances, fund administrators have submitted to the SEC inaccurate payment files after giving assurances that the files were accurate. The SEC relied on the work of fund administrators without clearly defining or documenting oversight procedures and did not identify the inaccuracies. Moreover, despite fund administrators' inaccuracies and failure to comply with the SEC's requirements for information security, the agency did not remove or exclude fund administrators from the pool and, in fact, continues to use them to administer distributions of disgorgement and penalty amounts resulting from filed enforcement actions.

We conclude that improvements are needed to strengthen internal controls; fully address the risks of relying on fund administrators, including the risk of accepting inaccurate payment files and making inaccurate payments; and comply with SEC requirements and Federal laws regarding fund administrators' information security controls.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve oversight of fund administrators, comply with applicable laws and agency policy and requirements, and ensure that goals and objectives are met, we recommend:

Recommendation 1: The Office of Distributions (OD) should use the Government Accountability Office's *Standards for Internal Controls in the Federal Government* to:

- (a) assess the risks in the SEC's use of fund administrators to distribute disgorgements and penalties to harmed investors; and
- (b) based on the risks identified, and considering the oversight framework provided by the Federal Acquisition Regulation as a best practice, document in OD's policies and procedures OD's oversight responsibilities and any internal control activities needed to meet those responsibilities.

Management's Response. The Office of Distributions concurred with the recommendation and will assess risks associated with relying on fund administrators to distribute payments to harmed investors. The Office will also continually consider risks and review processes to make improvements as recommended.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 2: The Office of Distributions should work with the Office of Information Technology to thoroughly review and document its review of the data security control reports for all fund administrators currently used in the distribution process and complete security assessments and privacy impact assessments of all fund administrators currently used in the distribution process, as required by the E-Government Act of 2002, including the Federal Information Security Management Act and the Office of Information Technology's Security Policy Framework Manual 24-04-08-06-FM (Rev. 2), dated May 13, 2015.

Management's Response. The Office of Distributions concurred with the recommendation and will work with the Office of Information Technology to complete the required assessments of all nine fund administrators by December 31, 2015.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 3: The Office of Distributions should update its policies and work with the Office of Information Technology to ensure information technology security evaluations of fund administrators are periodically conducted, and determine whether any noncompliance requires suspension of distribution activity or removal from the pool, in accordance with internal guidance.

Management's Response. The Office of Distributions concurred with the recommendation and will work with the Office of Information Technology as recommended.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Appendix I: Scope and Methodology

We conducted this performance audit from February 2015 through September 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope and Methodology. The audit covered FY 2010 through FY 2014 (the period between October 1, 2009, and September 30, 2014). Additionally, OD told us about issues that occurred before FY 2010 we considered relevant to our audit objectives. To address our audit objectives, we reviewed (1) disgorgement and penalty data; (2) Enforcement's efforts to collect disgorgement and penalty amounts; (3) Federal laws and regulations and the SEC's policies and procedures for collecting and distributing disgorgement and penalty amounts to harmed investors; and (4) Enforcement's role in overseeing fund administrators. We also:

- interviewed officials from Enforcement, OIT, and the Office of Financial Management to understand the SEC's policies and procedures for collecting and distributing disgorgement and penalty amounts;
- reviewed a sample of filed enforcement actions to determine whether the SEC's oversight of fund administrators complied with Federal laws and regulations and agency policies and procedures; and
- reviewed evidence to assess the SEC's continued implementation of previous OIG recommendations from Evaluation Report 432, "Oversight of Receivers and Distributions Agents."

The Federal laws and guidance, as well as the SEC policies, procedures, and administrative regulations we reviewed included:

Federal Laws and Guidance:

- Securities Act of 1933.²¹
- Securities Exchange Act of 1934.²²
- Securities Enforcement Remedies and Penny Stock Reform Act of 1990.²³

²¹ Pub. L. 73-22, 48 Stat. 74 (1933) (codified as amended at 15 U.S.C. §§ 77a-77aa (2012)).

²² Pub. L. 73-291, 48 Stat. 881 (1934) (codified as amended 15 U.S.C. §§ 78a-78kk (2012)).

- Sarbanes-Oxley Act of 2002.²⁴
- E-Government Act of 2002.²⁵
- Dodd-Frank Wall Street Reform and Consumer Protection Act.²⁶
- *Rules of Practice and Rules on Fair Fund and Disgorgement Plans*.²⁷
- *Standards for Internal Control in the Federal Government* (1999) and updated *Standards for Internal Control in the Federal Government* (2014).²⁸

SEC Policies and Procedures:

- *Statement of Requirements, Distribution Fund Administration Services* – Office of Collections and Distributions (2011).
- *Distributions Manual*, Division of Enforcement – Office of Distributions (August 15, 2013).
- *Guidelines for the Collection of Delinquent Debt*, Division of Enforcement – Office of Collections (April 21, 2015).
- *SEC OIT Security Policy Framework Manual 24-04-08-06-FM (Rev. 2)*, Office of Information Technology (May 13, 2015).

Internal Controls. During our audit, we assessed the SEC’s internal controls related to the collection and distribution of monies to harmed investors. Specifically, we considered the control environment, risk assessment, and control activities of collecting, distributing, and overseeing the work of external parties in distributing monies to harmed investors. As discussed in the report, we noted internal control weaknesses related to

²³ Pub. L. 101-429, 104 Stat. 931 (1990) (codified as amended in scattered sections of 15 U.S.C.).

²⁴ (Public Company Accounting Reform and Investor Protection Act) Pub. L. 107-204, 116 Stat. 745 (2002) (codified as amended in scattered sections of 15 U.S.C. and 18 U.S.C.).

²⁵ Pub. L. 107-347, Dec. 17, 2002, 116 Stat. 2899 (2002)(codified as amended in scattered sections of Titles 5, 10, 13, 31, 40, and 44 of U.S.C.). On December 18, 2014, FISMA was largely superseded by the Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073 (2014) (codified as amended at 44 U.S.C. §§ 101, 3531-38, 3541-49 and 3551-58). See 44 U.S.C. §§ 3551-3558 for current requirements.

²⁶ Pub. L. 111-203, 124 Stat. 1376 (2010) (codified as amended in scattered sections of Titles 7, 12, 15 and 22 of U.S.C.).

²⁷ 17 C.F.R. Part 201, Subparts D and F (2015).

²⁸ U.S. Government Accountability Office, GAO/AIMD-00-21.3.1, *Standards for Internal Control in the Federal Government* (1999). In September 2014, GAO revised the standards, issuing GAO-14-704G. However, the revised standards are not effective until FY 2016, although agency management may adopt them earlier.

the distribution program that impact the SEC's ability to (1) effectively distribute disgorgement and penalty amounts to harmed investors, and (2) ensure investors' PII is protected. Our recommendations, if implemented, should correct the weaknesses we identified. One of our audit objectives included an assessment of the SEC's policies, procedures, and efforts for timely collecting and distributing disgorgement and penalty amounts to harmed investors. We reviewed the timeliness of collections and distributions of disgorgements and penalties and did not identify any issues.

Computer-processed Data. The U.S. Government Accountability Office, GAO-09-680G, *Assessing the Reliability of Computer-Processed Data* (2009) states that "data reliability refers to the accuracy and completeness of computer-processed data, given the uses they are intended for. Computer-processed data may be data (1) entered into a computer system or (2) resulting from computer processing." Furthermore, GAO-09-680G defines "reliability," "accuracy," and "completeness" as follows:

- "Reliability" means that data are reasonably complete and accurate, meet your intended purposes, and are not subject to inappropriate alteration.
- "Accuracy" refers to the extent that recorded data reflect the actual underlying information.
- "Completeness" refers to the extent that relevant records are present and the fields in each record are appropriately populated.

We relied on computer-processed data from the SEC's financial management and case-tracking systems (Delphi, Phoenix, and HUB) to analyze filed enforcement actions with disgorgement and penalty amounts ordered between FY 2010 and FY 2014. We performed data reliability testing by comparing the detailed listing of enforcement actions to a summary file. We also traced information contained in the detailed listing of enforcement actions to and from source documents to test for accuracy. Based on these steps, we determined the detailed listing of enforcement actions for FY 2010 through FY 2014 was sufficiently reliable for the purposes of the audit.

Sampling. We judgmentally sampled 13 out of 198 enforcement actions from FY 2010 through FY 2014, including both administrative proceedings and District Court cases in which an actual distribution occurred or is in progress. We used a random number generator in Microsoft Excel to select our sample of 13 actions. Based on our analysis of administrative proceedings, we determined that the length of time between an initial order for payment of disgorgement and penalty amounts and the order terminating the disgorgement or fair fund was 6.2 years. Therefore, we allocated the sample items by fiscal year and selected more items from the earlier years to ensure that we reviewed actions including disbursements. Table 4 summarizes our sampled items by fiscal year.

Table 4. Summary of Sampled Enforcement Actions

Fiscal Year	Number of Administrative Proceedings	Number of District Court Cases	Total No. of Actions Sampled
FY 2010	0	5	5
FY 2011	2	1	3
FY 2012	1	1	2
FY 2013	0	1	1
FY 2014	0	2	2
Total	3	10	13

Source: OIG-generated based on information provided by Enforcement.

We used our sample to:

- test for sufficient support and internal controls for (1) determining disgorgement and penalty amounts collected, (2) identifying harmed investors, (3) distributing payments to harmed investors, and (4) referring debt to the U.S. Treasury;
- examine and analyze the SEC's selection, payment, and oversight of third party distributors in accordance with Federal laws, regulations, and SEC rules, policies, and procedures; and
- test the reliability of the enforcement action detail information.

Fraud. As noted in this report, fraudsters submitted to fund administrators fraudulent claims that were accepted and paid. In one case, the USPIS caught the fraudster, who was later convicted in a Federal District Court. In the other case, the U.S. Attorney's Office charged the claimant with fraud in connection with the claim. We identified these types of fraud as a potential risk in the context of our audit objectives and used our assessment of risk to determine auditing procedures and mitigate our overall audit risk to an acceptable level. In addition, we identified the potential for fraud as a potential risk when using fund administrators to distribute disgorgement and penalty amounts to harmed investors. Furthermore, we recommended that OD complete a risk assessment and, based on the risks identified, document OD's oversight responsibilities and any internal control activities needed to meet those responsibilities in OD's policies and procedures.

Prior Coverage. During the last 8 years, the SEC OIG and GAO issued seven reports of particular relevance to this audit. Unrestricted reports can be accessed over the Internet at http://www.sec.gov/about/offices/oig/inspector_general_audits_reports.shtml (SEC OIG) and <http://www.gao.gov> (GAO).

SEC OIG:

- *Oversight of Receivers and Distribution Agents*, Report No. 432 (December 12, 2007).
- *The Division of Enforcement's Draft Policies and Procedures Governing the Selection of Receivers, Fund Administrators, Independent Distribution Consultants, Tax Administrators and Independent Consultants*, Report No. 454 (September 16, 2008).
- *Audit of Disgorgement Waivers*, Report No. 452 (February 3, 2009).

GAO:

- *Additional Actions Needed to Ensure Planned Improvements Address Limitation in Enforcement Division Operations*, GAO-07-830 (August 15, 2007).
- *Greater Attention Needed to Enhance Communication and Utilization of Resources in the Division of Enforcement*, GAO-09-358 (March 31, 2009).
- *Securities and Exchange Commission: Information on Fair Fund Collections and Distributions*, GAO-10-448R (April 22, 2010).
- *Financial Audit: Securities and Exchange Commission's Fiscal Years 2014 and 2013 Financial Statements*, GAO-15-166R (November 17, 2014).

Appendix II: Management Comments



DIVISION OF
ENFORCEMENT

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

100 F Street, N.E.
Washington, DC 20549

MEMORANDUM

TO: Carl W. Hoecker, Inspector General, Office of Inspector General

FROM: Andrew J. Ceresney, Director
Victor J. Valdez, Managing Director

RE: Division of Enforcement's Response to the Office of Inspector General's Report on Audit No. 531

DATE: September 23, 2015

We appreciate the opportunity to review and comment on the Draft Report.

We are pleased that the audit function of the Office of Inspector General (OIG-Audit) found no concerns related to the controls over our extensive efforts to collect amounts due related to filed enforcement actions, and found no inaccurate payments in its sample of thirteen distribution matters spanning the past five fiscal years. We are pleased that OIG-Audit did not find any instance of an injured investor receiving less than the appropriate share of distributable amounts, including in those few distribution matters that were impacted by error or fraud over the past ten fiscal years. We consider these findings to be attributable to the effectiveness of the robust policies and procedures already adopted by both the Office of Collections and the Office of Distributions ("Distributions").

Investor protection is a key component of the agency's mission. At its discretion, the Commission may initiate a distribution of collected disgorgement and penalty amounts to harmed investors where appropriate and feasible. Distribution is not possible or appropriate in all cases. In assessing whether to distribute collected funds, the Commission considers, among other things, cost-effective and fair methods to identify harmed investors, calculate losses, allocate distributable amounts, and execute the distribution. Since the passage of the Sarbanes Oxley Act in 2002, the SEC has returned more than \$10 billion to harmed investors through the distributions process.

Over the past five fiscal years, the Enforcement Division made significant improvements designed to streamline the distribution of funds to harmed investors, and implemented significant controls over those processes. These improvements include: (i) the formation of a dedicated office to centralize the handling of distributions, develop expertise, and improve speed and efficiency in the distribution process; (ii) the creation of a comprehensive manual documenting

the policies and procedures for distribution activities; (iii) the establishment of a pool of Commission-approved fund administrators required to employ enhanced claims review processes and fraud controls; (iv) delegation of authority to the Division Director to appoint fund administrators from the approved pool in SEC distributions; and (v) development of controls around the selection, approval, appointment, and use of pool fund administrators.

The OIG-Audit Report referenced a limited number of distributions, all of which were initiated before 2010, where fund administrators submitted inaccurate payment files or considered fraudulent claims. Distributions took immediate and substantial action in every instance to diagnose the source of the error so that remedial steps could be taken by the fund administrator. In each instance, the related fund administrators were required to make corrective payments, at their own expense, so that no harmed investor received a smaller payment than that required by the applicable distribution plan. Thus, most significantly, every investor impacted by a payment file inaccuracy or fraudulent claim referenced in the OIG-Audit Report received the full amount of the funds to which they were entitled. Some inaccurate payments or fraudulent claims may have reduced the amount remitted to the U. S. Treasury, but did not negatively impact the amount returned to harmed investors.

It is important to note that before payments are distributed, the third-party fund administrator submits a payment file, which is the result of numerous steps completed by the fund administrator pursuant to a distribution plan approved by the Commission or a District Court. These steps may include (1) determining the appropriate method for calculating harm, (2) developing procedures for identifying and notifying harmed investors of their opportunity for recovery of their harm, (3) receiving, reviewing, and analyzing claims from harmed investors, (4) determining the validity of claims received and the amount of harm relative to each investor, (5) obtaining information needed from harmed investors in order to make payments to them and, if required, report the payments to the IRS, and (6) engaging an independent third party to verify that the processes were completed properly and correctly.

The established controls are designed to ensure that fund administrators have the responsibility to submit accurate payment files. The Commission has a long-standing policy of requiring fund administrators to obtain a bond in every distribution to further protect investors and the distribution funds from incurring any losses resulting from errors or fraud. To date, the SEC has never had to execute a claim on a bond.

Because the SEC needs to rely on the work of third-party fund administrators, Distributions recognizes the need to routinely assess possible risks associated with engaging these third parties to administer payments to harmed investors. We will continue to consider risks and review processes to make improvements where possible as recommended in Recommendation 1.

With regard to information security, the OIG-Audit Report describes the SEC's assessment of risks and implementation requirements for its pool of fund administrators. The Office of Information Technology (OIT) has developed a plan to complete required assessments of all nine fund administrators by December 31, 2015. We will continue to work with OIT as recommended in Recommendations 2 and 3.

Appendix III: OIG's Response to Management Comments

We are pleased that SEC management concurred with all three recommendations for corrective action. Management's proposed actions are responsive to the recommendations; therefore, the recommendations are resolved and will be closed upon completion and verification of appropriate corrective action. Full implementation of our recommendations should help the agency improve oversight of fund administrators, comply with applicable laws and agency policy and requirements, and ensure that goals and objectives are met.

Major Contributors to the Report

Colin Heffernan, Audit Manager

Kamran Beikmohamadi, Lead Auditor

Sumeer Ahluwalia, Auditor

To Report Fraud, Waste, or Abuse, Please Contact:

Web: www.reportlineweb.com/sec_oig

E-mail: oig@sec.gov

Telephone: (877) 442-0854

Fax: (202) 772-9265

Address: U.S. Securities and Exchange Commission
Office of Inspector General
100 F Street, N.E.
Washington, DC 20549-2736

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, please contact Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects at sharekr@sec.gov or call (202) 551-6061. Comments, suggestions, and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed above.