OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS
RISK ALERT

February 13, 2019

Transfer Agent Safeguarding of Funds and Securities

Key Takeaway:
Transfer agents should review their practices, policies, and procedures to ensure funds and securities are protected while held at the transfer agent.

I. Introduction

During the period of October 2014 through September 2017, the Office of Compliance Inspections and Examinations ("OCIE") conducted 75 examinations of transfer agents ("TAs") that also served as paying agents.[1] The staff examined for the possible misappropriation of funds and assessed the TAs' policies, procedures, and controls for paying agent activities.[2] This Risk Alert highlights some of the risks and issues associated with paying agent activities, identifies significant exam deficiencies related to the safeguarding of funds and securities by paying agents, and provides a listing of some common features of robust safeguarding policies, procedures, and controls for paying agents.

II. Background

TAs serve as agents for issuers and play a critical role in the settlement of securities transactions. Among their key functions, TAs are responsible for maintaining issuers' securityholder records, recording changes of ownership, canceling and issuing certificates, distributing dividends and other payments to securityholders, and facilitating communications between issuers and securityholders.

Paying agent activities vary, but commonly include:

- Processing and disbursing principal, interest, and dividend payments to bondholders or shareholders based on an issuer's payment schedule;
- Administering direct stock purchase and dividend reinvestment plans;
- Handling escheatment and lost shareholder search and report filing;
- Managing interest bearing accounts or demand deposit accounts in the name of mutual funds for activities such as inflows and outflows from fund orders; and
- Making distributions for mutual funds.

In certain circumstances, TAs that serve as paying agents are unable to distribute shareholder funds as intended. For example, checks may be returned to the TA as undeliverable, shareholders may receive a check but never cash it, or electronic banking instructions may be inaccurate. In these situations, shareholder funds may remain in the TA's bank accounts for years until the funds are escheated per relevant state law.

Exchange Act Rule 17Ad-12 (the "Safeguarding Rule") requires any registered TA in possession of funds or securities related to transfer agent activities to assure that:

---

[1] A paying agent accepts payments from the issuer of a security and distributes the payments to the holders of the security. *See* Rule 17Ad-17 under the Securities Exchange Act of 1934 ("Exchange Act").

[2] OCIE has prioritized examining for the safeguarding of funds and securities by transfer agents. *See* Examination Priorities for 2016, Examination Priorities for 2017, and Examination Priorities for 2018.

(1) the securities are held in safekeeping and are handled, in light of all facts and circumstances, in a manner reasonably free from the risk of theft, loss, or destruction; and

(2) the funds are protected, in light of all facts and circumstances, against misuse.

In evaluating which particular safeguards and procedures must be employed, two relevant factors are the cost of the various safeguards and procedures as well as the nature and degree of potential financial exposure.

Exchange Act Rule 17Ad-17 (the "Lost Securityholder/Unresponsive Payee Rule") requires every TA that maintains an issuer's master securityholder file[3] to conduct searches for lost securityholders within a defined time period and send notices to unresponsive payees within a defined time period. A TA must keep and maintain records to demonstrate compliance with the rule including written procedures that provide the TA's methodology for complying with the rule.[4]

III. Examination Observations and Compliance Issues

The staff's observations from recent examinations of paying agents generally fall into two categories: (i) safeguarding of funds and securities and (ii) notification to unresponsive payees and policies and procedures for lost securityholder searches.

1. Safeguarding Rule

Below are examples of deficiencies and weaknesses that OCIE staff observed in connection with the Safeguarding Rule:

- *Misappropriation and Theft.* OCIE staff observed the misappropriation of shareholder funds and the theft of physical certificates.[5] For example, in some instances, TA employees misappropriated issuer funds for personal use, and in other instances, a TA used shareholder funds to pay fees of the TA. The staff also observed TAs keeping physical certificates in unsecured locations for long periods of time, resulting in the reissuance of those certificates to different shareholders.

- *Policies, Procedures, and Controls.* OCIE staff observed that some TAs did not have adequate policies, procedures, and controls for the safeguarding of funds and securities. In some instances, TAs did not have policies and procedures for any paying agent activities, while in other instances, their policies and procedures did not address the issuance and handling of checks, the distribution of dividends, bank account reconciliation, escheatment, or periodic redemption requests for limited partnerships. Some TAs had policies and procedures, but they lacked specificity, did not designate responsibility for performing or documenting reviews, or only quoted rule requirements. Some TAs did not have reasonable controls to protect funds from misuse when conducting typical disbursement activities, such as requiring confirmation from multiple individuals in order to move issuer funds.

---

[3] Exchange Act Rule 17Ad-9(b) defines master securityholder file as "the official list of individual securityholder accounts."

[4] Exchange Act Rule 17Ad-17(d).

[5] The Commission has brought enforcement actions in this area. *See, e.g.*, Securities and Exchange Commission v. Robert G. Pearson and Illinois Stock Transfer Company d/b/a IST Shareholder Services (Litigation Release No. 23007, May 28, 2014) (complaint alleging Illinois Stock Transfer Company and its president, Robert Pearson, misappropriated approximately $1.3 million of issuer and shareholder funds).

- *Account Reconciliation.* OCIE staff observed that some TAs did not have adequate account reconciliation controls and procedures. For example, the staff observed the comingling of shareholder funds with TA operating funds without an adequate reconciliation process, as well as the commingling of funds in a single account despite policies and procedures stating that funds would be maintained in separate accounts designated for the benefit of each issuer.

- *Security Protocols.* OCIE staff observed instances where TAs did not secure access to vaults, computers, and areas of the firm that handle disbursement operations, creating a risk of theft, loss, or destruction.

2. Lost Securityholder Searches / Unresponsive Payee Notifications

Below are examples of deficiencies and weaknesses that OCIE staff identified in connection with the Lost Securityholder/Unresponsive Payee Rule.

- *Lost Securityholder Searches*. OCIE staff observed TAs that did not comply with the database search requirements of the Lost Securityholder/Unresponsive Payee Rule. For example, the staff observed TAs that did not conduct lost securityholder searches, or if searches were conducted, they were not conducted within the proper timeframe. In addition, some TAs conducted searches for lost securityholders using only public resources instead of an information database service, as required by Rule 17Ad-17(a)(1). The staff also observed TAs that did not identify securityholders as lost and record the lost status in their records and, as a result, were unable to determine whether lost securityholder searches were required.

- *Unresponsive Payee Notifications.* OCIE staff observed TAs that failed to send written notifications to unresponsive payees or had sent notifications after the required timeframe set by Rule 17Ad-17.

- *Policies and Procedures.* OCIE staff observed weaknesses with TAs' policies and procedures under Rule 17Ad-17, including written procedures that did not require database searches, address unresponsive payee notifications, designate responsibility for performing and documenting reviews, or outline the methodology utilized to comply with the rule. The staff also observed TAs that did not maintain records of their lost securityholder searches and unresponsive payee notifications.

IV. Features of Robust Policies, Procedures, and Controls[6]

During these examinations, the staff observed several TAs that appeared to have implemented robust written policies, procedures, and controls related to the processing of funds, handling of physical certificates, lost securityholder searches, and unresponsive payee notifications. For example, these TAs engaged in the following practices:

- *Safeguarding Funds.*
  - Using segregated and specifically designated accounts for client fund deposits and payments to prevent commingling of those funds with funds in the TAs' operation accounts.
  - Segregation of duties among different individuals holding different positions at the TA to limit any one person having too much control or access over the funds and securities.
  - Frequent bank reconciliations.

[6] This section is not intended to be a comprehensive listing of robust safeguarding policies, procedures, and controls. The adequacy of supervisory, compliance, and other risk management policies and procedures can be determined only with reference to the business profile of each specific transfer agent and other facts and circumstances.

- Implementing accounting controls such as the "positive pay system."
- Requiring all payment instruction changes be made in writing.
- Maintaining logs of unissued and uncashed checks.
- Establishing specific deadlines or timeframes for each step in the paying agent process or certificate movement.
- Identifying entities or positions responsible for specific tasks in the policies and procedures.

- *Safeguarding Physical Securities.*
  - The use of locked vaults to store certificates, and vault access was restricted to a limited number of personnel.
  - The use of video cameras throughout the vault area.
  - The requirement of multiple sign-offs on the certificate control log.
  - Periodic audits of blank certificates and cancelled certificates.
  - The use of passcodes and ID badges to restrict non-employees from entering the TA's office.

- *Lost Securityholder and Unresponsive Payee Practices.*
  - Establishing and maintaining written procedures that outline how the TA identifies and records a lost securityholder in its recordkeeping system.
  - Discontinuing the mailing of physical checks to securityholders that have been deemed lost.
  - Maintaining copies of dated, returned mail, including copies of the outer envelope.
  - In addition to the required lost securityholder database searches, reviewing the list of lost securityholders, including non-natural persons, to determine if an updated address can be easily attained by searching information available in the public domain.
  - Establishing and maintaining written procedures that outline the escheatment services provided to issuers and the requirements of each applicable state.

Transfer agents may wish to consider these practices in the implementation of safeguarding policies, procedures, and controls.

V. Conclusion

OCIE staff believes that safeguarding funds and securities is one of the highest risk areas for TAs because of the trillions of dollars that TAs control and distribute each year as paying agents. The objective in publishing this Risk Alert is to highlight significant exam deficiencies observed by the staff while also identifying robust practices in order to encourage TAs to review and strengthen their applicable policies, procedures, and controls related to their paying agent operations.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.