'Top 15'Audit and Field Exam Findings,
Computer Security Procedures

By Suzanne Hazard, Deputy Assistant Director,
Chapter 7 Oversight, Executive Office for U.S. Trustees

From time to time we review and discuss common findings in chapter 7 trustee audits and field exams to call attention to important issues and to note trends and changes in trustee practices. Most recently, in the Spring 2013 issue of *NABTalk*, we compared the top ten audit and field exam findings from 2000-2003 to their rankings in Fiscal Year (FY) 2012. In this article, we provide a timely update on frequent audit and field exam findings from FY 2011 through FY 2013. We also discuss several important computer security provisions added to the *Handbook for Chapter 7 Trustees* (Handbook) in October 2012 (http://www.justice.gov/ust/eo/private_trustee/library/chapter07/index.htm).

Audits and Field Exams, FY 2011-FY 2013

As most chapter 7 trustees and trustee assistants know, each trustee is audited by an independent Certified Public Accounting firm or examined by a representative of the United States Trustee Program (Program)–typically a Bankruptcy Analyst–at least once every four years. The focus of these reviews is to ensure that strong internal controls and other safeguards are in place and operating effectively.

During FY 2011 through FY 2013 (October 1, 2010 through September 30, 2013), 412 audits and 327 field exams were conducted and 7,289 findings were reported. The fifteen most common findings are presented in Table 1.

Table 1. Top 15 Audit and Field Exam Findings–FY 2011 through FY 2013

Description	Quantity	Percentage of Total Findings	Frequency (see note)
1. Form 1: scheduled assets do not match the debtor's schedules	502	6.9%	68%
2. Bank accounts are not timely or properly reconciled and reviewed	451	6.2%	61%
3. Prior findings are repeated in the current audit or field exam	435	6.0%	59%
4. Form 1: miscellaneous errors	349	4.8%	47%
5. Inaccurate uniform transaction codes	346	4.7%	47%
6. Form 1: asset status is not accurately reflected and tracked	336	4.6%	45%
7. Form 1: unscheduled assets are not recorded or properly identified	320	4.4%	43%
8. Form 1: debtor or trustee asset values are not verified or reasonably determined	318	4.4%	43%
9. Form 1: abandonments are not properly tracked	202	2.8%	27%
10. Report of sale or auctioneer's report is not timely filed	201	2.8%	27%
11. Non-compliance with domestic support obligation noticing guidelines	197	2.7%	27%
12. Form 2: transaction description is blank, inaccurate, or insufficient	197	2.7%	27%
13. No or inadequate case progress review procedures	185	2.5%	25%
14. Delay in case administration	181	2.5%	24%
15. Receipts log is not maintained by the person who opens the mail	169	2.3%	23%
Total Number of Findings Reported FY 2011 Through FY 2013	7,289		

Note: “Frequency” is the percentage of audits and field exams that reported this finding.

As in prior years, errors on the Individual Estate Property Record and Report (Form 1) were the most frequently reported finding, accounting for nearly 30 percent of all audit and field exam findings. As shown on Table 1, discrepancies between the assets listed on the debtor’s schedules and on Form 1 topped the chart. There were discrepancies in both dollar amounts and asset descriptions. Sometimes, assets were inadvertently omitted. To avoid these errors, as well as other types of errors involving Form 1, trustees should compare Form 1 to the schedules after downloading or entering the scheduled data to ensure the information was accurately transferred or entered. In addition, trustees need to ensure Form 1 is updated when debtors amend their schedules. Trustees also should carefully review these reports again before submitting them to the United States Trustee and filing them with the court.

While the error rate pertaining to scheduled assets continues to be high, accuracy in recording unscheduled assets is improving. Unscheduled assets are those assets identified by trustees that were not listed by the debtors in their schedules. As shown in Table 1, 320 audits and field exams contained this finding. Significantly, from FY 2011 to FY 2013 the number of findings in this category declined by nearly half.

The audits and field exams also reveal improvement in two related categories of findings: case progress review procedures (185 findings) and cases that evidence delay in case administration (181 findings). Bankruptcy Code Section 704(a)(1) directs trustees to close cases as expeditiously as is compatible with the best interests of parties in interest. To help trustees accomplish this duty, the Handbook requires that they implement a system to review the progress of each case at least quarterly to ensure that case administration and closure are not unduly delayed. Trustees must retain evidence of this ongoing review and provide it to the U.S. Trustee or auditor upon request. Although the two categories of findings still fell within the top fifteen, the number of findings in each category decreased markedly from FY 2011 to FY 2013. During that period, findings related to the adequacy of a trustee’s case progress review procedures fell by 33 percent and findings related to delay in case administration declined by 75 percent. Delay in case administration was reported in 37 percent of the audits and exams in FY 2011, but in only 10 percent of audits and exams in FY 2013.

One area that continues to be of major concern to U.S. Trustees is Number 3 on the Top 15 list: Prior findings are repeated in the current audit or field exam. Repeat findings are still too high, showing up in nearly 60 percent of the audits and field exams. This number should be closer to zero. The category of repeat findings includes the recurrence of internal control weaknesses as well as reporting errors similar to previously reported findings. U.S Trustees are particularly concerned about the recurrence of internal control weaknesses because this means that a promised correction was not implemented or a weakness was allowed to recur.

As part of the audit and field exam closure process, a trustee asserts that all findings will be corrected and new procedures will be implemented as needed. Depending upon the severity of the findings, the Program may visit the trustee’s office to verify that the promised corrective actions have been implemented. Audits and exams with less consequential findings do not require an office visit. The audit or field exam will be closed with the understanding that the trustee has implemented or will implement the actions described in the trustee’s written response. In the most egregious situations with a repeat finding, the trustee never implemented the promised correction or reverted to the old procedures after the Program’s office visit.

It is important for trustees to institute procedures that will detect and correct reporting errors on an ongoing basis. It is also important for trustees to know and implement the Handbook requirements for internal controls and to verify that the procedures remain in effect. Following these simple steps will help trustees ensure that strong internal controls and other safeguards are in place and operating effectively:

- Periodically review Handbook Chapter 5 and the Supplementary Materials, particularly the instructions for trustee interim reports, and evaluate whether the trustee's procedures are consistent with these instructions and policies.

- Annually review the prior audit or field exam report and the trustee's responses to ensure the promised corrective actions occurred and remain in effect.

- Annually review the internal control questionnaire completed for the previous audit or field exam and ensure the trustee operation still complies with the responses or changes made as a result of the audit or exam. If the trustee did not keep the prior internal control questionnaire, a blank form is available at www.justice.gov/ust/eo/private_trustee/library/chapter07/docs/field_exams/ICQ_2012.pdf.

New Computer Security Procedures

Turning to another aspect of chapter 7 trustee operations, this section discusses important updates regarding three computer security provisions added to the Handbook in October 2012. The new provisions address employee use of the computer system, encryption of laptop hard drives and encryption of mobile storage media.

Handbook Chapter 5.G.3.e (9) requires trustees to adopt a set of rules governing employee use of the trustee's computer system. A sample Rules of Behavior document is provided in the Handbook Supplementary Materials at http://www.justice.gov/ust/eo/private_trustee/library/chapter07/index.htm. The trustee's policy must explain the employee's responsibilities as a user and the penalties for non-compliance. In addition, it should include rules regarding Internet access, personal use of the computer, personal email and personal instant messaging. All employees must sign the policy acknowledging receipt of these rules of behavior and an understanding of their responsibilities.

Starting this fiscal year–FY 2014–audits and field exams will verify that the trustee has implemented this policy. Trustees who have not yet implemented a policy should do so now. The Program also recommends that trustees review the policy with their employees at least annually.

The implementation of Handbook Chapter 5.G.3.e (7) and (8), relating to encryption of laptop hard drives and mobile storage media, was postponed when the Handbook was issued in October 2012. As announced in April 2014, these provisions became effective on May 1, 2014.

Chapter 5.G.3.e. (7) and (8) state the following:

> "(7) Hard drives of all laptops must be encrypted. The encryption tool must meet industry standards such as the most current FIPS.

(8) Mobile storage media (for example, USB thumb drives) or the files on them must be encrypted."

Laptops and mobile storage media containing chapter 7 case information, debtor personally identifiable information (PII) and other sensitive information must now be encrypted using a tool that meets industry standards. FIPS is a reference to the Federal Information Processing Standards published by the National Institute of Standards and Technology. See http://www.nist.gov/information-technology-portal.cfm. It is one example of an industry standard, but there are others. A trustee's computer software provider or other information technology professional can help the trustee identify an appropriate encryption tool.

There is an exception to the requirement that a laptop hard drive be encrypted. If the laptop is used to access the trustee's data remotely and is never used to store sensitive information, encryption is not necessary.

Compliance with these provisions will be verified through audits and field exams. The internal control questionnaire used for these reviews asks the following question: "Are hard drives on laptops and mobile storage media encrypted to prevent unauthorized access in the event the laptops or storage media are lost or stolen?" A "no" answer will be reported as a finding.

Conclusion

This periodic review of common audit and field exam findings is intended to help trustees strengthen the internal controls and bolster the integrity of the financial record keeping and reporting procedures within their trustee operations. In particular, the article highlights several internal control and computer security measures to raise trustee awareness about important Handbook requirements that will be reviewed during audits and field exams. Questions about the information presented in this article should be directed to your local U.S. Trustee's office. In addition, trustees are encouraged to offer suggestions to improve the Handbook and the audit and field exam process.