

ACA Insight

The weekly news source for investment management legal and compliance professionals

“There is anecdotal evidence to support the contention that some firms are cleaning up a bit after we announce exams but before we arrive.”

Inside Insights

6 Revenue Sharing in
Exchange for Investments
May Be a Conflict

SEC Conducting Unannounced Examinations

At least one of the SEC’s regional offices is conducting unannounced examinations on investment advisers – and other SEC offices may notice and follow suit.

“We are doing unannounced exams,” said the agency’s Boston Regional Office associate director for examinations **Kevin Kelcourse**. While he said he cannot speak for other regional offices, “we are certainly doing them here.”

“SEC exam staff have been conducting unannounced exam visits to registered investment advisers in the Boston region and they could do this in other regions,”
[continued on page 2](#)

DOL Proposes Delaying Fiduciary Rule Exemptions to July 2019

It seems compliance with various aspects of the Department of Labor’s Fiduciary Rule keep getting pushed back. In the latest case, the DOL on August 9 issued a notice of administrative action¹, stating that it plans to delay the compliance date for three Fiduciary Rule exemptions, including the Best Interest Contract Exemption, from January 2018 to July 2019.

Whether the postponement actually becomes final will depend on a number of things, among them public comments on the proposed change and what the Department plans to do in light of those comments.

[continued on page 3](#)

OCIE Finds Increased Cybersecurity But Wants More

The SEC’s Office of Compliance Inspections and Evaluations on August 7 made public its observations² from its most recent round of cybersecurity exams – and what it found is encouraging only to a point. The message delivered by OCIE in its National Exam Program risk alert was this: Advisory firms, broker-dealers and investment companies have made strides in providing cybersecurity, but there is still a long way to go.

OCIE examined 75 firms under its Cybersecurity 2 Initiative, begun in 2015. These exams involved more validation and testing of procedures and controls related to cybersecurity than the agency’s 2014 Cybersecurity 1 Initiative.

[continued on page 4](#)

SEC Conducting

continued from page 1

said **Kirkland & Ellis** partner and former SEC Division of Investment Management director **Norm Champ**. “These visits emphasize again the importance of exam preparation for any registered investment adviser.”

Less than 20 unannounced exams have been performed since the regional office resumed doing them “in the last year or so,” Kelcourse said, adding that he may have the time frame wrong. He became associate director in the Boston office in November 2014, moving over from the Division of Enforcement.

“There is anecdotal evidence to support the contention that some firms are cleaning up a bit after we announce exams but before we arrive,” Kelcourse said in explaining why the regional office chose to revive the unannounced exam visits. Some advisory firms, he said, may have the philosophy of “I’ll obey the speed limit when I see there’s a cop there.”

That said, Kelcourse added that advisers “should not read anything into the fact that we are doing these exams.” No particular type of advisory firm is targeted, he said. There had been some reports from securities attorneys in the area that private firms were the focus of these unannounced visits, but he said that was not the case. Private advisers, retail advisers and others may be selected.

Just how are the advisory firms selected? “I don’t want to go into the selection process,” Kelcourse said, but added that those chosen for unannounced visits account for a very small percentage of all the advisory firms in the Boston region that are examined. “It’s just one tool in our toolbox.”

“The unannounced visits are always done in conjunction with an open examination,” he said. Typically, when examiners make these visits, they ask to meet with the chief compliance officer and, at that meeting, hand him or her a document request list. “We are not generally expecting that the firm will give us documents right then and there, but we may ask to see documents such as the ledger at that meeting.”

History

Unannounced or “surprise” examinations have not been performed by the agency in many years. The typical routine in current years is for an adviser to receive a letter from the SEC a few weeks prior to the exam visit. That letter not only lets the advisory firm know of a pending visit, but usually requests specific documents that examiners want to review.

Surprise examination visits in recent years might occur for “cause,” that is, if the agency believes it has good reason that some sort of malfeasance or other significant problem is occurring at a firm, and quickly makes plans to visit without an announcement.

Otherwise, however, surprise exam visits were a relic from the past – until now, that is.

“We are not generally expecting that the firm will give us documents right then and there, but we may ask to see documents such as the ledger at that meeting.”

Observations

Two securities attorneys in the Boston area both said they had heard that about six private fund advisers had been visited to date.

Sidley Austin counsel **Kara Brown** said that she first learned of unannounced exam visits in mid-July, and that the information was “just swirling around the Boston community. It’s causing some anxiety for advisers, particularly since it’s the summer and some employees are on vacation.”

“My understanding is that the SEC examiners show up in the lobby area of an advisory firm and ask to speak with the chief compliance officer,” she said. “Once in a meeting room with the CCO, the examiners ask for information about the firm’s compliance program, presumably to see where the adviser sits on OCIE’s risk spectrum.”

Morgan Lewis consultant attorney **Steven Hansen** said that he was aware of six advisers, managing either hedge funds or private equity funds that were visited in a one-week period in June. He had the impression that most of them were never-before-examined firms, a group that OCIE has focused on previously. Some of the examiners, he said, “were members of the private fund unit not based in Boston.”

Kelcourse said that during the Compliance Outreach (formerly CCO Outreach) program in Boston on June 13, he and his staff were “quite open” about the fact they were now doing unannounced exams. ☞

DOL Proposes

continued from page 1

“At the moment, the transition period ends December 31,” said **Wagner Law Group** partner **Stephen Wilkes**. “A lot has to happen for it to be extended. There could be DOL and Office of Management and Budget formal reviews of the impact of an extension, etc. So we are not there yet and one shouldn’t rush to conclude that we have an 18-month extension. There are procedural steps that must be undertaken, some of which are time consuming.”

On the other hand, “the DOL’s filing of a notice of administrative action providing an 18-month extension in the transition period is a strong indication that the transition period will, in fact, be extended until July 1, 2019,” said **Drinker Biddle** partner **Joan Neri**.

The proposed change would delay the compliance date – technically the “extension of transition period and delay of applicability dates” – of the following exemptions to the Rule:

- **Best Interest Contract Exemption.** This would require those providing fiduciary retirement advice, in many cases, to enter into contracts with clients, stating that fiduciaries will act in the best interest of the client.
- **Class Exemption for Principal Transactions.** This exemption would permit an adviser or financial institution to take part in the purchase or sale of a

principal traded asset in certain transactions with a plan, participant or beneficiary account, or IRA, and receive a mark-up, mark-down or other similar payment for themselves or an affiliate.

- **Prohibited Transaction Exemption.** Under this exemption, a person who serves as a fiduciary for employee benefit plans would be allowed to execute securities transactions under certain circumstances.

History

The DOL proposal follows the Department’s June 29 request for information¹⁶, in which it sought public input on extending the applicability date of these exemptive provisions, as well as possibly changing the requirements of those provisions in the exemptions.

Given this request for information, **Mayer Brown** partner **Lenine Occhino** said that she “did not find the DOL’s August 9 proposed delay to be surprising, given that the comment period for the DOL’s most recent request for information in connection with its re-evaluation of the Rule just recently closed and over 500 comment letters have been submitted to date. The Department clearly needs more time in order to properly consider and address all the issues and get it right this time.”

The recent history of the DOL Fiduciary Rule and its related exemptions began on February 3, when **President Trump** issued a Presidential Memorandum instructing the Department to analyze the likely impact of the Rule on retirees receiving retirement advice (*ACA Insight*, 2/13/17¹⁶). On March 2, the DOL delayed both the Rule and the exemptions for 60 days, while also seeking public comment on general questions concerning both (*ACA Insight*, 3/6/17¹⁶).

On April 7, the Department adopted a final Fiduciary Rule that extended the applicability date of the Rule and its exemptions to June 9 (*ACA Insight*, 4/10/17¹⁶). On May 22, the DOL said it would not seek enforcement against fiduciaries until January 1, 2018, if those fiduciaries worked diligently and in good faith (*ACA Insight*, 6/5/17¹⁶).

Now the January 1 compliance date may be pushed back further. ☞

OCIE Finds

continued from page 1

What the exam staff found in Cybersecurity 2 was definite progress, but shortfalls. “In general, the staff observed increased cybersecurity preparedness since our 2014 Cybersecurity I Initiative (*ACA Insight*, 2/9/15),” OCIE said in the risk alert. “However, the staff also observed areas where compliance and oversight could be improved.”

“It’s good to see that OCIE noticed improvements since the 2014 examinations,” said **ACA Aponix** partner **Raj Bakhru**. “It was interesting that they noted that the vast majority of the examinations still resulted in one or more issues found. Our experience has also been that most firms have taken a number of steps since OCIE’s initial risk alert.”

While the progress is encouraging, said **Eversheds-Sutherland** partner **Brian Rubin**, “firms need to be vigilant and keep modifying their approaches as they make further improvements.”

The six-page risk alert provides an overview of OCIE’s observations, including issues it observed and suggestions for what firms should consider including in their policies and procedures.

Suggestions or prescriptions?

The SEC historically tends to avoid being prescriptive in its guidance. While there are no “do this” or “do that” statements in this risk alert, OCIE comes close to prescribing actions in several areas. For instance, it lists a number of policy and procedure elements that examiners found some firms effectively using, and suggests that other firms “consider” using them. It does the same with a list of issues that it believes “firms would benefit from considering.”

“Everyone should be going through these lists and seeing what they have and don’t have,” said **Mayer Brown** partner **Jeffrey Taft**. On the other hand, he said, not all the suggestions are right for all firms, given difference in, for instance, firm size, resources and cybersecurity risk assessment.

Policy and procedure elements

Among the items that OCIE wants advisers, funds and broker-dealers to consider are the following specific policy and procedure elements that it said a majority of those it examined were effectively using.

- **Maintenance of an inventory of data, information and vendors.** “Policies and procedures included a complete inventory of data and information, along with classifications of the risks,” OCIE said.
- **Detailed cybersecurity-related instructions.** OCIE suggested specific examples, such as detailed instructions for penetration tests, security monitoring and auditing, access rights tracking, and reporting when sensitive information is lost, stolen or disclosed.
- **Maintenance of prescriptive schedules and processes for data integrity and vulnerability testing.** The risk alert notes that some firms require vulnerability scans of core IT infrastructure to “aid in identifying potential weaknesses in a firm’s key systems, with prioritized action items for any concerns identified.” It also said that some firms beta test patches with a small number of users and servers before deploying them across the firm, with an analysis of the problem the patch was designed to fix, the potential risk in applying the patch, and the method to use in applying it.
- **Established and enforced controls to access data and systems.** As examples, OCIE noted that it observed that some firms put in place “acceptable use” policies that specified employee obligations when using a firm’s networks and equipment; required and enforced restrictions and controls, such as passwords and encryption software, for mobile devices that connected to the firm’s systems; required third-party vendors to periodically provide logs of their activity on the firm’s networks; and required immediate termination of access for terminated employees and very prompt (typically same day) termination of access for employees who left voluntarily.
- **Mandatory employee training.** “Information security training was mandatory for all employees

at on-boarding and periodically thereafter, and firms instituted policies and procedures to ensure that employees completed the mandatory training,” OCIE said.

- **Engaged senior management.** Effective firms had their policies and procedures vetted and approved by senior management.

Issues requiring action

Examiners also found situations where firms were not taking what it considers needed action. These are issues that “the staff believes firms would benefit from considering.” They include:

- **Policies and procedures were not reasonably tailored.** The policies and procedures here provided employees with “only general guidance, identified limited examples of safeguard for employees to consider, were very narrowly scoped, or were vague, as they did not articulate procedures for implementing the policies.”
- **Implementation.** “Firms did not appear to adhere to or enforce policies and procedures, or the policies and procedures did not reflect the firms’ actual practices.” The risk alert provided several examples. Among them, it said that the annual customer protection reviews were performed less frequently than required; that ongoing reviews to determine whether supplemental security protocols were appropriate were performed only annually or “not at all;” that “contradictory or confusing instructions for employees,” such as for customer access, were inconsistent with instructions for investor fund transfers; and that failing to ensure that all employees complete required cybersecurity training.

Separately, examiners found Regulation S-P issues among firms that “did not appear to adequately conduct system maintenance, such as the inability of software patches to address security vulnerabilities and other operational safeguards to protect customer records and information.” As examples, the risk alert says that examiners found “stale risk assessments” with firms using “outdated operating systems that were no longer

supported by security patches;” and a “lack of remediation efforts” by firms after penetration tests or vulnerability scans “did not appear to be fully remediated in a timely manner.”

Observations

Despite the above, examiners did find that firms had made progress in cybersecurity, with the most notable progress being that “all broker-dealers, all funds and nearly all advisers examined maintained cybersecurity-related written policies and procedures addressing the protection of customer/shareholder records and information.” This finding, it said, contrasted with its Cybersecurity 1 observation that “comparatively fewer broker-dealers and advisers had adopted this type of written policies and procedures.”

“In some respects, broker-dealers appear to be doing a better job than advisers,” said Rubin. “For example, while the vast majority of broker-dealers have mapped out steps they will take if they are breached, fewer than two-thirds of advisers and funds had similar plans.”

Here are some of OCIE’s more specific observations from its Cybersecurity 2 Initiative:

- **Risk assessments.** Nearly all broker-dealers and the “vast majority” of advisers and funds conducted periodic risk assessments of critical systems to identify cyber threats, vulnerabilities and potential business consequences of a cyber incident.
- **Penetration tests.** “Nearly all broker-dealers and almost half of the advisers and funds conducted penetration tests and vulnerability scans on systems that the firms considered to be critical.” That said, OCIE also noted that “a number of firms did not appear to fully remediate some of the high risk observations that they discovered.”
- **Data loss tools.** Some form of system, utility or tool was used by all the firms examined to “prevent, detect and monitor data loss as it relates to personally identifiable information.”
- **System maintenance.** While all broker-dealers and “nearly all” advisers and funds had a process in place

to ensure regular system maintenance, including the installation of software patches to address security vulnerabilities, the staff did find some problems. Specifically, examiners “observed that a few of the firms had a significant number of system patches that, according to the firms, included critical security updates that had not yet been installed.”

- **Response plans.** Nearly all the firms examined had plans for addressing access incidents and the vast majority had plans for denial of service incidents and unauthorized intrusions. When it came to plans for data breach incidents or notifying customers of material events, however, advisory firms and funds fell short. While the vast majority of broker-dealers maintained such plans, OCIE said, “less than two-thirds of the advisers and funds appeared to maintain such plans.”
- **Operational charts.** Cybersecurity organizational charts or other methods of identifying and describing cybersecurity roles and responsibilities were maintained by all broker-dealers and a large majority of advisers and investment companies.
- **Vendor risk assessments.** “Almost all firms either conducted vendor risk assessments or required that vendors provide the firms with risk management and performance reports,” such as internal and/or external audit reports and security reviews or certification reports. However, OCIE observed, “while vendor risk assessments are typically conducted at the outset of a relationship, over half of the firms also required updating such risk assessments on at least an annual basis.”

Revenue Sharing in Exchange for Investments May Be a Conflict

Perception counts. Consider a third-party broker-dealer offering an adviser compensation in exchange for investing client dollars in certain mutual funds available on the broker’s platform. The SEC is likely to perceive that compensation as a conflict of interest. It’s not so much whether the adviser follows through and makes those favored investments – it’s that the financial incentive to make them exists.

The SEC’s recent settlement¹⁰ with Seattle-based **KMS Financial**, a dually-registered adviser and broker-dealer may be a case in point. Since 1962, the advisory firm has worked with a clearing broker to provide trade execution, custody and reporting services with half of its investment clients. KMS itself limits its role to that of the introducing broker.

From at least 2002, according to the SEC, the clearing broker, with KMS’ okay, offered its no-transaction-fee (NTF) mutual fund program to advisers. For those KMS clients that took part, the clearing broker waived transaction fees that it and KMS would normally charge for the purchase of certain mutual funds available on its platform. “These payments provided a financial incentive for KMS to favor the mutual funds in the NTF program over other investments when giving investment advice to its advisory clients, and thus created a conflict of interest,” the agency said in its administrative order instituting the settlement.

But that’s not all, the agency said. In 2014, KMS negotiated a reduction in the execution and clearing costs it paid the clearing broker, but neither passed on that cost reduction in brokerage costs to its clients nor analyzed whether its clients were obtaining best execution,” the agency said.

“This case demonstrates that investment advisers should continue to be alert to any potential conflicts of interests in areas that are historical hot spots for the SEC, particularly those involving advisory fees, revenue-sharing and best execution,” said **Paul Hastings** partner **Thomas Zaccaro**.

“Firm’s should be vigilant in considering any financial arrangements with third parties that could either create a conflict or potential conflict, so that various means of addressing the conflicts can be evaluated, including at a minimum, disclosure, let alone other options such as accounting for the arrangement in a way that directly benefits clients or avoiding the conflict altogether, said **Faegre Baker Daniels** partner **David Porteous**.”

“A key takeaway for firms seeking to avoid these types of ‘conflict risks,’” he said, “is being able to demonstrate that they have a process to identify potential and

actual conflicts as well as to mitigate and/or eliminate the conflict.”

KMS was charged with willfully violating Section 206 (2) of the Advisers Act, which prohibits fraud; Section 206(4) and its Rule 206 (4)-7 for failing to adopt and implement a reasonable compliance program; and Section 207 for making untrue statements of material fact on its SEC registration application, the SEC said.

The arrangements

KMS took part in the clearing broker’s NTF program since at least 2002, the agency said.

Under one arrangement, the clearing broker agreed to share with KMS a certain percentage of revenues the clearing broker received from the mutual funds in its NTF program. “In particular, KMS waived transaction fees it and the clearing broker would otherwise charge clients for the purchase of certain mutual funds and instead would get a certain percentage of revenues the clearing broker received from certain mutual funds KMS recommended to its clients,” the SEC said.

This created a “mutual fund platform revenue stream to KMS,” the agency said, one that ran the risk that KMS would respond to the financial incentive of revenue

sharing by sending more clients to the clearing broker’s mutual funds.

It should be noted that the SEC, in its settlement, does not state that KMS ever acted on this arrangement by improperly placing clients in the mutual funds. The agency simply states that the conflict of interest where this could happen was created, and that, apparently, was enough for the SEC to bring charges.

Further, the agency noted that KMS, in its Forms ADV from 2003 to 2014 “did not disclose that it received payments from the clearing broker based on KMS client assets invested in the NTF program mutual funds or that these payments presented a conflict of interest. Nor did KMS otherwise disclose this conflict of interest to its advisory clients.”

Under another arrangement, KMS in February 2014 negotiated an amendment with the clearing broker that reduced the broker’s clearance and execution costs for equity, options and fixed income transactions by \$1 per trade, “thus decreasing total clearing and execution costs KMS had to pay the clearing broker for KMS clients utilizing the clearing broker,” according to the SEC’s administrative order.

TO SUBSCRIBE

Call:
(800) 508-4140

Web:
www.acainsight.com

E-mail:
subscribe@acainsight.com

Fax coupon at right to:
(301) 495-7857

Send check to:
ACA Insight, 8401 Colesville
Road, Ste. 700, Silver Spring,
MD 20910

**Multi-user web site
licenses are available!**

Yes, I would like to subscribe to *ACA Insight*. Please sign me up for a one year (46 issues) subscription and send me my password to www.acainsight.com.

NAME _____ TITLE _____

FIRM _____

STREET _____

CITY _____ STATE _____ ZIP _____

E-MAIL ADDRESS _____ PHONE _____

Payment — \$1,295 per year. Includes electronic versions, web access, and breaking news.
DC residents add 5.75% sales tax (\$74.46)

Bill me Check enclosed (make payable to *ACA Insight*)
 Please charge my Visa Mastercard Amex

CREDIT CARD NUMBER _____ EXP. DATE _____ SIGNATURE _____

Apparently, according to the agency, KMS, and not its clients, were the main beneficiary of this arrangement. The advisory firm “did not pass this reduction in clearing and execution costs on to its advisory clients, thereby providing KMS with \$54,957 of additional revenue on certain transactions involving the clearing broker from April 2014 through December 2015,” the SEC said.


The arrangement raised best execution questions. “When KMS entered into the 2014 amendment, which ultimately increased KMS’ revenue, KMS, in its capacity as an investment adviser, did not conduct an adequate analysis to consider whether those advisory clients continued to receive best execution in light of this increase,” the agency said. “Thus, KMS failed to seek best execution for its advisory clients.”

In terms of policies and procedures, the SEC charged that, in terms of both arrangements, the advisory firm fell short. “From 2002 to 2015,” it said, “KMS did not have adequate written policies and procedures for disclosing all material conflicts of interest.” In addition, the agency said, the firm’s written policies and proce-

dures “did not address best execution analysis regarding introducing, clearing and execution brokerage costs charged to advisory clients as part of its overall best execution analysis.”

The price paid

As part of its settlement, KMS agreed to notify advisory clients of the settlement. The firm will need to send advisory clients, and post prominently on its website, a link to the SEC’s administrative order instituting this settlement, and keep it on the site for six months. KMS also agreed to include a summary of the settlement, including a link to the administrative order, in the September 2017 quarterly statement from its clearing broker to KMS clients.

KMS, in addition to being censured, was ordered to pay disgorgement of \$382,569, plus prejudgment interest of \$69,518. Finally, the firm agreed, as part of the settlement, to pay a civil money penalty of \$100,000. An attorney representing KMS did not respond to an email or voice mail seeking comment. 

Published by:

ACA Compliance Group
(301) 495-7850
(301) 495-7857 (fax)
service@acainsight.com

Editor/Publisher:

Robert Sperber
(301) 502-8718
rsperber@acainsight.com

To Subscribe:

(800) 508-4140
subscribe@acainsight.com
Annual subscriptions (46 electronic issues, web access, and breaking news alerts) are \$1,295.
Multi-user site licenses are available.

Customer Service:

(800) 508-4140
service@acainsight.com

On the Web:

www.acainsight.com

Copyright:

Want to routinely share *ACA Insight* stories with your colleagues? Please contact publisher ACA Compliance Group at service@acainsight.com or (301) 495-7850 to obtain a multi-user site license. Routine, unauthorized copying of *ACA Insight*, including routine e-mailing of issues or individual stories, violates federal copyright law. To inquire about authorization, please contact publisher ACA Compliance Group at service@acainsight.com or (301) 495-7850.

© *ACA Insight*. All rights reserved.

ACA Insight is a general circulation newsweekly. Nothing herein should be construed as legal advice or as a legal opinion for any particular situation. Information is provided for general guidance and should not be substituted for formal legal advice from an experienced securities attorney.