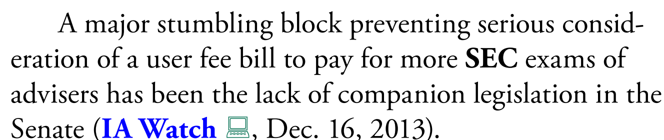
IA Watch
WEEKLY BRIEFING
COMPLIANCE NEWS, GUIDANCE & BEST PRACTICES

INSIDE...

Few Advisers Harmed by Cyber Attacks...... 2
A Warning about Custody & Checks.......... 3
CFTC Open to General Solicitation............ 4
Group to Examine Broker Fee Disclosure.... 5

September 22, 2014

Advocates for user fee bill have a Senate sponsor in the wings



A major stumbling block preventing serious consideration of a user fee bill to pay for more **SEC** exams of advisers has been the lack of companion legislation in the Senate (**IA Watch**, Dec. 16, 2013).

"There's a Democrat lined up on the Senate side willing to sponsor that bill," revealed **Skip Schweiss**, managing director of advisory advocacy for **TD Ameritrade Institutional** in Denver, in an exclusive interview with **IA Watch**. Schweiss declined to identify the Democrat, who is waiting for a Republican senator to sign on as a co-sponsor before coming forward. Advocates of the bill hope that will happen.

The user fee proposal is "an issue, that when we come up here to Washington, we don't hear any objections to," said Schweiss. However, the lack of participation in the political process by advisers hampers the advocates' efforts.

Often lawmakers or their staff ask "'where are the advisers? We're not hearing from them,'" said Schweiss. In contrast, the insurance, brokerage and real estate industries will produce thousands of calls, letters and visits when lobbying lawmakers. "I strongly encourage advisers to get more involved," he said. Visit your local lawmaker in their home offices, Schweiss suggested.

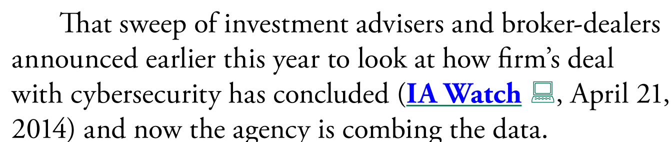
Fiduciary duty standard

Last week, TD Ameritrade brought together in Washington, D.C. investors, advisers, legislative staffers, industry association members and former regulators like **Robert Plaze.**

(Fees & Fiduciaries, continued on page 6)

IA Watch presents
IA COMPLIANCE 101 WORKSHOP
December 5, 2014
The Capital Hilton • Washington, DC
SAVE $300 when you register TODAY!
REGISTER TODAY! www.iawatch.com • 888-234-7281

A glimpse offered into early results of OCIE's cybersecurity sweep exam



That sweep of investment advisers and broker-dealers announced earlier this year to look at how firm's deal with cybersecurity has concluded (**IA Watch**, April 21, 2014) and now the agency is combing the data.

Examiners visited about 50 IAs and another 50 B-Ds, according to an OCIE source who spoke with **IA Watch**. "We found that the vast majority of advisers are conducting firm-wide inventories of their electronic resources," says the official. However, it varies widely as to which departments and individuals are in charge of these efforts.

Most advisers have written security P&Ps for electronic resources and "conduct periodic risk assessments to identify cybersecurity threats," says the official, while stressing that the sweep results are preliminary. The exams revealed that the "depth" of the P&Ps vary, as do how

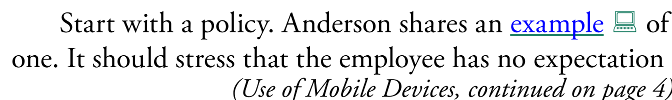
(Peek at Cyber Sweep, continued on page 2)

Steps to consider if you don't ban employee use of mobile devices for work

Odds are that within three feet of where you are lies your cell phone or other mobile device. These tools have become ubiquitous. It's tempting to use them for work. If your firm permits staff to do so, you should think about how this will affect regulatory compliance and could pose security risks.

Many firms ban the use of personal devices for work purposes unless they have been issued by the firm. Barring the use may be a waste of time. "You're not going to prevent [staff] from using their own devices," maintains **Jack Hewitt**, a director at **Gibbons** in New York. "They're going to use them anyway."

Whatever the decision, it should be made by the firm's leaders, including its CCO, says **Ben Anderson**, principal with **Anderson PLC** in Minneapolis. If the group elects to permit their use, decide which staff should get this right because the use triggers issues of privacy, security and recordkeeping, he adds.



Start with a policy. Anderson shares an example of one. It should stress that the employee has no expectation

(Use of Mobile Devices, continued on page 4)

Peek at Cyber Sweep (Continued from page 1)

frequently the risk assessments occur. More than one-third of retail advisers don't appear to be completing these assessments. Larger RIAs tend to be more sophisticated in their approaches to cybersecurity.

Many advisers also were found to have been assessing the adequacy of their security logins.

It's possible OCIE may initiate new cybersecurity sweep exams if a detailed review of the data suggests doing so, says the official. Otherwise, look for deeper results to be released in an upcoming risk alert or via public speeches by Commission staff. ■

State IAs experiencing few cybersecurity breaches, NASAA survey reveals

State-registered investment advisers still have work to do when it comes to cybersecurity practices, reveals a new survey from the **North American Securities Administrators Association**. It examines results of a pilot project designed to better understand how state-registered investment advisers were handling cybersecurity in the wake of an increase in cyber-attacks in the financial services industry.

A little more than 4% of responding firms indicated that they had experienced a cybersecurity incident. However, the survey revealed that firms could shore up their cybersecurity practices tied to securing e-mail, developing policies and procedures, authenticating client instructions and conducting risk assessments and training.

The survey of 440 state-registered investment advisers from nine states with AUM below $100 million found that 62% of firms have undergone a cybersecurity risk assessment. "The frequency of these assessments vary widely," noted NASAA. Of those firms hit with a cybersecurity event, just over 1% stated that they had experienced theft, loss, unauthorized exposure or unauthorized use of or access to confidential information.

P&Ps lacking

A troubling finding was that just under one in two firms (44.4%) reported actually having cybersecurity policies and procedures or training in place. Several states made the optional request that investment advisers submit relevant policies and procedures.

Fully 85% of state-registered investment advisers use computers, tablets, smartphones or other electronic devices to access client information. And while 92% of firms use e-mail to contact clients, only 50% of the firms use secure e-mail.

"State securities regulators are aware of the increase in cyber-attacks in the financial services industry, and the importance and associated difficulties of securely maintaining private data," said **Andrea Seidt**, NASAA President and Ohio Securities Commissioner. States participating in the pilot project used the survey as part of their examinations and inspections programs or as a separate survey or document request tool.

Additional NASAA jurisdictions plan to administer the template survey. ■

More than a dozen advisory firms settle short selling violations

It's déjà vu all over again. Nearly a year to the day that the **SEC** settled 22 cases tied to violations of short selling rules, the agency announced new settlements of rule 105 of Reg M breaches against 19 firms, including 13 investment advisers (**IA Watch**, Sept. 30, 2013).

(Short Selling, continued on page 3)

IAWatch SERVICE ACTIVATION FORM

Name ____________________

Title ____________________

Firm ____________________

Address ____________________

City ____________ State ______ Zip ______

Phone ____________________

Fax ____________________

E-mail ____________________

☐ **Payment Option 1:** Charge $2,495 to my credit card.

☐ **Payment Option 2:** Enclosed is my check or money order for $2,495 made payable to UCG (TIN: 26-3623723).

☐ **Payment Option 3:** Bill my company for $2,495.

Card # ____________________

Exp. Date ________ Signature ____________________

For fastest service, call TOLL FREE (888) 234-7281 or fax this card to (301) 287-2535.

IA Watch | 9737 Washingtonian Blvd., Suite 200 | Gaithersburg, MD 20878-7364 | (888) 234-7281 | Fax (301) 287-2535

Short Selling (Continued from page 2)

The culprits range in size from **Ironman Capital Management** ($78M in AUM) in Houston to Minneapolis-based **Whitebox Advisors** ($8.4B in AUM). The highest settled penalty went to **RA Capital Management** ($1.4B in AUM) in Boston, topping $3.5 million.

Rule 105 aims to prevent an equity purchaser in certain public offerings from selling the security short during a restricted period, which "is the shorter of … the period: (1) beginning five business days before the pricing of the offered securities and ending with such pricing; or (2) beginning with the initial filing of a registration statement or notification on Form 1-A or Form 1-E and ending with the pricing," according to the SEC.

Former CCO charged

Last week, the SEC also filed charges against **Sean Cooper**, the former co-owner and CCO at **WestEnd Capital Management** ($105M in AUM) in San Francisco. He's accused of overcharging hedge fund clients and stealing their money. The firm expelled Cooper in 2012. The adviser agreed to pay $150,000 and settled charges, including maintaining compliance policies and procedures that "were insufficient to prevent Cooper's fraud." The firm also failed to follow its procedures, for example, by not preventing staffers from using personal e-mail accounts for business.

Failing to timely file

Brown Brothers Harriman & Co. ($12.7B in AUM) in New York last week agreed to pay $120,000 to settle charges of violating Exchange Act requirements to report to the SEC the hitting of a beneficial ownership threshold. The rule calls on beneficial owners of more than 10% of a security's share class to report their ownership. Certain institutional investors, including investment advisers, can qualify for a reporting alternative to file a Schedule 13G instead of a Schedule 13D provided the filing comes within 45 days of the calendar year in which the beneficial ownership occurred and that the acquisitions were made "in the ordinary course of business" and not to control the issuer. ■

Custody: Adviser contemplates depositing checks for traveling clients

As a service to clients who travel extensively, an advisory firm is weighing offering to receive checks on their behalf and to deposit them into their bank accounts. There's no question this service would be considered custody by the **SEC**. We asked some experts whether the adviser should proceed – and heard words of caution (**IA Watch**, May 5, 2014).

The custody rule expects that an adviser that "inadvertently" receives tax refunds, securities, checks or the like would return these *to the sender* within three to five days. See question II.1 in the SEC's FAQs. In a 2007 "no-action" letter, the SEC warned that "an adviser could be out of compliance with the Rule if the adviser receives client assets and forwards those assets to a client or its custodian."

"The rule isn't flexible enough" to handle the situation contemplated by the adviser, says **Matthew Dallett**, a partner with **Edwards Wildman Palmer** in Boston. "Why stick your neck out when the client clearly is going to have … a lawyer [or] an accountant" who can deposit the checks on their behalf, he asks.

Maybe there's a way …

No doubt the situation the adviser describes constitutes custody, agrees **Heather Traeger**, a partner with **O'Melveny & Myers** in Washington, D.C., adding the checks should be returned within three days. However, she envisions a route an adviser could take to provide the service. It begins with the client having provided written instructions directing the adviser to deposit the check(s) and where to do so. "You'd want to have those on file," she says.

Other crucial documentation to keep would be a copy of the deposit slip and maybe even a copy of the client's bank statement, she adds. These documents should be made part of any surprise custody audit, Traeger adds.

Some complain the custody rule hasn't been updated to accommodate new ways of doing business. That 2007 "no-action" letter notes a situation similar to the one planned by the adviser. It reads that "temporary possession of a check made out to the client or a former client arguably is not 'possession' of 'funds' in that the check is not negotiated to the adviser and is not available for the adviser to cash or deposit. The adviser can only pass it along to a person or entity with authority to negotiate the instrument – the client or its custodian." And a bank would be considered a qualified custodian.

However, the agency didn't budge on giving these scenarios a green light.

All of this leaves Dallett recommending that clients set up these arrangements "with someone other than the adviser." The risks could be expanded because the rule mentions inadvertently receiving client checks and securities while the adviser's scenario isn't inadvertent – it's planned in advance, he notes.

(Custody & Checks, continued on page 4)

Custody & Checks (Continued from page 3)

A final best practice comes from **Michelle Jacko**, CEO of **Core Compliance & Legal Services** in San Diego. She has suggested keeping a log to record the receipt and the forwarding of any client checks. The log could include column headings: date funds/security received, from whom, client name, action taken, date action taken and notes. ■

Use of Mobile Devices (Continued from page 1)

of privacy if he elects to use his mobile device for work. This point can be made in a user agreement signed by the employee. This is necessary because some courts have interpreted the federal *Stored Communications Act* as implying employees do enjoy privacy protections with their devices, says Anderson.

Privacy vs. compliance

From a compliance standpoint, these privacy provisions could hamper a firm's ability to detect if an employee has abided by its P&Ps. The **National Institute of Standards and Technology** has released *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. The document warns that a firm may be able to verify a device's security only if it "controls the configuration" of the device. To do so, you need permission from the employee. A user agreement solves the issue.

But first you need to know that an employee is using his personal device for work. Anderson passes along a form staff must complete to get approval to use a personal device for work. A second form from Anderson allows for an employee to certify compliance with your P&Ps.

The next issue to address is security. Use of encryption and passwords and user names that change every 60 or 90 days is common, says Anderson. Some firms turn to technology that can wall off secure information into an online "container" so it doesn't reside on the actual device. **Good Technology** and **Drop Box** are two vendors. We've shared others before (**IA Watch**, Aug. 28, 2014).

Get all the benefits of a seminar without leaving your office!

LIABILITY: What Compliance Officers Can Do to Reduce Their Risk

Earn 1 CLE Credit or 1.5 CPE Credits

Live Webinar • Oct. 14, 2014 • 2:00 – 3:30 p.m.

REGISTER TODAY! www.iawatch.com • 888-234-7281

Another option is to "create a 'sandbox'" on the device itself that segregates work data, says Hewitt. There may even be technology that could wipe *only* the box's contents should the device be lost or its owner leaves the firm, he adds.

Married to technology

If all of this has you thinking you should have gotten a degree in technology, Hewitt says get used to it. The compliance role will be melded with IT's for the rest of your career. "This is not an easy task," he says, but a necessary one.

Anderson reminds that it's possible an employee has stashed certain documents – spreadsheets, models, research notes – on a mobile device that could be considered required books and records by a regulator. Your policy could call for the employee to hand over his mobile device periodically for an IT staffer to comb through it, he says. Employee certification semi-annually or annually may suffice, too.

Another alternative, according to the NIST report, is to have the mobile device connect with the firm's server, which would hold the sensitive data. The access to the data closes when the bond with the server is broken. Or your P&Ps could prohibit the storing of sensitive data – like Social Security numbers – on the mobile device.

Don't neglect to call for procedures in the event of a hacking incident or the loss or theft of a device, notes Anderson (**IA Watch**, Nov. 19, 2012). ■

CFTC acts on general solicitation, disclosure and recordkeeping

The wait's over if you're among those dually-registered advisers that hung back on using the new general solicitation authority to advertise private funds because you were waiting on the **CFTC** to follow the **SEC** in loosening the rules (**IA Watch**, Nov. 4, 2013).

A new "no-action" letter from the CFTC finally grants exemptive relief from Commission rules [regulations 4.7(b) and 4.13(a)(3)] that were seen to block general solicitation. The new letter harmonizes the CFTC's with the SEC's liberalization following enactment of the JOBS Act (**IA Watch**, July 15, 2013).

The CFTC applies conditions for the exemptive relief. One is you must alert the Commission by e-mail that you seek the relief. "You can well imagine in a future audit" that any entity that claims the relief will be asked about compliance with the general solicitation rules, says **Josh Sterling**, a partner with **Bingham McCutchen** in Washington.

(CFTC Relief, continued on page 5)

CFTC Relief (Continued from page 4)

"I would expect to see some more hedge funds" doing general solicitation thanks to the new relief, he adds. These hedge funds would likely be start-ups and smaller funds.

The CFTC's relief is limited to commodity pool operators that are issuers under the SEC's rules 506(c) and 144A.

Recordkeeping

A second new CFTC letter offers exemptive relief to permit CPOs to use third-party record-keepers. This is "another example of the CFTC staff trying their best to line up their rules with reality," says Sterling. The only catches are that the records must be provided to the CFTC within 48 hours of a request and the CPO will be held responsible if the third party fails in its role.

This new letter states that the CFTC plans to review a regulation that some have implored it to revise to fit with the modern world. In July, the **Managed Funds Association** petitioned the CFTC to revise regulation 1.31 (electronic records must be preserved in a nonrewritable, non-erasable format). The MFA has pushed for a rule that "substantially" mirrors Advisers Act rule 204-2(g) (books and records rule). The new letter indicates the Commission will review regulation 1.31's "applicability to the current technological environment."

Two other new "no-action" letters from the Commission ease disclosure responsibilities for commodity pools and their wholly-owned subsidiaries and give certain CPOs exemptive relief from other disclosures.

The rash of new letters reflects that Congress's gridlock on the CFTC has broken. The CFTC now has a full Commission and an approved budget. ■

Regulators and broker-dealers to work together on improved fee disclosure

Securities regulators, broker-dealers and other financial institutions will form a working group to figure out how to make brokerage fee disclosures easier for investors to understand, **NASAA** announced during its annual conference last week.

NASAA spokesman **Bob Webster** said the working group would not scrutinize the fees themselves, only how they're disclosed. "They're going to try to develop a plan for simple, concise fee disclosure," he said. Whether that means a uniform fee disclosure document that all firms will have to use or something else remains to be decided, he said.

The idea to form the working group arose from a study that NASAA released last April that found "a wide disparity among firms in the way fees were disclosed." For example, the study revealed that fee disclosure documents that firms sent to their customers varied from one paragraph to seven pages and "the actual fee verbiage itself was sometimes buried within a document having an overall length of between one and 45 pages."

The 14-page *broker-dealer and registered investment advisor fee disclosure* from **TransAmerica Financial Advisors** doesn't disclose any fee amounts. You must wade through 21 pages of **UBS's** fee disclosure document before getting a clear descriptions of various fees.

SIFMA , **FINRA** and NASAA say it's too early to know who will be appointed to the working group. Others who will appoint members to the group are the **Financial Services Institute**, **Bank of America**, **Wells Fargo**, **Merrill Lynch**, **LPL Financial**, **Edward Jones**, **Prospera Financial Services** and **Signator** investments, NASAA said.

"There's a great variety of fees," said FSI Executive Vice President **David Bellaire**. "Each firm has different terms to describe the fees. Sometimes those descriptions aren't very helpful."

He said the working group's goal "would be to provide investors with an easy-to-use disclosure document" that would allow them to clearly compare fees among firms.

NASAA has given the task force one year from its first meeting to produce a proposal. ■

IM Director cautions on alternative mutual fund compliance issues

Hedge fund advisers lured by rapid growth in the more than $300 billion alternative mutual funds market are increasingly becoming involved with the funds either as subadvisers or by launching their own registered investment companies. Last year alone, there were $95 billion of inflows into alternative mutual funds—five times more than 2012.

This growth has certainly caught the **SEC**'s attention and an alternative mutual funds sweep exam is ongoing (**IA Watch**, Aug. 28, 2014). In a speech last week, the SEC's Director of the Division of Investment Management **Norm Champ** cautioned private funds advisers that alternate mutual funds present heightened compliance risks with conflicts of interest, valuation, portfolio management and marketing.

(Mutual Fund Warning, continued on page 6)

Mutual Fund Warning (Continued from page 5)

Champ noted that managing a registered fund is “very different” from managing a private fund. ■

Read more from this story at www.iawatch.com. ■

Fees & Fiduciaries (Continued from page 1)

Besides the prospect for more IA exams, they talked about possible action by the SEC to redefine the fiduciary duty standard. “They don’t think the fiduciary rulemaking will occur,” said Schweiss.

There’s little consensus around the issue and “the SEC has an extremely difficult assignment coming up with something that is ‘no less stringent’ than [the Advisers Act’s standard] .... I’m just not sure how you do that” and whether it could withstand legal challenges, he maintained.

Plaze, who spent years in the SEC’s Division of Investment Management and is now a partner with **Stroock & Stroock & Lavan** in Washington, D.C., told the gathering to not “‘let the perfect be the enemy of the good,’” said Schweiss. Find a middle ground. Plaze suggested a “best interests standard” for B-Ds and for advisers to continue to function under the Advisers Act standard.

Editor’s Note: Click the box to the right to watch a 2:20 video interview of Schweiss discussing user fees. ■ below. To see a 2:00 **IA Watch** video featuring Schweiss talking about the fiduciary duty standard, click here. ■

NSCP THE NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS
FOR COMPLIANCE ✦ BY COMPLIANCE

BENEFITS OF MEMBERSHIP
GROW YOUR NETWORK :: TAKE CHARGE OF YOUR CAREER
BROADEN YOUR KNOWLEDGE

AS A MEMBER, YOUR BENEFITS WILL INCLUDE:
Access to the NSCP Member Directory;
Access to the NSCP Resource Library, a compendium of forms, checklists, policies and procedures;
NSCP Currents, our monthly compliance journal;
Meeting and Training materials discounts.

The benefits of joining NSCP are invaluable to your current and future career goals; don't miss out!

CALL: 860.672.0843 :: **VISIT:** www.nscp.org
EMAIL: membership@nscp.org

Group Publisher: Hugh Kennedy
301-287-2213 | hkennedy@ucg.com

Publisher: Carl Ayers
301-287-2435 | cayers@iawatch.com

Contributing Reporter: John Brinkley

IA Watch strives to provide you with accurate, fair and balanced information. If for any reason you believe we are not meeting this standard, please let us know.

Our Address: IA Watch
Two Washingtonian Center
9737 Washingtonian Blvd., Suite 200
Gaithersburg, MD 20878-7364

Subscriptions:
For questions about newsletter delivery, address change or online access, call our Customer Service department at (888) 234-7281. This symbol means a link to the web.

Register to attend our *IA Compliance 101 Workshop* in Washington, D.C. on Friday, December 5th. Find out more at http://www.iawatch.com/IACompliance101/.

Site Licenses for your firm:
If you are a subscriber, members of your firm qualify for a multi-user site license at a significant discount. Call our Site License Department at (888) 234-7281 and get access tomorrow at 7 a.m. Ask for Marge Gold (301-287-2353; mgold@iawatch.com).

The IA Watch weekly briefing is a general circulation weekly focused on regulatory and compliance issues in the investment adviser community. Nothing within should be interpreted as offering investment advice or legal counsel. Find us at www.iawatch.com.

Copyright 2014 UCG/IA Watch

The *IA Watch weekly briefing* is published 48 times a year by UCG. The yearly subscription rate is $2,495. COPYRIGHT NOTICE 2014. *No portion of this publication may be reproduced or distributed without the written permission of the publisher. IA Watch* shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal photocopying or electronic distribution. To report violations contact: Steve McVearry, UCG General Counsel, Two Washingtonian Center, 9737 Washingtonian Blvd., Suite 200, Gaithersburg, MD 20878; Confidential line: 301-287-2266 E-mail: smcvearry@ucg.com. For photocopying and electronic redistribution permission, please call Marge Gold at 301-287-2353 or mgold@iawatch.com.