IAWatch
WEEKLY BRIEFING
COMPLIANCE NEWS, GUIDANCE BEST PRACTICES

INSIDE...

April 25, 2016

National Exam Program deputy director reveals on-going and planned initiatives

The **SEC** will remain focused on never-before-examined investment advisers and investment companies and hopes to ratchet up the number of exams it conducts with a larger IA/IC exam team going forward. The current rate of enforcement referrals from NBE firm exams is "significantly lower" than those for risk-based exams, reported **Jane Jarcho**, deputy director of the SEC's National Exam Program. She spoke at the Commission's April 19 Compliance Outreach Program in Washington, D.C.

Jarcho noted that the SEC has now conducted 730 never-before-examined firm exams. Another 160 such exams are underway. While enforcement referrals are down for NBE firms, Jarcho stated the deficiencies being discovered are similar to those being detected on risk-based exams (e.g. books and records violations and custody issues).

Never-before-examined investment companies also are facing scrutiny. The Commission has examined about 30 never-before examined fund complexes. Jarcho stated that examiners are taking a look at such areas as compliance with rule 38a-1 (compliance procedures and practices of certain investment companies), sales literature, advertising, valuation, leverage, use of derivatives and proxy voting.

Initiatives status

At the Compliance Outreach Program, which was tailored to IA/IC senior officers, Jarcho outlined on-going

(OCIE Initiatives, continued on page 5)

In this election season, OCIE asking advisers about political contributions

Some may flinch at the thought of government asking private entities for the names of staffers who have made political contributions but OCIE's doing just that – using these inquiries as a means to track compliance with the **SEC**'s pay-to-play rule.

OCIE's 2016 exam priorities letter vowed it would examine public pension advisers (**IA Watch**, Jan. 14, 2016). **IA Watch** has obtained a document request letter that focuses on PTP. It requests names of all covered associates under the rule – including their "residential address" – as well as all government entities "to which the adviser" has provided IA services over the past five years.

OCIE also wanted to see all "direct or indirect" political contributions by associates "to an official of a government entity, and payments to a political party of a

(OCIE Exams, continued on page 2)

Compliance actions to take so B-Y-O-D doesn't turn into t-r-o-u-b-l-e

If you thought taking away grandma's car keys was tough, try prohibiting your colleagues from using their cell phones for work.

"You can never prohibit it today because it's a work habit," says **Mike O'Shaughnessy**, VP of guidance at **Advisor Armor** in Scottsdale, Ariz.

Still, some firms swim against the tide, fearful of cyber risks. Staff at **Trumbower Financial Advisors** ($1B in AUM) in Bethesda, Md., don't work from home or use their tablets or iPhones for work, assures **Karen Hunt**, the firm's operations associate.

The four employees at **Alexander Capital Advisors** in New Canaan, Conn., cannot access their work e-mails on their iPhones, says **Dina Myers**, senior compliance associate. Well, only one: the company owner. "We didn't want a lot of devices with company information out there," says Myers.

It is preferable to not allow employees to BYOD (bring their own devices to work), but it's not realistic in most cases to prevent it, agrees **Pamela Gupta**, president

(BYOD to Work, continued on page 3)

OCIE Exams (Continued from page 2)

(**IA Watch**, July 7, 2014) – drew interest. Examiners pressed on what the adviser does to assess best execution under these circumstances.

"You need to be doing an analysis" of these costs, implores the CCO. The firm's evaluation eyes one year's worth of trades based on bid-ask spread, daily trading dollar volume, security and market capital and comes up with medians and averages, says the CCO.

Another technique you may wish to add to this analysis relies on execution expenses provided by sponsors of model-based programs. The adviser compares these costs against the execution expense of the step-out trades "on the theory that the model trading desk of the sponsor is probably getting exactly ... or similar execution [costs] that they would get" within the wrap program itself, states the CCO.

Soft dollars

Another topic to be on the lookout for is soft dollars, especially mixed use, says the CCO (**IA Watch**, March 19, 2015). Be sure to have a paper trail that's specific. Review your software usage at least annually and understand what products you're getting through soft dollar benefits, counsels the CCO. For example, know how many **Bloomberg** terminals your staff uses and instruct them to alert compliance when terminals are added or removed. ■

BYOD to Work (Continued from page 1)

of **Outsecure** in Shelton, Conn.

A sort of middle ground

Wedgewood Partners ($6.3B in AUM) in St. Louis, lands on middle ground. Employees "can only use their device in the office," says CTO **Steve Rolfe**. The firm uses an "intrusion protection device" that acts as a firewall and keeps wireless traffic off of the adviser's network.

Staff also must agree to use the **Microsoft Outlook App** on their phones rather than connecting them to the firm's e-mail system – for extra security, says Rolfe. The adviser is moving toward using the Microsoft Cloud Services/Apps to allow employees to connect any device using multifactor authentication security. It may even introduce a VPN option in the future, he says.

A South Carolina adviser permits BYOD. Two key compliance P&Ps govern the activity. "You have to sign an acceptable use policy and a remote use policy," says the firm's CCO. In doing so, employees agree to permit the firm to monitor their device. The employees must review and annually attest to follow both policies.

The policies give the firm the ability to remotely wipe the device under certain scenarios. If an employee were to tap in his password incorrectly three times, "they're going to wipe it because the deduction will be that somebody's stolen your phone," the CCO states.

The disappearing device

"This is non-negotiable," states Gupta of the need for employees to sign agreements that permit their employer to remotely wipe a device that might fall into the wrong hands. But employees must "know that going in," she says. Make sure they understand the implications, Gupta adds.

Consent is necessary before taking such drastic actions under the federal *Stored Communications Act* (**IA Watch**, Sept. 18, 2014). Some employees have sued under the law because of their employer's access to their devices, although none of the lawsuits originated in financial services, says **Ben Anderson**, principal with **Anderson PLC** in Minneapolis.

Although O'Shaughnessy's not a fan of software that permits the wiping of devices, he recognizes the risks should a bad guy worm his way through a phone, tablet or laptop containing sensitive information and remotely connect to a business's system. He provides examples of a BYOD acceptable use policy and a remote access control P&P. Gupta passes on an example of a BYOD agreement.

"It's actually pretty simple" to remove an employee from a firm's server when someone is leaving on good terms, says **Fred Shane**, chief risk officer at **Commonwealth Financial** in Waltham, Mass. The policy calls for human resources and IT staff to disconnect the employee. It could go so far as to call for the employee to show that the device contains no company data.

An unfriendly split

The challenge comes when the parting is not so

(BYOD to Work, continued on page 4)

BYOD to Work (Continued from page 3)

friendly. "They could be susceptible to a remote wipe," says Shane. But "what if they had important information on it," such as medical data, he asks.

A separation agreement could hold the person to wipe items like a tablet left at home, he adds.

If you're intent on getting technology that can launch remote wipes, Anderson notes two vendors are **Good Technology** and **MobileIron**.

Long before you arrive at this stage, first take an inventory of all devices that can access your system, recommends **Jyotin Gambhir**, managing director of **SecureFLO** in Arlington, Mass. His other tips:

√ Keep the devices current with the most recent data security patches.

√ Hold the employee accountable to use authentication to gain access to your network.

√ Encrypt the data on the devices or make them encryptable (they should have the capability to accept levels of authentication tokens).

√ Install some type of malware detection software (**Trend Micro** and **Security 360** are two types).

√ Consider using endpoint-level protection, which eyes traffic coming from remote devices so that a device can be jettisoned from the network if trouble's detected.

Be sure to hold 2-4 cyber training sessions annually, even if they're as short as 30 minutes, suggests O'Shaughnessy. Malware designed for mobile devices will surpass computers in 2017, he predicts, pointing to the increased need for precautions. "The bad guys have this figured out, too," he says of the trend toward work and devices.

Be consistent and fair with any disciplinary action assessed against violators of your BYOD P&Ps, says Shane. Steps could include re-training, notifying management or disconnecting one from the network.

Editor's Note: Hear cybersecurity best practices at **IA Watch**'s *Cybersecurity for Financial Services* conference May 16 in Washington, D.C. To see the agenda, click here. ■

FSOC concerned about leverage at hedge funds

In a bid to better assess the relationship between a hedge fund's level of leverage and corresponding risk, the **Financial Stability Oversight Council** is moving on an initiative to evaluate the sufficiency of data currently being reported, including on Form PF. FSOC released an update April 18 on its review of potential risks to U.S. financial stability that may arise from asset management products and activities and offered up some next steps.

FSOC's evaluation of risk focused on: 1) liquidity and redemption; 2) leverage; 3) operational functions; 4) securities lending; and 5) resolvability and transition planning. It is the leverage risk section that has garnered a fair amount of industry discussion. The release comes only days after it lost a court decision reversing its declaration of an asset manager as a systemically important financial institution (**IA Watch**, April 7, 2016).

Concentrated leverage

FSOC reported that an analysis of Form PF data showed that while many hedge funds use "relatively small amounts" of leverage, leverage appeared to be concentrated in larger hedge funds. The Council is concerned that Form PF does not provide "complete information on the economics and corresponding risk exposures of hedge fund leverage." A further concern is that no single regulator has all the information necessary to evaluate the complete risk profiles of hedge funds.

To combat those concerns FSOC has determined to create an interagency working group—comprised of experts from the relevant FSOC agencies—who will share and analyze pertinent regulatory information. The goal is to gain a better understanding of the activities of hedge funds and to ultimately determine whether they pose potential risks to financial stability.

Augmenting data

The working group has been tasked with using available data to "evaluate the use of leverage in combination with other factors—such as counterparty exposures, margining requirements, underlying assets, and trading strategies—for purposes of assessing potential risks to financial stability." The group will further consider how existing data reported on the likes of Form PF could be augmented to improve the ability to make such risk evaluations. *(FSOC's Concerns, continued on page 5)*