




IA Watch Exclusive: Cyber Sweep Letter	1
Fidelity Hit with Another Lawsuit.....	4
Regulators Share Their Views on Issues	4
Tool: Cybersecurity Glossary.....	5

April 1, 2019

High Court hands the SEC a victory in case tied to misleading e-mails

The **Supreme Court** March 27 by a 6-2 vote ruled that a key Exchange Act rule permits a defendant to be liable for sending investors misleading e-mails even when the messages were written by the staffer's boss.

In *Lorenzo v. SEC*, the Justices sided with the **SEC**, which had brought charges against **Frank Lorenzo** in 2013 and later fined him for securities violations ([IA Watch](#) , Jan. 6, 2014). The High Court's ruling clarifies the regulator's use of Exchange Act [rule 10b-5](#)  (employment of manipulative and deceptive devices) following disparate rulings by several lower courts.



The decision follows a High Court ruling eight years ago in *Janus* that cleared an adviser under rule 10b-5 because the communications at question weren't made by the communicator ([IA Watch](#) , June 20, 2011). The new decision focused on rule 10b-5(a) ("To employ any device, scheme, or artifice to defraud") while *Janus* was limited to rule 10b-5(b) ("To make any untrue statement of a material fact").




What happened


Lorenzo worked as director of investment banking with the B-D **Charles Vista** on Staten Island, New York, in 2009 when his boss directed him to send two e-mails to prospective investors about an opportunity to buy debentures. The boss had written that the firm selling the securities had "confirmed" assets of \$10 million. But Lorenzo knew the real figure was less than \$400,000. Still, Lorenzo sent the e-mails under his name.

(High Court Ruling, continued on page 2)

OCIE's cybersecurity sweep #3 letter zeroes in on branch offices

Last month we reported that the **SEC's** latest cybersecurity sweep exam is in full swing ([IA Watch](#) , March 14, 2019). Now **IA Watch** shares with you a copy of OCIE's document request letter .


An advisory firm received the request letter recently, according to our source. The 6-page, 42-question request letter contains many similarities to OCIE's second cybersecurity sweep letter  ([IA Watch](#) , June 7, 2016). However, there are differences that reflect the improved sophistication the regulator possesses – no doubt borne of its own cybersecurity travails ([IA Watch](#) , Jan. 17, 2019).


It's been five years since OCIE launched its initial cybersecurity sweep exam ([IA Watch](#) , April 21, 2014). The agency has made no secret of its continuing interest *(Cyber Sweep 3, continued on page 2)*

Examples of how your peers are seeking to strengthen their vendor contracts

The latest twist in OCIE's ongoing interest in how you're protecting your firm's cybersecurity plunges into how deeply you're scrutinizing your vendors' cyber protections.

Ben Anderson, principal with **Anderson PLC** in Minneapolis, reports examiner interest stretching from Boston to San Francisco probing how advisers are measuring their vendors' cybersecurity. "The focus is on material vendors," he says, meaning those that have access to your sensitive data.

Once again, cybersecurity appears among OCIE's 2019 exam priorities. This will probably be an annual occurrence as long as cyber bad guys ply their sinister trade on the Internet ([IA Watch](#) , Jan. 2, 2019).

IA Watch asked CCOs recently how they're revising their vendor contracts – when they have the power to do so – and most noted they're focusing on cybersecurity ([IA Watch](#) , March 31, 2014).

Sailingstone Capital Partners (\$4.6B in AUM) in San Francisco hired outside counsel to review three *(Vendor Deals, continued on page 3)*

11th ANNUAL
IA Compliance
The Full 360° View Southwest

Proven-in-Practice Guidance to Keep Your Compliance Program Sharp

JUNE 7, 2019
Fairmont Dallas
Dallas, TX

SUBSCRIBERS SAVE 150! REGISTER NOW!

www.iawatch.com/dallas2019



High Court Ruling *(Continued from page 2)*

Justice **Brett Kavanaugh** had recused himself from the Lorenzo case. ■

This story first appeared as breaking news at www.regcompliancewatch.com on March 27. ■

Vendor Deals *(Continued from page 1)*

vendor contracts and to suggest changes. “We chose our three highest dollar contracts,” says CCO **Kathlyne Kiaie**.

A data security addendum

The exercise resulted in a data security addendum. “It can be appended to any standard vendor contract to ensure that you are protected on the info-tech front,” says Kiaie. The addendum deals with industry standards; data safeguards; security audits; required notification of a cyber incident within 24 hours; connecting to the adviser’s network; EU data protections and more.

Clark Capital Management Group (\$7.2B in AUM) in Philadelphia has sought to harden provisions limiting the firm’s liability and indemnification to decrease the firm’s cybersecurity risks, says CCO **Conor Mullan**.

Congress Wealth Management (\$1.6B in AUM) in Boston updated cybersecurity clauses to match Massachusetts’ legal definitions of personally identifiable information. CCO **Candace Cavalier** also pushed a clause requiring the vendor to notify the firm of a breach and insisting that the vendor acquire cybersecurity insurance.

It’s natural to seek these types of provisions only with vendors that have access to your sensitive data. “It depends upon the services that they’re providing,” says **Joseph McDermott**, CCO at **THL Credit Senior Loan Strategies** (\$3.7B in AUM) in Chicago. So language that binds a vendor to protect the firm’s data won’t make its way into a contract with the adviser’s pricing vendor, notes McDermott.

Lacking clout

Many advisers can’t insist upon contract clauses. “We’re too small to effect any change in a contract,” says **Jillian Carlson**, CCO at **ICW Investment Advisors** (\$146M in AUM) in Scottsdale, Ariz.

ICW has contracted with a vendor to help check on its other vendors. The RIA has hired **Vendor Insight** to do due diligence on its vendors. “It is extremely expensive,” notes Carlson. The cost is about \$1,200 per vendor. For that price, the RIA gets a vendor’s SOC1

report, a confirmation the vendor has insurance, and a peek at the vendor’s cybersecurity, BCP and privacy policies, she adds. Vendor Insight produces a report on each vendor ICW asks about.

Vendor Insight also will look into the cybersecurity of 4th parties, that is the vendor’s vendors, noted Carlson.

Who owns your data?

Don’t forget who owns the data in your vendor contracts, states **Peter Maftciu** with **Sound Compliance Services** in Gig Harbor, Wash. Your contracts should detail what happens to your data should you change vendors. This is important because the **SEC** could consider the data a required book and record that you should have access to, he adds (**IA Watch** ■, July 9, 2012).

Another important provision sets out when the vendor would have to notify you of a data breach. It’s reasonable to give a vendor some time to assess a potential breach, says attorney, author and former RIA CCO **Tery O’Malley**. He believes one week is a fair deadline for a vendor to report a breach.

He also recommends another clause that’s unrelated to cybersecurity. This would be a non-disclosure provision. Say, an adviser obtains certain information under an NDA. This clause would allow the adviser to share that information without notifying the other party should the topic come up in a routine SEC exam. “If you don’t ask for that carve out, you could find yourself in a situation where” you have to notify parties of a routine exam, O’Malley notes.

11 provisions to consider

There are many other clauses you may consider for your contracts. One [source](#) ■ recommends 11 key provisions: 1. A relationship clause (defining how the two parties will work together); 2. Contract term and termination; 3. Services (what are you getting?); 4. Payment; 5. Insurance; 6. Indemnification; 7. Protection of confidential data or non-disclosure; 8. Intellectual property (data ownership); 9. Compliance with laws; 10. Governing law and jurisdiction; and 11. Arbitration.


Maftciu has seen advisers insist on a non-compete clause. This would prevent a consultant from revealing to third parties an adviser’s investment strategy.

Carlson notes she has been working with her custodian **Fidelity** for more than a year trying to get the firm to change a liability provision in its contract. Fidelity insists the adviser assume the liability when using a third-party vendor, even one that Fidelity recommended and

(Vendor Deals, continued on page 4)

Vendor Deals *(Continued from page 3)*

that uses the custodian's data feed. She reports progress on the negotiations but no resolution yet.


Anderson shares a [vendor contracting checklist](#)  he has created. He saves a more formal version for his clients but this checklist can be a good starting point for you. It would list provisions (e.g., description of products, fees, most favored nations clause, etc.) and what would be necessary for each (e.g., representation, warranty, covenant or negative covenant).

Take cybersecurity again. You may wish for the vendor to warrant that it uses "some type of commercially reasonable test," like a penetration test, to detect cyber weaknesses. Next, a covenant would have the vendor pledging to maintain recognized cybersecurity standards to detect and deter intrusions and to notify you of breaches, says Anderson.

If you happen to have enough clout, you next may mandate real-time reporting of cyber test results and even the right to visit the vendor's offices to assess its cybersecurity program in-person, he adds. ■

Fidelity hit with a second lawsuit over mutual fund 'infrastructure' fees

Three separate 401(k) investors have joined to file a new federal lawsuit claiming **Fidelity** violates its fiduciary duty and ERISA by charging mutual funds a fee to gain access to the firm's platform.

The [complaint](#)  filed in U.S. District Court in Boston follows a similar lawsuit launched last month, and an inquiry to Fidelity over the issue by Massachusetts authorities ([IA Watch](#), March 8, 2019).

As with the first lawsuit, Fidelity "emphatically" denied the allegations. The custodian vowed to fight "this lawsuit vigorously. Fidelity fully complies with all disclosure requirements in connection with the fees that it charges and any assertion to the contrary is not only misleading, but simply false."

"As a fiduciary for thousands of Savings Plans, Fidelity must act prudently and in the sole interest of these plans and their participants and beneficiaries," reads the latest lawsuit in *Summers v. FMR*.

As with the earlier lawsuit, this legal action claims Fidelity has been charging for at least three years "an 'infrastructure' fee," which the suit claims is "an illegal and undisclosed pay-to-play fee" that gets passed on to investors.

This lawsuit reveals that "Fidelity warned mutual

funds in written materials that any fund refusing to pay the Fee would 'be subject to a very limited relationship' with Fidelity." It goes on to claim the fees are really kickbacks in exchange for appearing prominently on Fidelity's platform.


Fidelity responded. "We are committed to remaining an open architecture platform that provides access to thousands of funds to all of our customers, but such a broad offering requires substantial infrastructure. For example, Fidelity must support systems and processes needed for recordkeeping, trading and settlement, make available regulatory and other communications, and provide customer support online and through phone representatives. It is costly to maintain this kind of infrastructure, and Fidelity requires the fund firms on our platform to compensate us for those costs. For a small number of those companies, this includes an infrastructure fee that is charged to the fund firms. The fee is not charged to the plan sponsor or plan participants."

The plaintiffs seek class-action status, a jury trial and penalties and disgorgement. ■

This story first appeared as breaking news at www.regcompliancewatch.com on March 22. ■

Regulators sound off at SIFMA conference

They are, in the words of one moderator at **SIFMA's** annual compliance and legal conference, "the folks ... who have the potential to make your life miserable." Regulators dotted the Phoenix-based conference last week.

Among the revelations were that **FINRA** wants the power "to lower the boom on the defiant non-compliant" without having to get a final enforcement order, said **Robert Colby**, FINRA's chief legal officer ([BD Watch](#) , July 26, 2018). The SRO is concerned that enforcement actions drag on while investors continue to be harmed. "We hope to get inched towards the bank model where what the examiner says has more impact," Colby said.

The intended quarry: Firms that ignore exam findings and recommendations "over and over again" and firms "at the 97% outlier level based on their record," said Colby.

"We know our task here will be to convince the firms and the **SEC** that we could be trusted with this new approach," Colby said, acknowledging industry concern that due process rights of firms in the cross-hairs could be compromised.

The largest crypto-currency firms late last year
(Regulators Talking, continued on page 6)