

ACA Insight

The weekly news source for investment management legal and compliance professionals

“The key thing is to let clients know that cybersecurity is a top priority, and that their data is considered one of their most valuable assets.”

Cybersecurity: Best Practices to Reassure Anxious Clients

Every few weeks, it seems, a major company is in the news because a hacker breached its cybersecurity system. Confidential information, including personal identification data like social security numbers, account numbers and emails, are stolen. What can advisory firms do to reassure justifiably concerned clients and prospective clients that their information is well protected?

It's not as easy as it sounds, and the first rule is not to give ironclad guarantees, because there are none, as any system may be breached. But there are steps advisory firms can take to demonstrate to clients that the possibility of hacking is taken seriously, and that your firm is taking all necessary steps to protect their information.

[continued on page 2](#)

SEC Catches a Big Fish in Its 12b-1 Fee Dragnet

The SEC shows no sign of letting up in its scrutiny of investment advisory firms that place clients in more expensive share classes when less expensive class shares of the same securities are available. It reached a settlement with a small, financially troubled adviser last month, and early this month settled charges with a large financial institution, **Credit Suisse**, and one of its investment adviser representatives.

Credit Suisse and its IAR, **Sanford Michael Katz**, will pay almost \$8 million to settle charges that they placed clients in more expensive “Class A” shares of mutual funds while less expensive “institutional” shares were available. The added expense of

[continued on page 3](#)

Check on Disclosure Across All Firm/Client Interactions

There's no doubt that disclosure is a major issue for the SEC – so much so that the agency is often referred to, perhaps somewhat inaccurately, as a “disclosure agency.” Smart chief compliance officers would therefore be wise to monitor and enforce disclosure requirements horizontally across all areas where firm actions affect their clients.

The “disclosure agency” appellation is somewhat inaccurate because not every enforcement action the SEC takes has a disclosure component. For instance, said **Stradley Ronon** partner **Lawrence Stadulis**, “You can't disclose away non-compliance with the Custody Rule.”

[continued on page 6](#)

Cybersecurity

continued from page 1

“The key thing is to let clients know that cybersecurity is a top priority, and that their data is considered one of their most valuable assets,” said **ACA Aponix** consultant **Jose Ramos**. Share with them that a layered security approach is the only way to protect client data. Such an approach is a combination of administrative, technical, and physical controls. Encryption, annual assessments and penetration testing, employee training, and physical security are just a small portion of what goes into securing a client’s data.

“Be as proactive and as transparent as possible,” suggested **Eversheds-Sutherland** partner **Mark Thibodeaux**. “Let clients know the steps you take: ‘We encrypt data, only people who absolutely need to see confidential information are able to do so, we hire white-hat hackers who test our systems, we provide you with identity-theft protection, if you in fact take these steps.’”

Best practices

Let’s explore some of these ways to reassure clients and potential clients, as well as others, in more detail.

- **Assessment and certification.** Certified professionals from a well-respected cybersecurity firm may go a long way to reassuring those concerned that your firm will take proper care of confidential information. There are many firms providing these services, with a wide range in terms of what they assess, how they assess, and cost. “Each organization requires tailored configurations to fit their needs,” said Ramos. “There is a baseline that needs to be followed for security. However, implementing a multi-million dollar enterprise solution on a small five-person network might not always be the best solution. A certified professional would be able to evaluate the needs of the client and customer, and then recommend a solution that fits the needs of the client and the business.” Many certified professionals follow standards from third-party international or national standards such as the **International Standards Organization** (which offers ISO 27001 certification[®]) and the **National Institute of Standards and Technology** (which offers the NIST

Framework for Improving Critical Infrastructure Cybersecurity[®]). Other possibilities include seeking assessments and certification from consultants or major accounting firms, which, Thibodeaux said, will test your firm’s controls against its own goals, rather than against an independent standard. There are also vendors, such as **Verizon**[®] and ACA Aponix, which provide security assessments and certification. “Check these vendors out before signing,” he suggested, and if you do choose to work with one, make sure that it has some name recognition, otherwise the certification will not carry much clout.

“Let clients know the steps you take: ‘We encrypt data, only people who absolutely need to see confidential information are able to do so, we hire white-hat hackers who test our systems, we provide you with identity-theft protection.’”

- **Penetration testing.** Let clients and potential clients know your advisory firm does this at least on an annual basis – and make a point of distinguishing it from vulnerability scans, which pale by comparison, Ramos said. Here’s the difference: A vulnerability scan merely finds locations where your network is open to exploitation, while a penetration test, after finding such locations, goes into them to see what kind of mischief can be done. If your firm had penetration testing performed, he said, “let clients know that ‘We had someone try to exploit our vulnerabilities.’ Many organizations do not understand the difference.”
- **Encryption and passwords.** “Encryption, encryption, I cannot say it enough,” said Ramos. It’s critical to protecting your data, which also means that it’s critical to let your clients know that your firm uses it. Password protection on documents like **Microsoft Word** and **Adobe Acrobat** files, which many non-technical people think of as something separate from encryption, really is the same thing,

as the encryption process occurs on the backend, unbeknownst to the user, he said. When an individual correctly enters his or her password, they are not only unlocking entry to a file, they are allowing it to be read decrypted. Whether your clients understand this or not, let them know that your firm always uses both – and that they are used not only for data “at rest,” that is, data that resides on your officer server, but for data “in transit,” as in emails both leaving and entering your network. Also let clients know that laptops, which fall between in transit encryption (in that they are mobile) and at rest encryption (because the data they contain is on your network) are also full-disk encrypted, Ramos said.

- **Internal private security standard.** This one may seem obvious, but sometimes obvious solutions are overlooked. “Establish a robust private security standard at your firm, stating clearly what you do to protect confidential data,” said Thibodeaux. Make sure that what you state is actually being done, he added, otherwise your state attorney general or the Federal Trade Commission may take notice.
- **Insurance.** “This is a tricky question. Some believe it is needed, some believe it is not,” said Ramos. He tends to fall among those who believe it is more useful than not, but said he sees cybersecurity insurance “as an addition, not a selling point.” It won’t cover all costs and may not even cover the harm done to the reputation of a firm that gets hacked, but it may cover the costs of the business disruption itself and allow the adviser to resume operations after the hacking. But perhaps the main benefit, he said, may be the psychological comfort it brings the client. Thibodeaux noted that the cybersecurity insurance market has “matured” over the years, with several insurance companies offering it, but the insurance itself has yet to become standardized. Those interested should be able to see what’s available from the regular business insurance broker. A number of insurers provide clients with free identity theft protection for a limited period of time, such as two years, he said.
- **Security training.** Let clients and potential clients know that employees are training in a wide breadth of

cybersecurity best practices. These practices might include anything from awareness of rogue emails (phishing) to the directive of a “clean desk policy” under which downloaded confidential information may not be left on desktops, Ramos said. He also suggested that advisers let clients know that their firms have physical security training, as well, including that “we lock our doors at night.” ☞

SEC Catches a Big Fish

continued from page 1

the Class A shares covered marketing and distribution (sales) expenses, known as 12b-1 fees, something that the agency said was not adequately disclosed to clients. Credit Suisse collected approximately \$3.2 million in these “avoidable 12b-1 fees,” which were paid out of the assets of the mutual fund, according to the SEC.

“Thus, 12b-1 fees decreased the value of advisory clients’ investments in mutual funds and increased the compensation paid to Credit Suisse and its [investment advisory representatives,]” the agency said.

Two separate settlements were reached. In one¹, New York City-based Credit Suisse, a dually registered adviser/broker-dealer, agreed to pay disgorgement of \$2.1 million, prejudgment interest of more than \$380,000, and a civil money penalty of \$3.3 million.

In the other², Katz, who the SEC said generated the majority of avoidable 12b-1 fees from clients, agreed to pay disgorgement of \$1.1 million, prejudgment interest of almost \$197,600, and a civil money penalty of \$850,000. Both parties were censured.

These financial penalties stand in contrast to what the agency meted out to **Alison, LLC** and its owner, **Stephen Alison**, in a March 29 settlement in which they paid no disgorgement or fines (*ACA Insight*, 4/10/17³). That firm, however, was in financial distress, according to the SEC’s administrative order instituting the settlement, and had already ceased operation, so collection of any money would have been difficult. It’s also possible that the low financial penalties are the result of settlement negotiations with the agency.

The crackdown

In any event, the multiple settlements in less than a month demonstrate that the SEC, as it stated in a July 2016 “share class initiative” risk alert from its Office of Compliance Inspections and Examinations, remains quite serious about addressing “the risk that registered advisers may be making certain conflicted investment recommendations to their clients.” Examiners will be on the lookout for conflicts of interest tied to advisers’ compensation or financial incentives in recommending, among other things, mutual fund share classes that have “substantial loads or distribution fees,” the risk alert says.

“The SEC has been quite vocal on this topic,” said **Shartsis Friese** partner **Jahan Raissi**. “Advisers need to remember that they are fiduciaries and best execution must always be pursued.”

Why are 12b-1 fees so important? Mutual funds that pay for distribution services must do so in accordance with Investment Company Act Rule 12b-1, meaning through a 12b-1 plan. They may then pass on these distribution costs to investors – as long as they disclose that they are doing so. It’s not the use of 12b-1 fees that gets advisers in trouble, it’s not letting clients know they are being charged for them.

As the Credit Suisse settlement demonstrates, placing clients in more expensive share classes that include 12b-1 fees without letting the clients know that less expensive share classes are available, constitutes, from the SEC’s point of view, not only a conflict of interest, but a failure to meet 12b-1 disclosure requirements.

The particulars

From January 2009 through most of January 2014, Credit Suisse, through its PB North America subsidiary, offer investment advisory services and programs, including a fee-based wrap program. That program offered investment advice, execution, custody, administrative and account reporting services, according to the SEC’s administrative order. The advisory accounts in the wrap fee program were overseen by Credit Suisse’s Discretionary Managed Portfolio (DMP) program. These accounts could be invested in a wide selec-

tion of mutual funds, including multiple share classes of the same funds.

The Class A shares charged an additional 25 basis points per year as 12b-1 fees. These differed from the institutional share classes, which did not charge 12b-1 fees.

“An investor who holds institutional share classes of a mutual fund will pay lower fees over time – and earn higher investment returns – than an investor who holds Class A shares of the same fund,” the SEC said. “Therefore, if a mutual fund offers an institutional share class, and an investor is eligible to own it, it is almost invariably in the investor’s best interests to select the institutional share class.”

“Given that the client in this case was in a wrap fee program which is supposed to include all ‘trading’ costs (which I would expect the SEC says would include distribution costs like 12b-1 fees),” said **Faegre Baker Daniels** partner **Jeffrey Blumberg**, “any compensation payable to the investment adviser in excess of the wrap fee is a huge red flag.”

“Institutional share classes weren’t all that available until a few years ago, when they began to be offered more with the advent of wrap fee programs,” said Raissi. Advisers should keep this in mind when reviewing their products and fees, as lower-fee investments for certain securities may now be available that were not available before.

The IAR

Katz joined Credit Suisse in October 2008 as an investment adviser representative in its San Francisco branch office, the agency said. Once on board, he was allowed to manage DMP accounts in accordance with his own strategy, which the SEC said utilized investments in mutual funds to a greater degree than other Credit Suisse investment adviser representatives involved with DMP clients.

According to the SEC, Katz made a point of ensuring that his team was receiving 12b-1 fee income. Upon discovering that his team was not receiving the 12b-1 fees from clients with Class A mutual fund holdings, and that the reason for this was because Credit Suisse had previ-

ously instructed its clearing broker to block and return such fees to the mutual funds they came from, Katz took steps to change this. He “questioned Credit Suisse management about the block, asserting that he had received credit for such revenue at his prior employer and that his DMP accounts generated \$300,000 to \$500,000 in annual 12b-1 revenue to Credit Suisse,” the agency said. “Following Katz’s inquiry, Credit Suisse instructed its clearing broker to lift the block, thereby allowing Credit Suisse and its [investment adviser representatives] to receive 12b-1 fees derived from its DMP accounts.”

Katz, according to the SEC, handled another situation in June 2009, when an administrative manager in the San Francisco branch office questioned his proposed purchase of Class A shares for DMP clients “when the mutual fund prospectuses suggested that less expensive institutional share classes may be available.” The administrative manager did not approve the transactions. “Katz escalated the issue to the San Francisco branch manager and to DMP management,” the agency said. DMP management then consulted with Credit Suisse’s legal and compliance departments, and the branch manager approved the Class A purchases. Thereafter, the SEC said, administrative managers approved Katz’s purchase of Class A mutual fund shares in DMP accounts without evaluating whether the account was eligible to purchase an institutional share class.”

From January 2009 through most of January 2014, Katz allegedly purchased or held Class A shares for his DMP clients when:

- the mutual fund prospectus indicated that institutional share classes were available for wrap fee accounts,
- other Credit Suisse investment adviser representatives had purchased institutional share classes for DMP accounts, and/or
- Katz himself had previously purchased the institutional share classes for other DMP clients.

“As a result, Katz received approximately \$1.1 million in 12b-1 fees that he would not have collected had his DMP clients been invested in lower-cost share classes for which they were eligible,” the SEC said. At the same

time, according to the agency, Credit Suisse did not require that the Class A shares be exchanged for the less-expensive institutional share classes, even though they were eligible for conversion on a tax-free basis.

“The SEC has been quite vocal on this topic. Advisers need to remember that they are fiduciaries and best execution must always be pursued.”

Disclosure and best execution


Credit Suisse, as an investment adviser, was required to fully disclose all material conflicts of interest between itself and its clients. While the firm disclosed in its Forms ADV and in its advisory agreements that it “may” receive 12b-1 fees and that this might create a conflict of interest, “the disclosure did not address the selection or recommendation of share classes of mutual funds that paid 12b-1 fees when less expensive share classes were available for purchase,” the agency said.

Further, the advisory firm did not identify the actual conflict of interest, according to the SEC. “Because there was no mention of share class distinctions, Credit Suisse’s disclosures did not inform clients that Credit Suisse would recommend or discretionarily purchase or hold a share class that bears 12b-1 fees when a less costly share class of the same fund was available. . . . Rather than make that required disclosure for [investment adviser representatives] who received 12b-1 fees, Credit Suisse disclosed that the [investment adviser representative] ‘[did] not receive compensation from any other person or entity other than Credit Suisse in connection with the provision of investment advice to clients.’”

Of course, by allegedly steering its clients into more expensive share classes, Credit Suisse also was not meeting best execution requirements. “By purchasing Class A shares when its DMP clients were eligible for institutional share classes, and by failing to disclose to its clients that best execution might not be sought for mutual funds with multiple available share classes,

Credit Suisse breached its duty to seek best execution on behalf of its DMP clients,” the agency charged.

Violations

Both Credit Suisse and Katz were charged with having willfully violated Section 206(2) of the Advisers Act, which prohibits fraud. Credit Suisse alone was charged with having willfully violated Section 207, for making an untrue statement on its registration application, and with having willfully violated Section 206(4) and its Rule 206(4)-7, the Compliance Program Rule, for failing to adopt and implement written compliance policies and procedures that would have prevented these violations. An attorney representing Credit Suisse did not respond to a voice mail or email seeking comment. An attorney representing Katz was reached, but chose not to comment. 

Check on Disclosure

continued from page 1

That said, many, if not most, agency enforcement actions include allegations that an adviser failed to disclose material facts to clients and/or to the agency. Nor are these allegations limited to individual aspects of securities management, like fees or marketing, but appear to cover almost all areas of management that affect clients.

Don’t fall into the trap of checking on disclosure in only one or two problem areas that have drawn SEC attention. That may lead CCOs into the equivalent of a game of whack-a-mole, where only the agency’s enforcement topics of the day get scrutinized for disclosure, while areas not currently drawing SEC attention do not. In addition to paying attention to disclosure in key problem areas, be aware that there are commonalities to disclosure that can and should be checked on across the board.

“I like the idea of a holistic disclosure approach,” said Stadulis. “Failure to do so means you failed to do your homework, you really didn’t think about the practices and/or investments in your shop and, as a result, you may miss an important disclosure area.”

Best across-the-board disclosure practices

Consider the following steps to ensure your firm is firing on all disclosure cylinders:

- **Disclose everything that might reveal a conflict of interest.** “Most SEC enforcement actions against investment advisers involve allegations of violations of Advisers Act Section 206 and involve conflicts of interest,” said **Ropes & Gray** partner **Jason Brown**. Are you disclosing, for instance, your firm’s fees and expenses, the allocation methodology it uses, or that the firm has an affiliated service provider? “Enforcement often occurs because of an issue that was not disclosed at all.” Then, ask yourself if the disclosure was specific enough. “Would a reasonable investor understand from your disclosure the exact nature of the potential conflict of interest?”

“Ask yourself, ‘If I don’t disclose it, am I leaving out something that could affect an investor’s decision?’”

- **Disclose all information that is material.** “Material,” said Stadulis, means “whatever a reasonable investor would find important or relevant in making investment decisions.” There does not have to be a conflict of interest for this to be the case – the information simply has to be about investments. “Ask yourself,” he said, “‘If I don’t disclose it, am I leaving out something that could affect an investor’s decision?’ and, after you disclose that information, ‘Have I left out something in what I told the investor?’” This is a judgment call to a certain degree, so, to get a handle on what the SEC thinks a reasonable investor would find important, stay up to date on agency enforcement actions and settlements, as well as agency staff guidance, and statements made by SEC officials at conferences and in other venues.
- **Be consistent.** It’s important that your disclosures are consistent from one area to another. In other words, what is written in registration materials must match what is written elsewhere. “If you say in your Form ADV that your firm does not engage in leveraging

when making investments, your marketing should not indicate that you have done leveraging,” said Stadulis. “Similarly, if you say in your Form ADV that you require pre-clearance for all access persons for all securities transactions, but your Code of Ethics requires pre-clearance only for private placements and initial public offerings, you have a consistency problem.”

- **Create and maintain disclosure policies and procedures.** Make sure your firm has compliance policies and procedures that address the accuracy of disclosures made to regulators and to clients,” said **Mayer Brown** partner **Amy Ward Pershkov**. “The exam staff expects these policies and procedures to be in place,” she said. “They need to address how you make fair and accurate disclosures that are not misleading.”
- **Inventory your disclosures.** “What are the ways – websites, social media, email communications, any way that the firm is using to disclose – and then assess,” Pershkov said. “Review them to understand what each piece needs to have in terms of disclosure, how you describe your firm, assets under management, and more.” For marketing pieces, she suggested creating a standard template with disclosure language that can be used in all marketing pieces.

Beyond marketing, consider having a standard paragraph that describes the firm. “In the real world,” Pershkov said, “this may not always be that easy. You may want to describe things differently to different clients –but if you do so, be aware that is a red flag for examiners.”

- **Keep your disclosures up to date.** “It does no good to have stale disclosures,” said Stadulis. Practices change to take into account market conditions, clients, regulatory requirements and more. To keep your firm’s disclosures timely, “you may need to update your Form ADV more than annually.”
- **Let go of the belief that disclosures fix everything.** “That is a false belief,” Stadulis said. In addition to disclosure not inoculating a firm from being charged for stealing someone’s money, there are violations that are not disclosure-related, such as not having a proper guardian for custody, or using a testimonial or past specific recommendation in marketing materials. “Business people sometimes tend to think, ‘We can just disclose it away.’ But that is not always the case.”
- **Consider automation.** Vendors that provide software to automatically gather data and disclosure from mul-

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 _____

multiple places can help reduce human error, although advisers should be aware that there may be some expense involved. If you go this route, Pershkov said, be aware that “even monitoring software needs to be periodically checked for necessary updates. You can’t just set it and forget it.”

- **Make sure information and compliance language is correct.** Of course, the information a firm places in its disclosures must be accurate. Doing so means having good communication lines throughout the firm, said Pershkov, “otherwise the wrong disclosures will be made.” If your firm is GIPS compliant, you will need to state the required up-to-date GIPS disclosures in presentations.
- **Tailor disclosures to your business.** “Disclosures cannot be canned,” said Stadulis. If disclosures are boilerplate, not only might these be noticed as inadequate by examiners, “but you are creating a problem for yourself, because it means that you failed to truly consider what your firm does and the investments it

makes and, as a result, you may miss an important disclosure area.”

- **Monitor and enforce disclosures.** One way to do this is to test different portions of your firm’s Form ADV and compliance policies in how they disclose specific types of information, such as fees. “Are they consistent?” Stadulis asked. “Consider creating an ongoing disclosure grid where, for each topic, you list all the places where there needs to be disclosure, and then check what’s really out there against that grid.” Items to include in the grid include Form ADV or Form PF, compliance policies and procedures, limited partnership agreements and private placement memorandums if private funds are involved, description of your firm’s investment strategy, and marketing materials. “Also check Form ADVs from competitors. Take a sample of their registration statements and see what they are disclosing. You may find an evolving disclosure area – see what your competitors are doing and what you may not be doing,” he said. ☒

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.