Schulte Roth&Zabel

Private Funds Regulatory UPDATE

Compliance Roundup

November 2020

Contents

SEC Touts Twin Goals Served by Form CRS and Reg BI, Advises Investment Advisers to Keep Form CRS Simple
During a roundtable hosted by the SEC on Oct. 26, 2020, Chairman Jay Clayton discussed how Form CRS and Regulation Best Interest together seek to enhance the transparency and quality of relationships between investment advisers, broker-dealers and retail investors and shared the staff's observations in the four months since the compliance date for each.
› Read more

CCPA Amendment Extends Exemptions for B2B and HR Data
A recent amendment extends the California Consumer Privacy Act partial exemptions for business-to-business-related and certain human resources information from Jan. 1, 2021, to Jan. 1, 2022. The outcome of a ballot initiative on election day could extend the exemptions one additional year, i.e., until Jan. 1, 2023.
› Read more

Facebook Takes Aim at NYU Web Scrapers
On Oct. 16, 2020, Facebook sent a cease-and-desist letter to researchers behind the NYU Ad Observatory project, who are web scraping Facebook to collect data on how Facebook targets political ads to Facebook users.
› Read more

SRZ Partner Addresses FBI Bulletin on Money Laundering by Private Funds
A leaked FBI intelligence bulletin warns that criminals and foreign adversaries may be using hedge funds and private equity funds to launder money, but reported instances of money laundering through private funds are rare. In an article published by *Morning Consult* and reprinted here, SRZ partner Gary Stein discusses the reasons why the FBI's concerns may be overstated and the efforts by the private fund industry to prevent money laundering.
› Read more

Private Fund Regulators Double Down on Whistleblower Programs
In a series of recent actions, the SEC and the Commodity Futures Trading Commission reaffirmed their commitment to their respective whistleblower programs, including awarding a record-breaking $114-million SEC whistleblower payout.
› Read more

FCA Update on Short Selling Reporting Post-Brexit
On Oct. 28, 2020, the UK Financial Conduct Authority published a new webpage on net short position reporting and preparing for Brexit. This webpage explains the short sale reporting requirements in the UK following the "onshoring" of the EU Short Selling Regulation at the end of the Brexit transition period on Dec. 31, 2020, at 11:00 PM (GMT).
› **Read more**

Fund Manager to Disgorge $1 Million for Charging Management Fees Inconsistent with Fund Documents
On Oct. 22, 2020, the SEC settled fraud charges with a private equity fund adviser in an enforcement case that demonstrates the SEC's continued focus on management fees and expenses.
› **Read more**

Treasury Makes It More Difficult for Ransomware Victims to Pay Ransoms
On Oct. 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control and the U.S. Department of the Treasury's Financial Crimes Enforcement Network each issued advisories on ransomware that, when taken together, make it more difficult for victims to lawfully pay ransoms to regain access to hijacked systems and recover stolen data.
› **Read more**

Executive Order May Aid Targets of Government Investigations
A recent Executive Order and implementing guidance from the Office of Management and Budget directs federal executive departments and agencies to be more lenient, expedient and transparent in investigations and enforcement actions.
› **Read more**

DC Circuit Affirms Disciplinary Action Against Compliance Chief
On Oct. 23, 2020, the United States Court of Appeals for the District of Columbia upheld two disciplinary orders by the SEC, finding there was "substantial evidence" that the former chief compliance officer of a broker-dealer had missed clear "red flags" and had failed to ensure review of electronic correspondence.
› **Read more**

Reg SHO Action Is a Reminder for Fund Managers on Locates for "Hard to Borrow" Securities
A recent Financial Industry Regulatory Authority enforcement action highlights a specific locate issue in the context of Regulation SHO that has implications for certain fund managers.
› **Read more**

CFTC Aims to Reward Cooperation
On Oct. 29, 2020, the CFTC announced new guidance for enforcement staff when recommending the recognition of a respondent's cooperation, self-reporting or remediation in CFTC orders (without changing the existing policy for how cooperation credit is determined).
› **Read more**

SEC Touts Twin Goals Served by Form CRS and Reg BI, Advises Investment Advisers to Keep Form CRS Simple

During a roundtable hosted by the SEC on Oct. 26, 2020, Chairman Jay Clayton discussed how Form CRS and Regulation Best Interest ("Reg BI") together seek to enhance the transparency and quality of relationships between investment advisers, broker-dealers and retail investors and shared the staff's observations in the four months since the compliance date for each.[1]

The Chairman also defended his decision to maintain the June 30 compliance date, saying he believed "the significant benefits of Reg BI and Form CRS would be crucially important to Main Street investors as they sought to address the economic impacts of the COVID-19 pandemic and resulting market volatility."

Form CRS

As a reminder, Form CRS requires SEC-registered investment advisers to provide a brief relationship summary to their clients who are natural persons (defined for this purpose as "retail investors" but not including investors in pooled investment vehicles).[2] The summary must contain plain English disclosures on certain topics (e.g., fees, costs, conflicts of interest and disciplinary history) under standardized headings and in a prescribed order. It is designed to help retail investors make informed choices and improve the dialogue between retail investors and investment advisers.[3]

During the roundtable, the staff gave practical guidance for the disclosures, noting that, on average, the Forms CRS they reviewed were written at an 11th grade reading level and encouraging firms to write their Forms CRS at an eighth grade reading level to maximize readability.[4] The Chairman also observed that some filings failed to include required information regarding disciplinary history and directed managers to several recent FAQs[5] the staff has published on the topic.

Regulation Best Interest

Also, as a reminder, Reg BI establishes an enhanced standard of conduct that requires broker-dealers to act in the best interest of their retail customers and prohibits broker-dealers from placing their own

[1] *See* Statement at the SEC's Staff Roundtable on Regulation Best Interest and Form CRS ("Chairman's Statement"); *see also* our April 10, 2020, *Alert* regarding Form CRS.

[2] *See* our August 2019 Private Funds Regulatory Update regarding Form CRS and Reg BI.

[3] *See* Chairman's Statement.

[4] *See* Roundtable on Regulation Best Interest and Form CRS.

[5] Securities and Exchange Commission, Division of Investment Management: Frequently Asked Questions on Form CRS.

interests ahead of their retail customers' interests.[6] Notably, this heightened standard applies when a broker-dealer recommends either a securities transaction or an investment strategy involving securities, including an account recommendation such as a retirement fund "rollover," and cannot be satisfied through disclosure alone. According to the Chairman, "Reg BI codifies the fundamental principle that investment professionals should not put their interests ahead of the interests of their clients and customers."

‹ Table of Contents Read Next ›

[6] *See* our August 2019 Private Funds Regulatory Update regarding Form CRS and Reg BI.

CCPA Amendment Extends Exemptions for B2B and HR Data

A recent amendment extends the California Consumer Privacy Act ("CCPA") partial exemptions[1] for business-to-business ("B2B")-related and certain human resources ("HR") information from Jan. 1, 2021, to Jan. 1, 2022. The outcome of a ballot initiative on election day could extend the exemptions one additional year, i.e., until Jan. 1, 2023.[2] Either outcome should come as welcome news to fund managers because it preserves the status quo for portions of the CCPA for which implementation would otherwise be difficult.[3]

B2B Contacts

Until Jan. 1, 2022, the CCPA will remain largely inapplicable to information collected in a purely B2B context, such as the name and email address of a California resident acting on behalf of an institutional investor or a vendor.[4] The amendment provides more time for the California legislature to potentially address the burdensome challenges presented by applying the CCPA's requirements — in particular the requirements of making disclosure to consumers at the "point of collection" and responding to individual consumer requests[5] — to a B2B relationship.

HR-Related Information

The CCPA contains a partial exemption from its extensive disclosure requirements for information about employees, job applicants and contractors and permits employers to use more limited privacy disclosures with respect to these groups. Employers may continue to provide abbreviated disclosures until Jan. 1, 2022, after which the CCPA's full requirements will apply to this HR-related information absent further legislative action.

[1] The exemptions do not extend to the CCPA's private right of action for consumers whose sensitive personal information has been subject to unauthorized access or disclosure as a result of the covered business' failure to maintain "reasonable" security procedures.

[2] On Sept. 29, 2020, California Governor Gavin Newsom signed AB-1281 into law. AB-1281 will only take effect if California voters do not approve the California Privacy Rights Act (CPRA) ballot initiative on Nov. 3, 2020. If voters approve the initiative, the CPRA would extend the exemptions for another year, until Jan. 1, 2023.

[3] The CCPA applies to private fund managers that collect certain personal information from natural persons who reside in California. Our Dec. 6, 2019 *Alert* discusses the CCPA's requirements with respect to different types of information, including HR- and B2B-related data.

[4] The exemption is not complete as it applies to B2B data only if the personal information is collected in the context of conducting due diligence or providing or receiving a product or service.

[5] Where no exemption applies, the CCPA requires businesses to respond to requests from individual consumers for information such as the categories of personal information collected and how that information is used, as well requests to delete personal information (subject to regulatory limitations).

The amendment, however, does not lessen the current CCPA requirements. Private fund managers are reminded to continue to provide abbreviated notice requirements to California employees, job applicants and independent contractors as required under the CCPA.

‹ Table of Contents

Read Next ›

Facebook Takes Aim at NYU Web Scrapers

On Oct. 16, 2020, Facebook sent a cease-and-desist letter to researchers behind the NYU Ad Observatory project, who are web scraping Facebook to collect data on how Facebook targets political ads to Facebook users.[1]

Web scraping, a technique used to extract large amounts of data from websites, is popular with sophisticated investors, including investment fund managers, as a source of alternative data, which is purchased from third-party vendors or scraped directly.

In the letter, Facebook contended, "Scraping tools, no matter how well-intentioned, are not a permissible means of collecting information from us" and threatened additional enforcement action if the project continued to scrape and refused to delete the collected data. The university researchers provide volunteers a plug-in that, when added to a browser, copies ads seen on Facebook and shares them with the project.

The action is the latest in Facebook's efforts to more aggressively police web scraping on its sites[2] and comes at a time when the industry is closely watching *hiQ Labs, Inc. v. LinkedIn Corp.* — a web scraping case pending in federal district court in California, with a petition for review of an initial preliminary injunction in favor of hiQ pending in the U.S. Supreme Court.

In 2017, LinkedIn sent a cease-and-desist letter to hiQ claiming hiQ's scraping of LinkedIn's public profiles violated LinkedIn's user agreement and state and federal law, including the Computer Fraud and Abuse Act ("CFAA"). LinkedIn threatened to implement technical measures to prevent further scraping.

In response, hiQ went on offense and sued LinkedIn in federal court for injunctive relief and a declaratory judgment that hiQ's activities were legally permissible. In August 2017, the district court granted hiQ a preliminary injunction, ordering LinkedIn to withdraw its cease-and-desist letter and remove any technical barriers to hiQ's access to public profiles. In September 2019, the Ninth Circuit affirmed on appeal.[3] LinkedIn sought Supreme Court review, and its petition for certiorari is currently pending.[4]

---

[1] Wall Street Journal

[2] In June, Facebook filed actions in federal court in California, *Facebook, Inc. v. Zaghar*, 3:2020-cv-04054 (N.D. Cal.), and in Spain against two different web scrapers. *See* ZDNet

[3] https://cdn.ca9.uscourts.gov/datastore/opinions/2019/09/09/17-16783.pdf

[4] If the Supreme Court agrees to hear the case, it will consider the narrow issue of whether accessing public websites can be deemed to be "without authorization" under the CFAA. The Supreme Court already has agreed to hear a different CFAA criminal case this term, *Van Buren v. United States*. Although the case itself does not involve web scraping, it has potential implications

While it remains to be seen if the Supreme Court will hear the appeal of the preliminary injunction, the rest of the case is proceeding in the district court.

The case has significant implications for fund managers who purchase web scraped data or engage directly in web scraping regarding the legality of such practices and the potential limits of what companies can do to prevent web scraping on their public websites.

‹ Table of Contents

Read Next ›

for web scrapers. Indeed, the Reporters Committee for Freedom of the Press filed an amicus brief for the appellant arguing that too broad an interpretation of the CFAA in the *Van Buren* case could threaten to criminalize web scraping.

SRZ Partner Addresses FBI Bulletin on Money Laundering by Private Funds

A leaked FBI intelligence bulletin warns that criminals and foreign adversaries may be using hedge funds and private equity funds to launder money, but reported instances of money laundering through private funds are rare. In an article published by Morning Consult and reprinted below, SRZ partner Gary Stein discusses the reasons why the FBI's concerns may be overstated and the efforts by the private fund industry to prevent money laundering.

Leaked FBI Bulletin on Private Funds Misses the Mark

By Gary Stein

October 23, 2020

Criminals, drug cartels and corrupt foreign officials are notoriously creative when it comes to laundering their ill-gotten gains. Financial service firms must stand vigilant against this kind of illicit activity. As a lawyer who counsels hedge funds and private equity funds on their anti-money laundering programs, I have found that the private fund industry takes this responsibility seriously.

Unfortunately, a recently leaked Federal Bureau of Investigation intelligence bulletin displays a profound misunderstanding of the limited money laundering risks posed by private investment funds. The bulletin warns that criminals and foreign adversaries "likely" are using hedge funds and private equity funds to launder money. But reported instances of money laundering through private funds are quite rare. The Federal Bureau of Investigation ("FBI") bulletin itself identifies only one individual convicted for such activity — and he was a corrupt lawyer who launched fraudulent funds to launder dirty money from his clients.

Professionally run private funds are not attractive vehicles for money laundering. Liquidity is limited, including lengthy "lock-up" periods that can prevent investors from withdrawing their capital for years. Investors cannot transact with third parties, and distributions and redemptions must be paid to the investor's own account. Given these structural characteristics, it is not surprising that the majority of fund assets come from long-term institutional investors such as public pension plans, private pension plans, endowments and foundations.

The FBI bulletin nonetheless claims that private funds are especially vulnerable to money laundering for three primary reasons. Each is based on a flawed understanding of how private funds work, how they are regulated and the industry's longstanding commitment to AML compliance.

First, the FBI's bulletin claims private funds enable investors to "circumvent" traditional AML regulations. This is simply not the case. As a rule, private funds do not accept cash deposits from investors — the investor's funds must come from an existing account at a bank or other financial institution subject to AML regulations. Before opening that account, the investor will have had to satisfy the financial institution's AML program, including identification and verification of its beneficial owners. Then, the investor will be subject to the private fund's own AML screening. It therefore would be illogical for criminals looking to avoid AML scrutiny to opt to place their money with a private fund.

Second, the FBI bulletin asserts that private funds are "largely exempt" from regulatory oversight. This, too, is incorrect. Since 2012, under the Dodd-Frank Act, the vast majority of U.S. private fund managers have been registered with the Securities and Exchange Commission or a state securities regulator. The U.S. Securities and Exchange Commission ("SEC") and state regulators actively regulate private fund managers, even conducting on-site examinations. According to the SEC, there are at least 13,475 registered investment advisors, with assets under management of $84 trillion.

Third, the FBI bulletin incorrectly assumes that AML programs are not adequately designed to monitor and detect money laundering through private funds. In fact, private fund managers typically maintain robust AML programs that are modeled after those of other financial institutions. They do so because they are subject to federal criminal money-laundering statutes and because their counterparties — including brokers, lenders and co-investors — require fund managers to demonstrate that they have implemented effective AML programs. The SEC has for years allowed brokers to rely on fund managers' AML programs.

These AML programs typically include, among other things, written AML policies and procedures; "know your investor" requirements; screening for negative public information about the investor; enhanced due diligence for higher-risk investors; stringent restrictions on transfers to third parties and AML training of relevant fund employees. The programs are implemented by internal compliance personnel and, often, by third-party administrators staffed by AML professionals.

It's true that private funds are not required by current law to have AML programs. That is not because of opposition from the industry. In 2015, FinCEN, the arm of the U.S. Treasury Department chiefly responsible for combating money laundering, proposed an AML program rule for fund advisors. Industry groups like the Managed Funds Association actively supported FinCEN's proposal, which was consistent with what fund managers are already doing in practice. Five years later, the proposed rule still has not been finalized. This strongly suggests that FinCEN does not share the FBI's assessment that private funds are a substantial source of money laundering risk.

The FBI's efforts to identify weaknesses in the U.S. financial system that facilitate money laundering are commendable. However, any such assessment should be based on a proper understanding of how the private fund industry actively works to prevent money laundering.

‹ Table of Contents **Read Next ›**

Private Fund Regulators Double Down on Whistleblower Programs

In a series of recent actions, the SEC and the Commodity Futures Trading Commission reaffirmed their commitment to their respective whistleblower programs, including awarding a record-breaking $114-million SEC whistleblower payout.

On Sept. 23, 2020, the SEC announced changes to its decade-old whistleblower program[1] intended to streamline the determination of reward amounts and speed payments to tipsters. The whistleblower program has become an important part of the SEC's enforcement effort and, while the new rules include provisions that seek to make it easier to weed out meritless claims,[2] the overall goal is to "get more money to whistleblowers faster."

Whistleblowers are typically awarded a percentage of the amount recovered by the SEC and, in the 2020 fiscal year alone, the SEC paid over $175 million in whistleblower awards.[3] However, the actual percentage of a recovery (which is capped at 30% by statute) is determined by weighing a number of factors, such as whether the specific violation is an SEC priority. The Commission controversially proposed specifically considering the size of the award as a factor in setting the award, including the ability to make downward departures for "exceedingly large" awards.[4] While this provision was not adopted, the adopting release indicates that the Commission already has the authority to consider the size of the award as part of its broader authority. The uncertainty that results from the Commission's discretion in setting awards can dis-incentivize reporting smaller violations.

The revised rules, however, set out criteria that create a presumption that a whistleblower is entitled to the maximum 30% award if it would be less than $5 million.[5] The revisions also ease the number of procedural requirements for whistleblowers to qualify for awards and clarify that while the SEC has discretion over both the percent and dollar amount of awards, particularly for the largest awards, this discretion does not suggest any cap on large awards other than the statutory maximum of 30%.

Soon after announcing the revised program, the SEC put it into action. First, on Oct. 15, 2020, the SEC awarded $800,000 to a whistleblower — overruling the SEC staff's recommendation to deny the

[1] 17 CFR Parts 240 and 249; Release No. 34-83557; File No. S7-16-18

[2] Public Statement of Jay Clayton, Strengthening our Whistleblower Program, Sept. 23, 2020, available at https://www.sec.gov/news/public-statement/clayton-whistleblower-2020-09-23.

[3] SEC Whistleblower Program Ends Record-Setting Fiscal Year With Four Additional Awards.

[4] SEC Proposed Whistleblower Rule Change at 10-11.

[5] These criteria are the absence of any "negative award factors." These include (1) culpability; (2) unreasonable reporting delay; and (3) interference with internal compliance and reporting systems. 17 C.F.R. § 240.21F-6(b).

claim. This award exemplifies the increased flexibility of the new rules; the SEC seemingly considered information provided prior to the submission of a formal whistleblower complaint and approved the award.

Then, on Oct. 22, 2020, the SEC awarded $114 million to a whistleblower — the highest award in the program's history. That single award — issued only three weeks into the SEC's new fiscal year — represented 65% of the total of all whistleblower awards in fiscal year 2020, which itself was a record-setting year. The SEC whistleblower program has come a long way since its first award of $50,000 in 2012.

Though more modest by comparison, the CFTC has also increasingly rewarded whistleblowers, including a $9-million award in July and a $6-million award in June.[6] The CFTC's program, which started under Dodd-Frank and was designed to harmonize with the SEC's program, provides for awards between 10% and 30% where the information leads to fines over $1 million.

The net result is that the two primary U.S. regulators of private fund managers are actively seeking, and incentivizing, whistleblowers. Further, the increasingly broad awareness of these programs in the industry may make it more likely that employees will "report out" internal problems, instead of pursuing internal solutions.

These developments highlight the importance of investing in regulatory compliance and internal audit resources and personnel, conducting rigorous assessments and self-examinations and creating (or reinforcing) a culture that values integrity and rewards internal reporting of issues and potential wrongdoing. Indeed, in a recent panel discussion about the success of the whistleblower program, a former SEC deputy director encouraged firms to "hug your whistleblower" and "treat them with respect and care and thoughtfulness."[7]

‹ Table of Contents Read Next ›

[6] *See* Press Release, CFTC Awards Approximately $9 Million to Whistleblower, July 27, 2020; Press Release, CFTC Announces $6 Million Whistleblower Award, June 9, 2020.

[7] Law360

FCA Update on Short Selling Reporting Post-Brexit

On Oct. 28, 2020, the UK Financial Conduct Authority published a new webpage on net-short position reporting and preparing for Brexit. This webpage explains the short-sale reporting requirements in the United Kingdom following the "onshoring" of the EU Short Selling Regulation at the end of the Brexit transition period on Dec. 31, 2020, at 11:00 PM (GMT).

Following the transition period, the FCA expects position holders to report their net short positions in shares at the 0.2% (rather than the ESMA temporary 0.1%) threshold and to consult the FCA's UK list of exempted shares and the FCA Financial Instrument Reference Data System to determine whether a notification is required. The UK list will be published on the FCA's website starting Jan. 1, 2021. The disclosure thresholds with respect to UK sovereign debt and uncovered positions in UK sovereign credit default swaps remain unchanged.

Managers should be mindful of their short sale reporting obligations, particularly in light of the recent fine of GBP 873,118 levied by the FCA against Asia Research and Capital Management Ltd, a Hong Kong manager, for failure to disclose a net short position in a UK listed company. This fine marks the first action taken by the FCA to enforce a breach of the short selling regulation.

‹ Table of Contents **Read Next ›**

Fund Manager to Disgorge $1 Million for Charging Management Fees Inconsistent with Fund Documents

On Oct. 22, 2020, the SEC settled fraud charges with a private equity fund adviser in an enforcement case that demonstrates the SEC's continued focus on management fees and expenses.[1]

The relevant limited partnership agreement ("LPA") provided for a 1.5% management fee on all invested capital but required that amount to be reduced in the event of a write down of portfolio securities. According to the SEC, five different securities were subject to write-downs during a three-year period. The adviser, however, did not reduce its management fees at any time. The SEC found the adviser's failure to take into account the write-downs of the portfolio securities in accordance with the LPA caused the fund and its limited partners to overpay $901,760.91.

The SEC charged the adviser with violations of Section 206(4) and Rule 206(4)-8, which make it unlawful to "engage in any act, practice, or course of business that is fraudulent, deceptive or manipulative with respect to any investor or prospective investor in the pooled investments vehicle." Although fraud typically requires a finding of intent, negligence is sufficient to establish a violation of these provisions. The adviser was required to pay approximately one million dollars in disgorgement and prejudgment interest.

This case is a good reminder of the need for fund managers to review their governing documents, Form ADV Part 2A and due diligence questionnaire responses to ensure they are actually doing what their disclosures say.

‹ Table of Contents Read Next ›

[1] *In re EDG Management Co., LLC*, SEC Admin. Proceeding No. 3-20133 (Oct. 22, 2020).

Treasury Makes It More Difficult for Ransomware Victims to Pay Ransoms

On Oct. 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") and the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") each issued advisories on ransomware that, when taken together, make it more difficult for victims to lawfully pay ransoms to regain access to hijacked systems and recover stolen data.

The frequency of ransomware attacks has surged, as has the amounts cybercriminals demand. In the last quarter of 2019, the average ransom payment more than doubled from $84,116 to $190,946, with several organizations reporting seven-figure payments.[1] Navigating a ransomware attack has also become increasingly challenging as perpetrators develop more sophisticated means to infiltrate systems.

The OFAC advisory warns OFAC will impose sanctions on U.S. persons who engage in transactions (including making payments or facilitating payments) with individuals and entities involved in ransomware if they have appeared on OFAC's Specifically Designated Nationals and Blocked Persons List (an "SDN") or if they are covered by country or region embargoes. OFAC cautions that a U.S. person need not know that the recipient of payment has been designated because civil penalties may be imposed for sanctions violations based on strict liability (i.e., without knowledge the transaction was prohibited). This poses a significant risk when paying a ransom, as cybercriminals often disguise their identities when demanding payment, and ask for payment by digital currency, making it nearly impossible to determine whether a recipient has in fact been designated by OFAC.

The FinCEN advisory discusses predominant trends, typologies and potential red flag indicators of ransomware and associated money laundering activities and the related suspicious activity reporting requirements applicable to financial institutions. Specifically, FinCEN reminds financial institutions they may be required to file a SAR when dealing with an incident of ransomware.

The new advisories raise the familiar debate over "negotiating with terrorists." On one hand, paying ransoms makes ransomware attacks more lucrative for cyber criminals and encourages future attacks. On Oct. 13, member nations of the G-7 warned that perpetrators of ransomware attacks might be state-sponsored or linked actors who might use the ransom funds for further illicit purposes, such as funding weapons of mass destruction.[2] On the other hand, regulations that cause delays or impose

[1] The New York Times

[2] LAW360

prohibitions on paying ransoms inhibit what can be an economically efficient way for victims to respond to attacks and minimize the damage to their business continuity.[3]

For private equity sponsors and other fund managers that establish control positions, OFAC's new restrictions could have significant consequences for portfolio companies in certain subsectors, such as hospitals, that have been particularly hard hit by ransomware and have relied on ransom payments to avert attacks with devastating (and potentially deadly) consequences. In addition to potential sanctions from OFAC, G-7 officials have warned of additional coordinated sanctions applying across member nations.

The restrictions and other risks involved with ransom payments reinforce the importance of fund managers having plans in place to prevent and respond to ransomware attacks.[4] Fund managers should be familiar with the OFAC and FinCEN advisories and review them carefully if they become victims of ransomware. In the heat of the moment during a ransomware attack, it will be critical for the manager to determine if the ransom payment that is being demanded would violate applicable U.S. or non-U.S. law.

‹ Table of Contents Read Next ›

[3] The Department of Justice ("DOJ") has also signaled an increased focus on the payment of ransoms and other interactions with cyber criminals. On Aug. 20, 2020, the former Chief Security Officer of Uber was indicted in federal court in California for obstruction of justice and misprision of felony in connection with the attempted cover-up of a 2016 hack, which included a ransom payment. The executive allegedly lied to the Federal Trade Commission, which was investigating a 2014 hack at the time the 2016 ransom was paid, and took efforts to conceal the ransom payment. The DOJ said the case should send a broader message about not concealing cybercrime: "While this case is an extreme example of a prolonged attempt to subvert law enforcement, we hope companies stand up and take notice. Do not help criminal hackers cover their tracks. Do not make the problem worse for your customers, and do not cover up criminal attempts to steal people's personal data."

[4] Our Aug. 17, 2020 *Alert* provides further information on the increasing risk of ransomware attacks, including steps that fund managers and financial institutions can take to increase preparedness for a cyber-attack.

Executive Order May Aid Targets of Government Investigations

A recent Executive Order[1] ("Executive Order") and implementing guidance from the Office of Management and Budget ("OMB")[2] directs federal executive departments and agencies to be more lenient, expedient and transparent in investigations and enforcement actions.[3] The Executive Order addresses several longstanding concerns about procedural and substantive fairness for entities facing investigations and enforcement actions. Regulated entities should evaluate their compliance programs to ensure that they are well-positioned to take advantage of promised leniency for good faith compliance efforts.

To promote economic recovery, the Executive Order directs a number of changes that potentially could impact enforcement activity by the SEC and other regulatory agencies. Most significantly, executive departments and agencies are directed to find places to be lenient, such as declining to bring enforcement actions where there has been a good faith attempt to comply with the law. This marks a significant change from the "broken windows" approach the SEC had implemented previously.

The Executive Order states that liability should only be imposed for violations "of statutes or duly issued regulations, after notice and an opportunity to respond." According to the implementing guidance, this means telling investigation targets what statutes and regulations are asserted to have been violated, along with an explanation of how the conduct at issue runs afoul of that statute or regulation. This approach would mark a sea change for those familiar with handling SEC inquiries. Traditionally, SEC staff decline to provide any information during most investigations, other than to say they are conducting a fact-finding inquiry. Transparency during investigations would enable targets to more efficiently contextualize facts shared with the SEC and prepare potential defenses. Also, in stark contrast to current SEC practice, agencies were directed to turn over evidence favorable to the target — akin to the standard practice in criminal investigations.

[1] Exec. Order No. 13924, 85 C.F.R. 31353 (2020).

[2] U.S. Office of Management and Budget, M-20-31, Memorandum for the Deputy Secretaries of Executive Departments and Agencies (Aug. 31, 2020).

[3] The text of the Executive Order and implementing guidance appear to include the SEC, which is not an executive department, because of the conjunctive reference to executive departments and agencies. The OMB guidance is directed to the "heads of all agencies," and not limited to those agencies that are a part of the executive branch. That said, the SEC, which is an independent agency and not part of the executive branch, may take the position that the order only applies to agencies that are part of the executive branch and thus within the power of the executive branch to set policy.

The OMB implementing guidance also instructs agencies to reward cooperation and self-reporting with reduced or waived civil fines and to allow firms grace periods to cure minor violations. This focus on cooperation and self-reporting mirrors recent actions and statements by the SEC and the CFTC, including large scale amnesty initiatives and formal guidance regarding cooperation credit.[4]

The Executive Order and OMB guidance additionally directed agencies to expedite investigations. The OMB took particular aim at the routine use of tolling agreements, seeking to limit the duration of investigations and to set deadlines for bringing charging decisions.[5]

Regarding transparency, the Executive Order directs agencies to notify targets of investigations when the investigation is concluded, including providing affirmative statements that no violation has been found. This is a significant and welcome change for regulated entities, which traditionally were left in limbo for extended periods of time not knowing whether an investigation had been concluded. Moreover, in the rare instances the SEC provided notification that an investigation had ended, it frequently noted that the closing of the investigation did not mean that no violation of law had occurred.

It remains to be seen to what extent the Executive Order will impact SEC and other regulatory investigations, particularly if the SEC takes the position that it is not subject to the Executive Order. At a minimum, this guidance should empower subpoena recipients or investigation targets to seek these additional substantive and procedural protections. Additionally, regulated entities would be well served to evaluate their compliance policies and supervisory efforts to maximize their ability to seek lenience for good faith compliance efforts. Regulated entities should also consider the Executive Order as another factor in evaluating whether to self-report potential violations of law.

‹ Table of Contents Read Next ›

[4] The CFTC recently formalized its self-reporting and cooperation program to more closely mirror that of the Department of Justice. *See,* e.g. Enforcement Advisory: Cooperation Factors in Enforcement Division Sanction Recommendations for Companies https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisorycompanies011917.pdf.

[5] In its 2020 fiscal year report, released on Nov. 2, 2020, the SEC Division of Enforcement highlighted its continued "focus on shortening the amount of time it takes to complete investigations and recommend enforcement actions," noting it had reduced the average time it takes to complete financial fraud and issuer disclosure investigations from 37 months to 34 months.

DC Circuit Affirms Disciplinary Action Against Compliance Chief

On Oct. 23, 2020, the United States Court of Appeals for the District of Columbia upheld two disciplinary orders by the SEC, finding there was "substantial evidence" that the former chief compliance officer of a broker-dealer had missed clear "red flags" and had failed to ensure review of electronic correspondence.[1]

Although this case involved a disciplinary action pursuant to the Securities Exchange Act of 1934, the same standard of review applies to federal judicial review of SEC disciplinary actions under the Investment Advisers Act of 1940.[2]

The former CCO initially was found to have violated Financial Industry Regulatory Authority ("FINRA") rules related to disclosure and monitoring, including failure to report a relationship with a statutorily disqualified individual, to develop written supervisory procedures ("WSPs") for review of electronic correspondence, to conduct review of electronic correspondence consistent with the firm's existing policies and to enforce WSPs. At his disciplinary hearing, the former CCO had defended his actions, in part, saying "all email review is boring."[3]

Before review by the federal courts, the SEC had upheld FINRA's disciplinary action in separate decisions in 2018 and 2019. In the 2018 decision, the SEC offered insights into how it thinks about CCO liability, saying it is guided by "the principle that, in general, good faith judgments of CCOs made after reasonable inquiry and analysis should not be second guessed. In addition, indicia of good faith or lack of good faith are important factors in assessing reasonableness, fairness and equity in the application of CCO liability."[4]

In both decisions, the SEC questioned whether FINRA should have also charged the firm (which was no longer registered): "A firm [ ] can act only through its agents, and is accountable for the actions of its responsible officers. We think it important to make it clear to firms — by holding them responsible

[1] *North v. SEC,* No. 18-1341 (D.C. Cir. Oct. 23, 2020).

[2] A court must uphold the Commission's decision unless it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A); *see Kornman v. SEC*, 592 F.3d 173, 184 (D.C. Cir. 2010). The Commission's findings of fact are conclusive when supported by substantial evidence. 15 U.S.C. § 80b–13(a).

[3] *In re Thaddeus J. North*, Admin. Proc. File No. 3-17909, Oct. 29, 2018 ("2018 Decision"), at 3.

[4] *Id.* at 12

when there are compliance failures — that it is in their interest to have effective, diligent compliance officers to help them remain in compliance with their obligations."[5]

The SEC also suggested an action against the CEO might have been warranted: "It is not sufficient for the person with overarching supervisory responsibilities to delegate supervisory responsibility to a subordinate, even a capable one, and then simply wash his hands of the matter until a problem is brought to his attention. . . . Implicit is the additional duty to follow-up and review that delegated authority to ensure that it is being properly exercised."[6]

The case outlines the principles guiding the SEC on decisions regarding CCO liability and reinforces the SEC's view that compliance failures are not solely the responsibility of the compliance department. In the appropriate case, the firm and/or principals may be held responsible for the CCO's actions and inactions.

‹ Table of Contents

Read Next ›

[5] *Id.* at 13 (internal quotations omitted); *In re Thaddeus North*, Admin. Proc. File No. 3-18150, Nov. 27, 2019 ("2019 Decision"), at 8 (internal quotations omitted).

[6] 2018 Decision at 13; 2019 Decision at 8.

Reg SHO Action Is a Reminder for Fund Managers on Locates for "Hard to Borrow" Securities

A recent Financial Industry Regulatory Authority enforcement action highlights a specific locate issue in the context of Regulation SHO ("Reg SHO") that has implications for certain fund managers.[1]

By way of background, the SEC adopted Reg SHO in 2004 to address concerns regarding failures to deliver securities sold short and abusive naked short selling (i.e., sales in which the seller does not borrow or arrange to borrow the securities in time to make delivery). While Reg SHO's order marking and locate rules only directly apply to broker-dealers, several provisions of Reg SHO impact fund managers due to industry practice and because broker-dealers rely on their customers' (e.g., investment funds') representations concerning long/short order marking and whether a short sale is supported by a third-party locate.

Fund managers frequently ask whether they may reapply a locate after effecting an intra-day buy-to-cover trade (that is, can they "recycle" a locate after repurchasing shares previously sold short earlier in the day). According to Q&A 4.4 of the SEC's Division of Trading and Market's frequently asked questions concerning Reg. SHO ("Q&A 4.4"), Reg SHO generally permits the re-application of locates following intra-day buy-to-cover trades as long as the subsequent sale is for an amount no greater than the original locate and the original locate is good for the entire trading day.[2] However, for "hard to borrow" and threshold securities, Q&A 4.4 states that locates may not be reapplied and the seller must obtain a new locate prior to the subsequent short sale.

The disparate treatment that Q&A 4.4 requires for "hard to borrow" and threshold securities has been controversial because Reg SHO's locate provision does not distinguish between these types of securities.[3] Further, Q&A 4.4 seems to ignore the mechanics and practicalities of the locate and settlement process.

Until recently, the SEC and self-regulatory organizations have not taken action with respect to violations of Reg SHO Rule 203(b)(1) by virtue of failing to adhere to the Q&A 4.4 guidance. However, in July 2020, FINRA charged a broker-dealer with violating Reg SHO's locate requirement by failing to distinguish between threshold and non-threshold securities when re-applying locates following intra-day buy-to-cover trades. The broker-dealer agreed to a $225,000 fine and a censure. Notably, FINRA's

[1] *See* FINRA Letter of Acceptance, Waiver, and Consent, No. 2016050929001.

[2] *See* https://www.sec.gov/divisions/marketreg/mrfaqregsho1204.htm.

[3] The SEC staff acknowledges that its "frequently asked questions" do not have the force of law, cannot establish new laws, rules or standards and merely reflect the staff's interpretations of existing rules that have neither been approved nor disapproved by the Commission.

investigation included other Reg SHO and FINRA violations that were part of the resolution, which may have influenced the firm's decision to settle.

Because broker-dealers often rely on fund managers to represent that a short sale is supported by a third-party locate, fund managers should ensure that their representations concerning long/short order marking and third-party locates are accurate. Mistakes regarding a seller's ability or intent to deliver securities can put a fund manager's relationship with its broker-dealers at risk and invite regulatory scrutiny.

‹ Table of Contents

Read Next ›

CFTC Aims to Reward Cooperation

On Oct. 29, 2020, the CFTC announced new guidance for enforcement staff when recommending the recognition of a respondent's cooperation, self-reporting or remediation in CFTC orders (without changing the existing policy for how cooperation credit is determined). Chairman Tarbert commented that the CFTC aims to foster a "culture of compliance" and seemingly hopes to incentivize cooperation by recognizing that a respondent cooperated or self-reported, which can lead to a reduced penalty. Further, the CFTC may also recognize a respondent's *failure* to cooperate and self-report.

Under the new guidance, any of the following scenarios may be noted by CFTC staff: (i) no self-reporting, cooperation or remediation; (ii) no self-reporting, but cognizable cooperation and/or remediation that warrant recognition but not a recommended reduction in penalty; (iii) no self-reporting, but substantial cooperation and/or recognition resulting in a reduced penalty; and (v) self-reporting, substantial cooperation and remediation resulting in a substantially reduced penalty.

‹ **Table of Contents** **Contacts** ›

Schulte Roth&Zabel

Private Funds Regulatory UPDATE

Contacts:

Brian T. Daly
Partner
+1 212.756.2758
brian.daly@srz.com

Marc E. Elovitz
Partner
+1 212.756.2553
marc.elovitz@srz.com

Anna Maleva-Otto
Partner
+44 (0) 20 7081 8037
anna.maleva-otto@srz.com

Edward H. Sadtler
Partner
+1 212.756.2290
edward.sadtler@srz.com

Gary Stein
Partner
+1 212.756.2441
gary.stein@srz.com

Craig S. Warkol
Partner
+1 212.756.2496
craig.warkol@srz.com

Kelly Koscuiszka
Special Counsel
+1 212.756.2465
kelly.koscuiszka@srz.com

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com