Schulte Roth & Zabel

Private Funds Regulatory UPDATE

Compliance Roundup

October 2020

Contents

SEC Accredited Investor Definition Updated
On Aug. 26, 2020, the Securities and Exchange Commission broadened the definitions of "accredited investor" in Regulation D under the Securities Act of 1933.
› **Read more**

Fund Administrators Sanctioned by SEC
On Sept. 18, 2020, the SEC sanctioned two related administrators for contributing and causing violations of sections 206(2) and 206(4) of the Investment Advisers Act and Rule 206(4)-8 thereunder by L-R Managers LLC.
› **Read more**

SEC Staff Provides Guidance Regarding Disciplinary History Disclosure Standard in Form CRS
On Oct. 8, 2020, the staff of the SEC's Division of Investment Management and of the Division of Trading and Markets released additional FAQs relating to Form CRS focused on disciplinary history disclosures required of Form CRS filers (e.g., registered investment advisers with natural person clients) and their personnel.
› **Read more**

SEC Chairman Highlights Robust Rulemaking, Enforcement and Examination Statistics
At the "SEC Speaks" forum on Oct. 8, 2020, SEC Chairman Jay Clayton provided an overview of the SEC's 2020 fiscal year goals and accomplishments, including its rule enforcement activities and highlighted the SEC's rulemaking, examination and enforcement statistics, which show that the SEC has remained highly active in its oversight of market participants even in the midst of the COVID-19 global pandemic.
› **Read more**

SEC Provides Observations on "Credential Stuffing" Cyberattacks
On Sept. 15, 2020, OCIE issued a cybersecurity Risk Alert warning about an increase in cyberattacks against registered investment advisers and broker-dealers using "credential stuffing."
› **Read more**

SEC Resolves Digital Token Offering Case
On October 20, 2020, the SEC and Kik Interactive Inc. resolved a multi-year litigation regarding Kik's offer and sale of digital tokens called Kin. The SEC sued Kik alleging that the Kin offering should have been registered with the SEC.
› **Read more**

Schulte Roth & Zabel

Private Funds Regulatory UPDATE

CFTC Sanctions Trader for Insider Trading by "Misappropriating" Employer's Trade Data and Analysis

Although insider trading cases typically arise in the equities markets, managers should be reminded that the Commodity Futures Trading Commission has asserted its authority to bring such actions in the commodity interest space as well.

› **Read more**

CFTC Compliance Program Evaluation Factors Released

On Sept. 10, 2020, the CFTC announced new guidance from its Division of Enforcement outlining factors that will be considered when evaluating a regulatory compliance program in connection with an enforcement matter.

› **Read more**

"Spoofing" Continues to Draw Heavy Enforcement Attention

Spoofing, a form of manipulative trading conduct in which a trader enters buy or sell orders into the market that they have no genuine intention of fulfilling, remains an area of keen interest for regulators as well as exchange-level enforcement officers.

› **Read more**

CFTC Finalizes Simplifying Amendments to CPO Quarterly Reporting Form

On Oct. 6, 2020, the CFTC voted to adopt amendments to Form CPO-PQR, the standard quarterly reporting form that is furnished to the CFTC (via submission to the NFA) by registered commodity pool operators.

› **Read more**

NFA Updates Annual Questionnaire

National Futures Association member commodity pool operators are required to update their "Annual Questionnaire" — an online template that aggregates various information about a member's business and operated commodity pools — on an annual basis (or upon the occurrence of certain events).

› **Read more**

NFA Announces Expiration of COVID-19-Related Relief from Fingerprinting Requirements for New APs and Principals

Earlier this year, the CFTC and the NFA implemented temporary relief from the requirement to obtain fingerprints in connection with registering principals and associated persons. On Sept. 29,2020, the NFA announced that this relief would end and provided additional guidance.

› **Read more**

SEC Sanctions a Registered Broker-Dealer for Text Message Recordkeeping Failures

On Sept. 23, 2020, the SEC released a cease-and-deist order imposing remedial sanctions arising out of the failure of a registered broker-dealer to retain business-related texts with clients, as required by the provisions of Section 17(a) of the Securities Exchange Act and SEC Rule 17a-4(b)(4).

› **Read more**

European Funds — ESMA Liquidity Stress-Testing Guidelines Take Effect
ESMA Liquidity Stress-Testing Guidelines took effect on 30 Sept. 2020. The guidelines set out detailed requirements applicable to EU managers of alternative investment funds and UCITS.
› **Read more**

SEC Accredited Investor Definition Updated

As we discussed in an earlier *Alert,*[1] on Aug. 26, 2020, the Securities and Exchange Commission broadened[2] the definitions of "accredited investor" ("AIs") in Regulation D under the Securities Act of 1933. The AI definition is key in determining who is eligible to participate, under the safe harbor contained in Rule 506 of Regulation D, in offerings of securities not subject to registration under the Securities Act. The exemption afforded by Regulation D is widely relied upon by private fund managers as well as other types of issuers.

The final rule largely reflects the SEC's December 2019 proposal, and is primarily a collection of gap-filling amendments. Among other changes, the Final Rule adds to Rule 501(a) two new categories of natural person AIs ("knowledgeable employees" as defined in Rule 3c-5(a)(4) of the Investment Company Act of 1940, and holders of the FINRA Series 7, 65 and 82 exam credentials) and several new categories of qualifying entities (including exempt reporting advisers, family offices and their clients, and, as a "catch all," entities not otherwise covered with more than $5 million in investments generally).

While the expansion of the types of investors that qualify as AIs is relatively modest, they should be understood by all private fund managers that rely on Regulation D, if only because these amendments likely will require changes to fund subscription documentation.

‹ **Table of Contents** **Read Next** ›

---

[1] *See SRZ Alert*, "SEC Updates Accredited Investor and QIB Definitions," (Sept. 21, 2020), available here.

[2] *See* SEC, Amending the "Accredited Investor" Definition, Release Nos. 33-10824; 34-89669, (Aug. 26, 2020), available here.

Fund Administrators Sanctioned by SEC

On Sept. 18, 2020, the SEC sanctioned two related administrators for contributing and causing violations of sections 206(2) and 206(4) of the Investment Advisers Act and Rule 206(4)-8 thereunder by L-R Managers LLC ("L-R").[1] Beginning in January 2016, the administrators performed several actions at the request of L-R, including permitting unsupported withdrawals by the adviser and allowing questionable accounting classifications and unsupported valuations that resulted in inaccurate valuations of client portfolios.

While the violations that the SEC cited for the administrators do not directly relate to investment management activities, private fund managers should view this action as a reminder that they are expected to provide administrators and other gatekeepers with sufficient support for all instructions and actions that can affect asset values. Also, this action serves as a reminder that performing effective due diligence and understanding the controls that key service providers have in place is essential.

‹ Table of Contents **Read Next ›**

[1] https://www.sec.gov/litigation/admin/2020/ia-5585.pdf

SEC Staff Provides Guidance Regarding Disciplinary History Disclosure Standard in Form CRS

On Oct. 8, 2020, the staff of the SEC's Division of Investment Management and of the Division of Trading and Markets released additional FAQs[1] relating to Form CRS. These FAQs are focused on disciplinary history disclosures required of Form CRS filers (e.g., registered investment advisers with natural person clients) and their personnel. Public statements from SEC personnel indicate they have observed that many Form CRS filers were either omitting the disciplinary history section of Form CRS altogether or providing additional disclosure with respect to disciplinary history, which is inconsistent with the Form CRS instructions.[2] The FAQs clarify that:

- Even if a Form CRS filer does not have a reportable disciplinary history, it must include an affirmative statement to that effect in its Form CRS;
- An adviser may separately respond for the adviser and for its personnel (e.g., "No for our firm. Yes for our financial professionals.");
- An adviser may not alter the headings and prompts required by the Form CRS instructions to fit its disciplinary situation; and
- The Form CRS should not be used as a platform to provide additional context around a disciplinary disclosure beyond what the instructions require.

Advisers required to file Form CRS should carefully review their filings to confirm that their disciplinary history disclosures are consistent with the Form CRS instructions and other regulatory reporting.

‹ **Table of Contents** **Read Next** ›

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

[2] Securities and Exchange Commission, Joint Statement Regarding New FAQs on Form CRS, available here.

SEC Chairman Highlights Robust Rulemaking, Enforcement and Examination Statistics

On Oct. 8, 2020, SEC Chairman Jay Clayton provided an overview of SEC's 2020 fiscal year goals and accomplishments, including its rule enforcement activities, at the "SEC Speaks" forum.[1] Of particular note, Chairman Clayton highlighted the SEC's rulemaking, examination and enforcement statistics, which show that the SEC has remained highly active in its oversight of market participants even in the midst of the COVID-19 global pandemic (and has been very much on the lookout for violations connected to the pandemic).

The Chairman noted that the Division of Enforcement brought over 700 actions in the 2020 fiscal year, many of which occurred after the onset of COVID-19-related shutdowns in March, and obtained financial remedies of more than $4 billion, which exceeded last year's total. In addition, the SEC awarded record whistleblowing compensation: 39 individual whistleblowers received approximately $175 million — a significant increase over "any prior fiscal year."

He also reported on the performance of the Office of Compliance Inspections and Examinations ("OCIE"), noting that, in the 2020 fiscal year, OCIE:

- Examined 15% of all SEC-registered investment advisers;
- Verified 4.8 million investor accounts totaling $3.4 trillion in assets; and
- Performed extensive outreach activities to "[drive] a culture of compliance," including over 300 outreach events, a report on Cybersecurity and Resiliency Observations and eight risk alerts.

In addition to providing data on the increased supervision of areas relevant to private fund managers, Chairman Clayton's remarks show that the SEC intends to be and remain a vigorous market regulator.

‹ Table of Contents **Read Next ›**

[1] *See* SEC Chairman Jay Clayton, An Update on FY 2020 Results — Remarks at SEC Speaks (Oct. 8, 2020), available here.

SEC Provides Observations on "Credential Stuffing" Cyberattacks

On Sept. 15, 2020, OCIE issued a cybersecurity Risk Alert[1] warning about an increase in cyberattacks against registered investment advisers and broker-dealers using "credential stuffing." Based on recent examinations, OCIE has observed that credential stuffing is an increasingly effective method of attack that can be used to steal assets from customer accounts and access sensitive information.

What is credential stuffing?

Credential stuffing is a type of cyberattack perpetrated by collecting compromised client login credentials from the dark web and, through the use of automated scripts, employing those credentials to gain unauthorized access to customer accounts and firm systems. These attacks are more effective than more traditional means, such as trying to guess passwords by attempting all of the words in a dictionary, because attackers are able to leverage specific information collected online, such as user names, email addresses and associated passwords. If successful, a cybercriminal gains access to a firm's accounts and systems, enabling the theft of assets from customer accounts and access to confidential information (including additional login credential information) and network resources. Information obtained by the attacker could be sold to other cybercriminals on the dark web. Bad actors may even monitor or take control of a customer's or employee's account.

OCIE observed that internet-facing websites — sites that are accessible to the public as opposed to sites that may only be access internally — are most vulnerable. This often includes sites hosted by third-party vendors. The presence of personal information on easily located internet-facing sites, such as the email address of a CTO, can also be combined with information retrieved from the dark web to obtain unauthorized access to accounts.

What steps should managers take to safeguard accounts and systems against credential stuffing?

OCIE encourages fund managers to be proactive in mitigating the risk of credential stuffing, including:

- *Password Policies and Procedures*. Periodic review of policies and programs with a specific focus on updating password policies to incorporate a recognized password standard requiring strength, length, type and change of passwords practices that are consistent with industry standards. OCIE has observed that successful attacks occur more often when (1) individuals

[1] *See* Cybersecurity: Safeguarding Client Accounts against Credential Compromise (Sept. 15, 2020), available here.

use the same password or minor variations of the same password for different online attacks; or (2) using login usernames that are easily guessed;

- *Multi-Factor Authentication ("MFA")*. Use of MFA to authenticate the person seeking to log in to an account, which can offer one of the best defenses to password-related attacks and significantly decrease the risk of an account takeover. As MFA frequently relies on sending data to mobile devices, OCIE warns of the need to be alert to when devices are lost or no longer working;
- *CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)*. Deployment of CAPTCHAs, which requires users to enter information to verify that they are not bots, frustrates the use of automated scripts used in credential stuffing;
- *Controls to Detect and Prevent*. Implementation of controls to detect and prevent credential-stuffing attacks. For example, monitoring for a higher than usual number of login attempts or implementing a Web Application Firewall ("WAF") that can identify and thwart credential stuffing attacks);
- *Dark Web Monitoring*. Surveillance of the dark web for lists of leaked user IDs and passwords; and
- *Training*. Educate employees and customers on the use of strong, unique passwords and on potentials signs of an attempted or successful cyberattack.

‹ **Table of Contents** **Read Next** ›

SEC Resolves Digital Token Offering Case

On October 20, 2020, the SEC and Kik Interactive Inc. resolved a multi-year litigation regarding Kik's offer and sale of digital tokens called Kin. The SEC sued Kik, a Canadian company known for its instant messaging program, alleging that the Kin offering should have been registered with the SEC. Kik countered that the Kin token was not an offering of securities requiring registration under the securities laws. The case received significant press coverage because Kik was one of only a few companies to challenge the SEC's crackdown on initial coin offerings in federal court.

After extensive discovery, the U.S. District Court for the Southern District of New York granted summary judgment in the SEC's favor ruling that Kik violated Section 5 of the Securities Act by offering and selling securities without a registration statement or exemption from registration. In ruling for the SEC, the Court focused on the "economic realities" of the transaction at issue. According to the SEC, the Kin tokens were securities under Supreme Court precedent. The test of whether a transaction is an investment contract or security is whether it involves an (1) investment of money; (2) in a common enterprise; (3) with the expectation of earning profits; and (4) solely from the efforts of the promoter or a third party." The Court ruled in the SEC's favor, but left it up to the parties to negotiate a final judgment. The parties have proposed a $5-million fine and a requirement that Kik inform the SEC about any future transactions involving digital assets for a period of three years. The Court has not yet approved the final terms of the agreement.

This case, along with similar enforcement actions, makes clear to digital asset providers and purchasers that the SEC and federal courts will scrutinize the underlying economics of these asset sales to determine whether they comply with the registration requirements and antifraud provisions of the federal securities laws.

‹ Table of Contents **Read Next ›**

CFTC Sanctions Trader for Insider Trading by "Misappropriating" Employer's Trade Data and Analysis

Although insider trading cases typically arise in the equities markets, managers should be reminded that the Commodity Futures Trading Commission has asserted its authority to bring such actions in the commodity interest space as well. In recent years, the CFTC has shown a particular interest in pursuing such actions under a "misappropriation" theory — i.e., where an individual has used proprietary information of an employer to advantage his or her personal trading, breaching confidentiality and duty-of-loyalty obligations through the use of material, non-public information.

As part of this trend, on Sept. 30, 2020, the CFTC settled charges[1] against Marcus Schultz, a former natural gas futures trader who, over a period of approximately three years, provided a broker with unauthorized disclosures of proprietary information about his employer's planned trading and private market analysis. Using "insider" trading information, the broker and Mr. Schultz contrived scenarios in which Mr. Schultz would execute non-competitive trades on behalf of his employer against the broker or its customers, permitting the latter to earn enhanced profits, in which Mr. Schultz shared. Mr. Schultz and his broker used obfuscating tactics to hide his kickbacks as legitimate payments or investments, such as funneling money through intermediate entities owned by the broker or Mr. Schultz or his family members. For these and other alleged wrongful actions (including making false statements to the CFTC staff), Mr. Schultz was issued combined monetary penalties and disgorgement of $1.1 million and a six-year trading ban.

The CFTC's posture on insider trading is still developing, and it remains unsettled as to how far the CFTC is willing to extend its view of insider trading. However, by pursuing relatively straightforward insider trading actions in a misappropriation context, the CFTC may be laying the groundwork for more aggressive enforcement in this area.

‹ **Table of Contents** **Read Next ›**

[1] *See* CFTC Release No. 8266-20 (Sept. 30, 2020), available here.

CFTC Compliance Program Evaluation Factors Released

On Sept. 10, 2020, the CFTC announced new guidance[1] from its Division of Enforcement outlining factors that will be considered when evaluating a regulatory compliance program in connection with an enforcement matter. The guidance, which is the first of its kind issued by the Division, is intended to help staff identify whether an examinee's compliance program was reasonably designed and implemented to:

- *Prevent* the underlying misconduct at issue in the enforcement matter (for example, does the examinee have "written policies and procedures in effect throughout the period of misconduct reasonably addressed the type of misconduct at issue");
- *Detect* any misconduct (for example, were there adequate "internal surveillance and monitoring efforts"); and
- *Remediate* any misconduct (for example, was timely and appropriate action taken to "effectively address any impact of the misconduct, including to mitigate and cure any financial harm to others and restore integrity to the relevant markets").

While this high-level guidance is ostensibly intended to aid its staff in conducting an investigation — rather than as a guide to market participants in crafting an effective compliance program — it may serve as a useful reference for CFTC-registered managers when self-evaluating the robustness of their compliance programs. Managers whose compliance programs are benchmarked only against National Futures Association guidance on supervision and internal controls are apt to find that their programs exhibit many of the hallmarks of effectiveness that the CFTC identifies, but should confirm that their programs are broad enough to cover the full breadth of the CFTC's focus.

‹ **Table of Contents** **Read Next ›**

[1] See CFTC Release No. 8235-20, available here.

"Spoofing" Continues to Draw Heavy Enforcement Attention

Spoofing, a form of manipulative trading conduct in which a trader enters buy or sell orders into the market that they have no genuine intention of fulfilling, remains an area of keen interest for regulators as well as exchange-level enforcement officers. At the end of September alone, the CFTC, the Intercontinental Exchange ("ICE") and the CME Group announced settlement of a number of spoofing cases.

- Most prominently, on Sept. 29, 2020,[1] the CFTC issued an order filing and settling charges against JPMorgan Chase & Company and several subsidiaries (collectively "JPM") for extensive manipulative conduct over at least an eight-year period involving hundreds of thousands of spoofed precious metals and U.S. Treasury futures orders on the COMEX, NYMEX and CBOT exchanges. The order, which includes restitution, disgorgement and civil monetary penalties totaling over $920 million, is the largest monetary relief ever imposed by the CFTC. Parallel criminal, civil and individual enforcement actions for key involved traders were also implicated. According to the order, JPM's conduct involved numerous traders sending false market signals to induce counterparties to execute against certain orders by placing misleading buy or sell orders with an intent to cancel prior to execution, thus artificially affecting prices. Contrary to its compliance obligations, JPM failed to identify, investigate and terminate such practices. Its supervision failures persisted in spite of a variety of red flags and internal alerts, as well as regulators' inquiries. While noting that JPM became cooperative in later phases of its investigation, the CFTC remarked that JPM's responses to certain earlier communications had been misleading.
- On Sept. 30, the CFTC issued an order[2] filing and settling charges against Sunoco LP for spoofing-related violations. For approximately a year, ending January 2015, the CFTC found that on multiple occasions a former Sunoco LP trader engaged in a pattern of placing small and large orders on opposite sides of the market in NYMEX crude oil, gasoline and heating futures, frequently canceling the larger buy or sell order shortly their smaller (actually intended) order was filled. Sunoco was fined $450,000 for this disruptive conduct. The CFTC did, however, acknowledge that upon discovering the trader's spoofing, the firm took substantial remedial actions, including conducting a full investigation, suspending the implicated trader, and improving its trade monitoring, compliance processes and training to make its compliance

[1] *See* CFTC Release No. 8260-20 (Sept. 29, 2020), available here.

[2] *See* CFTC Release No. 8267-20 (Sept. 30, 2020), available here.

program more robust against spoofing. These measures appear to have resulted in a reduced financial penalty.

- Also on Sept. 30, ICE announced a settlement with ARB Trading Group North LLC involving approximately $78,500 in penalties including fines and disgorgement for ARB, along with separate financial penalties (spanning approximately 40 to 56 thousand dollars each) and trading suspensions for three affiliated traders.[3] In each case, ICE had identified conduct involving a pattern of futures trading in which the sanctioned persons "instead of entering orders with the intent to trade, … appeared to have entered multiple orders on one side of the orderbook to create false depth, put pressure on the market, and mislead market participants into trading against, or moving the market closer to, [their] opposing small-quantity orders." In addition to possible trading practices violations, ICE also observed that ARB may have failed to adequately supervise its employees. Under the terms of the settlements, ARB and its traders neither admitted nor denied rule violations.
- On the same day, CME Group announced two spoofing-related settlements totaling $75,000[4] against 303 Proprietary Trading LP (for activity on both CME and COMEX), as well as two settlements (including trading suspensions) of $35,000[5] and $50,000[6] against individual traders for activity on CME and COMEX, respectively. In each case, the sanctioned party neither admitted nor denied violating any rules. CME Group sanctioned Proprietary Trading LP for failing to adequately train and supervise its employees (rather than for disruptive trading, per se), citing conduct in which an employee entered layered orders without the intent to trade ("after receiving fills on smaller orders he entered that were resting on the opposite side of the order book, the employee canceled the layered orders"). In each of the latter cases, the involved individual was sanctioned for disruptive trading involving a similar pattern of conduct.

Managers should note that these cases illustrate the same basic pattern of conduct: In an attempt to improve the favorability of an authentic, smaller, buy or sell order, a trader places a much larger order opposite to this position, only to cancel it as soon as their desired position is filled. Such behavior can

[3] *See* ICE Disciplinary Notice (Sept. 30, 2020), available here; ICE Disciplinary Notice (Sept. 30, 2020), available here; ICE Disciplinary Notice (Sept. 30, 2020), available here; and ICE Disciplinary Notice (Sept. 30, 2020), available here.

[4] *See* CME Notice of Disciplinary Action (Sept. 30, 2020), available here; COMEX Notice of Disciplinary Action (Sept 30, 2020), available here.

[5] *See* CME Notice of Disciplinary Action (Sept. 30, 2020), available here.

[6] *See* COMEX Notice of Disciplinary Action (Sept. 30, 2020), available here.

potentially disrupt efficient price discovery in the market, which makes spoofing a persistent and serious concern for regulators and exchange-level enforcement officers.

As always, market participants must remain vigilant about enforcing compliance with all applicable rules (including exchange-level rules) against non-bona fide, disruptive and manipulative trading, such as spoofing. Merely adopting written policies against such trading, without further surveillance and similar actions, likely will not be deemed to be sufficient.

Compliance officers should also take note that enforcement actions in these areas can be based on failure to supervise as well as trading conduct violations. Accordingly, employees must be fully trained so as to understand what constitutes impermissible trading under a firm's policies, and firms must actively monitor for employee compliance.

‹ Table of Contents **Read Next ›**

CFTC Finalizes Simplifying Amendments to CPO Quarterly Reporting Form

On Oct. 6, 2020,[1] the CFTC voted to adopt amendments to Form CPO-PQR, the standard quarterly reporting form that is furnished to the CFTC (via submission to the NFA) by registered commodity pool operators. Broadly speaking, the CFTC's amendments will simplify this common filing, particularly for certain larger filers. Most notably, the amendments will:

- Eliminate filing thresholds and categories that currently result in CPOs of different sizes having significantly different reporting obligations on Form CPO-PQR;
- Delete the detailed Schedules B and C of Form CPO-PQR (except for the "Schedule of Investments"), which were previously completed by large filers (and with respect to Schedule B, mid-size filers in the fourth quarter);
- Request LEI codes for CPOs and commodity pools that make use of them;
- Delete questions regarding auditors and marketers; and
- Replace the current "substituted compliance" system of accepting Form PF in lieu of Form CPO-PQR with accepting NFA Form PQR — the NFA's own quarterly pool report — in lieu of CFTC Form CPO-PQR.

In practice, these changes mean that NFA Form PQR will effectively replace CFTC Form CPO-PQR, as even investment advisers filing on SEC Form PF and relying on substituted compliance have still been completing NFA Form PQR as an NFA membership requirement. Large filers (those with assets under management exceeding $1.5 billion) who were *not* relying on Form PF substituted compliance will see the most benefit from the CFTC's amendments, due to no longer having to complete most of Schedules B and C of the current Form CPO-PQR.

To further ease registrants' transition to the new format, the revised Form CPO-PQR will be due following first quarter end in 2021. The CFTC's staff is currently preparing updated "FAQs" reflecting its amendments.

‹ **Table of Contents** **Read Next ›**

[1] *See* Press Release: CFTC Unanimously Approves a Final Rule Amending Form CPO-PQR (Oct. 6, 2020), available here.

NFA Updates Annual Questionnaire

National Futures Association member commodity pool operators are required to update their "Annual Questionnaire" — an online template that aggregates various information about a member's business and operated commodity pools — on an annual basis (or upon the occurrence of certain events). On Oct. 2, 2020, the NFA announced a streamlined Annual Questionnaire[1] which, among other things:

- Consolidates multiple, member category-specific questionnaires into one master Annual Questionnaire;
- Adds dynamic question logic that removes irrelevant questions; and
- Improves integration with other NFA filing systems such as EasyFile and the Online Registration System.

A transcript and recording from a webinar on the updated Annual Questionnaire will be made available to acquaint compliance personnel with the new framework. NFA members should note that there will be no grandfathering in of the old format — all members who access the system on or after Oct. 2 (including those who have an in-progress update) will need to complete their changes using the new system.

‹ **Table of Contents** **Read Next ›**

[1] *See* NFA Notice I-20-33, available here.

NFA Announces Expiration of COVID-19-Related Relief from Fingerprinting Requirements for New APs and Principals

Earlier this year, the CFTC and the NFA implemented temporary relief from the requirement to obtain fingerprints in connection with registering principals and associated persons. On Sept. 29, 2020,[1] the NFA announced that this relief would end and, accordingly:

- As of Oct. 1, 2020, all new applications for principal or associated-person registration must submit a fingerprint card as previously required; and
- All persons who are currently relying on the CFTC's and NFA's relief from the fingerprinting requirement (including APs granted a temporary license) must submit a fingerprint card to the NFA by Nov. 2, 2020.

The NFA is willing to address the circumstances of applicants who may still find it "impossible or inordinately difficult" to obtain fingerprints on a case-by-case basis (firms with such applicants are directed to contact information@nfa.futures.org or dial their information center at +1-800-621-3570). However, we expect that the NFA will now begin requiring fingerprint cards from the large majority of registrants as per usual.

‹ **Table of Contents** **Read Next ›**

[1] *See* NFA Notice I-20-37 (Oct. 6, 2020), available here.

SEC Sanctions a Registered Broker-Dealer for Text Message Recordkeeping Failures

On Sept. 23, 2020,[1] the SEC released a cease-and-deist order imposing remedial sanctions arising out of the failure of a registered broker-dealer to retain business-related texts with clients, as required by the provisions of Section 17(a) of the Securities Exchange Act and SEC Rule 17a-4(b)(4).

The background to this action is interesting in that the violations were uncovered indirectly. During the course of an unrelated investigation, the SEC requested records from the broker-dealer that indicated the existence of text messages between the firm's representatives and the investigation subject. When the broker was unable to furnish copies of these messages, which also were prohibited by its policies, the SEC's subsequent investigation revealed that several employees in fact were using text messages on personal devices for business communications for a variety of trade order and market communications with clients, and that such activities were known to senior management (who had even participated in certain impermissible text messaging practices themselves). These communications were not retained in the broker's books and records.

As part of a settlement in which the broker-dealer neither admitted nor denied wrongdoing, the firm was required to pay a $100,000 fine and is subject to a cease-and-desist order. The SEC highlighted that the broker-dealer had taken substantial remedial measures to address its violations, including employee education and implementation of a specialized retention system for employees interested in using personal devices for business communications.

While not involving an investment adviser, this case underscores the increasing importance of attention to personal device text messaging as a firm communication channel, and reaffirms that having written policies and training in this area will not immunize registrants — including registered investment advisers — whose personnel ignore firm and SEC recordkeeping requirements in practice.

‹ **Table of Contents** **Read Next** ›

[1] *See* SEC matter (Sept. 23, 2020), available here.

European Funds — ESMA Liquidity Stress-Testing Guidelines Take Effect

ESMA Liquidity Stress-Testing Guidelines took effect on 30 Sept. 2020. The Guidelines set out detailed requirements applicable to EU managers of alternative investment funds and UCITS. The requirements set out the regulatory expectations with regards to the arrangements and procedures adopted by such managers to monitor and manage liquidity risk within their fund porfolios. The aim of liquidity risk management policies is to ensure alignment of the investment strategy, liquidity profile and redemption policy of each fund. Among other things, the Guidelines specify the regulatory expectations with regards to the content of written liquidity stress-testing policies, governance and oversight of liquidity management, and recommended frequency of liquidity stress tests.

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

Schulte Roth & Zabel

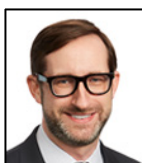
Private Funds Regulatory UPDATE

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

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

This communication is issued by Schulte Roth & Zabel LLP and Schulte Roth & Zabel International LLP for informational purposes only and does not constitute legal advice or establish an attorney-client relationship. In some jurisdictions, this publication may be considered attorney advertising. ©2020 Schulte Roth & Zabel LLP and Schulte Roth & Zabel International LLP. All rights reserved. SCHULTE ROTH & ZABEL is the registered trademark of Schulte Roth & Zabel LLP.