FIA Commodities Symposium
June 10 – 11, 2019

Hot Topics in CFTC and FERC Enforcement

The U.S. Commodity Futures Trading Commission is now investigating money laundering: What does the recent creation of a "Bank Secrecy Act Task Force" mean for market participants?

Gregory Mocek, Partner Anthony Mansfield, Partner Jonathan Flynn, Senior Counsel Chelsea Pizzola, Associate Allen & Overy LLP Washington, D.C.

The US Commodity Futures Trading Commission (CFTC), the primary US regulator of the commodities and derivatives markets, recently announced the formation of a new Bank Secrecy Act Task Force (Task Force) within the CFTC's Division of Enforcement.[1] According to the CFTC, the purpose of the Task Force is to ensure that CFTC registrants who are subject to the Bank Secrecy Act – namely futures commission merchants (FCMs) and introducing brokers (IBs) – comply fully with their anti-money laundering (AML) obligations.[2] In announcing the Task Force, the CFTC pronounced that "when an FCM or an IB fails to … [maintain or] appropriately implement [Bank Secrecy Act] and AML procedures" … it "[w]ill be held accountable for the violation." For the first time, the CFTC has publicly acknowledged that it will pursue market participants for failure to fulfill AML regulatory obligations. This intention to pursue AML program deficiencies was further evident in the language in a recent CFTC complaint filed in litigation in federal court and the simultaneous announcement of the Task Force.

Background

AML requirements in the commodities and derivatives markets are not new – they have applied to FCMs and IBs since 2003, when the CFTC and Financial Crimes Enforcement Network (FinCEN), a bureau of the US Department of the Treasury, jointly adopted rules implementing the Patriot Act of 2001.[3] The FinCEN regulations require, among other things, that FCMs and IBs

---

1 *See* CFTC Release No. 7809-18 (Sept. 27, 2018).

2 Currently, the CFTC's AML requirements do not apply to commodity pool operators, commodity trading advisors, swap dealers, or major swap participants; however, the CFTC has be noted that such entities have certain AML-related reporting obligations under the existing currency transactions reporting regulations, foreign bank and financial account reporting regulations and international transportation of currency or monetary instrument regulations. They also have obligations under the sanctions programs that target jurisdictions or individuals and further US foreign and domestic policies.

3 CFTC Rule 42.2 implements the authority FinCEN delegated to the CFTC to examine FCMs and IBs and ensure that they comply with the Bank Secrecy Act regulations to which they are subject, and specifically requires every FCM and IB to comply with the applicable provisions of the Bank Secrecy Act, the FinCEN regulations promulgated thereunder, and with the requirements of

implement reasonable know-your-customer (KYC) procedures to verify the identity of any person seeking to open an account; maintain records of the information used to verify the person's identity; and determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to FCMs and IBs by any US government agency. The FCMs and IBs must also have appropriate risk-based procedures for conducting ongoing customer due diligence, including, but not limited to: (1) understanding the nature and purpose of customer relationships for the purpose of developing customer risk profiles; and (2) conducting ongoing monitoring to identify and report suspicious transactions (and, on a risk basis, to maintain and update customer information, including information regarding the beneficial owners of legal entity customers). The rules also require FCMs and IBs to file suspicious activity reports (SAR) with FinCEN in connection with suspicious transactions that an FCM or IB believes are relevant to a possible violation of any law or regulation.[4] As a matter of fact, the National Futures Association (NFA) adopted NFA Compliance Rule 2-9(c) to specifically impose these requirements on its member FCMs and IBs pursuant to its responsibilities as the designated self-regulatory organization for commodities and derivatives market participants.

Historically, the NFA ensured that FCMs and IBs complied with their AML obligations through annual audits and ongoing oversight of its members. For example, NFA Interpretive Notice to Compliance Rule 2-9 highlights the minimum standards of an adequate AML program and provides FCMs and IBs with specific guidance on satisfying the relevant requirements, which include:

(1) Establishing and implementing policies, procedures, and internal controls reasonably designed to prevent the financial institution from being used for money laundering or the financing of terrorist activities;

(2) Providing for independent compliance testing;

---

31 U.S.C. 5318(l) and 31 CFR 1026.220, which require that a customer identification program be adopted as part of the firm's Bank Secrecy Act compliance program.

[3] Importantly, the FinCEN rule that delegates authority to the CFTC, 31 CFR § 1010.810, provides, "Overall authority for **enforcement and compliance**, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter [i.e., 31 CFR Chapter X], is delegated to the Director, FinCEN." (Emphasis added) The rule only delegates to the CFTC (and other financial regulators) the authority to "**examine** institutions to determine compliance with the requirements of" the Bank Secrecy Act. *Id*.

[4] A transaction requires reporting where it is conducted or attempted by, at, or through a FCM or IB, it involves or aggregates funds or other assets of at least $5,000, and the FCM or IB knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part): (1) involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity; (2) is designed to evade the Bank Secrecy Act or its implementing regulations; (3) has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the FCM or IB knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or (4) involves use of the FCM or IB to facilitate criminal activity.

(3) Designation of an individual responsible for implementing and monitoring the day-to-day operations and internal controls of the AML compliance program;

(4) Providing ongoing training for appropriate personnel; and

(5) Including appropriate risk-based procedures for conducting ongoing customer due diligence.

The NFA also offers FCMs and IBs access to a proprietary system designed to assist in developing written compliance programs while furnishing supplementary information on the minimum components of programs and examples of suggested language. The NFA's AML Procedures System is intended to provide an outline for programs with the understanding that modifications may be necessary to address the specific AML risks associated with an FCM's or IB's business.

In contrast, the CFTC's role has traditionally been more limited. CFTC Rule 42.2 implements the authority FinCEN delegated to the CFTC *to examine* FCMs and IBs and to ensure that they comply with the Bank Secrecy Act regulations to which they are subject, including FinCEN's AML regulations. Because authority "to examine" is arguably narrower than authority to investigate and enforce, the CFTC's role in AML enforcement may have been interpreted as more of a supporting position relative to FinCEN. However, interpretations can evolve and creation of the Task Force appears to be an early sign that such a shift is taking place.[5]

Significance of the Bank Secrecy Act Task Force

Oversight by the NFA will continue, yet the creation of the Task Force signals a new, heightened attention by the CFTC's Division of Enforcement on AML and Bank Secrecy Act issues. This new scrutiny was manifest in the complaint filed by the CFTC against 1Pool Ltd. (1Pool) and its Austrian chief executive officer on September 27, 2018.

The CFTC alleged that 1Pool engaged in unlawful retail commodity transactions, failed to register as an FCM, and, notably, committed various supervisory violations under CFTC Rule 166.3 by failing to implement even basic KYC procedures to prevent money laundering.[6] 1Pool was *not* a CFTC registrant, but according to the CFTC, it was nevertheless required to adopt and oversee an

[5] In a 2016 case, the CFTC indicated that a private litigant may bring a claim for reparations for a violation of Rule 42.2. *Qureshi v. Nagel*, Comm. Fut. L. Rep. ¶ 33,787 (June 27, 2016).

[6] Notably, the CFTC did not pursue a claim under Rule 42.2, perhaps recognizing that FinCEN delegated to the CFTC only the authority to examine institutions for compliance with Bank Secrecy Act requirements and that FinCEN remains the government agency with overall authority to enforce compliance with the Bank Secrecy Act.

adequate AML program because CFTC Rule 166.3 applies to "any person who is registered *or required to be registered with the [CFTC]*" and 1Pool should have been registered as an FCM.[7] Moreover, because the CFTC has long taken the position that a violation of CFTC Rule 166.3 is a standalone claim that requires no underlying violation, this interpretation gives the impression that the CFTC believes that it has the authority to bring Bank Secrecy Act-related cases against any entity that is operating in a capacity that requires registration as an FCM or IB, at least through a failure to supervise claim under CFTC Rule 166.3. This authority is in addition to the NFA's authority to audit and supervise its members in its capacity as a designated self-regulatory organization. Accordingly, all market participants that function as FCMs and IBs must be aware of the AML obligations and should regularly confirm that they are in compliance with these regulatory requirements.

Cryptocurrency connection

The CFTC's new focus on AML and Bank Secrecy Act issues may be due, at least in part, to the rise of cryptocurrencies, which often allow for transactions to take place on an anonymous basis. The CFTC has successfully argued that cryptocurrencies are commodities and, therefore, transactions involving cryptocurrencies are subject to its jurisdiction under the Commodity Exchange Act.[8]

In the complaint filed against 1Pool, the CFTC specifically noted that 1Pool failed to perform its supervisory duties diligently as evidenced by the fact that "it requires its customer to provide nothing more than a username and email address as identifying information, in order to trade on its platform."[9] In this respect, 1Pool is not unlike many cryptocurrency trading platforms that may be currently operating unlawfully on an unregistered basis, even though they nominally do not solicit or accept business from the US. In practice, many such platforms could easily lack the robust KYC procedures that are necessary to ensure that they know the identity of their customers sufficiently to remain in compliance with the Bank Secrecy Act. Such entities should take note and develop AML programs that comply with the Bank Secrecy Act. Failure to do so may result in a CFTC enforcement action, regardless of where the entity is located.

* * * * *

7 *See CFTC v. 1Pool Ltd. et al*, Case No. 1:18-CV-2243 (D.D.C. Sept. 27, 2018) at para. 62 (emphasis original).
8 *See CFTC v. My Big Coin Pay, Inc.*, Case 1:18-cv-10077-RWZ, Doc. No. 106 (D. Mass. Sept. 26, 2018).
9 *See CFTC v. 1Pool Ltd. et al*, Case No. 1:18-CV-2243 (D.D.C. Sept. 27, 2018) at para 64.