

THE REVIEW OF  
**SECURITIES & COMMODITIES  
REGULATION**

AN ANALYSIS OF CURRENT LAWS AND REGULATIONS  
AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 55 No. 19 November 9, 2022

## AML RECENT DEVELOPMENTS: WHAT PRACTITIONERS NEED TO KNOW

*Recent AML legislation includes the AML Act of 2020, the Corporate Transparency Act, and FinCEN's initiatives in this area. In this article, the authors discuss these developments and then turn to other aspects of the AML Act and its implementation. These include FinCEN's first set of government-wide priorities for AML and counter-terrorist financing; a pilot program on sharing SARs with affiliates; and AML issues in ransomware, decentralization, and microcap securities. Finally, they note recent enforcement actions, including a \$100 million fine levied on Bitmex, a digital assets entity.*

By Betty Santangelo, Melissa G.R. Goldstein, and Hannah Thibideau \*

The last few years have been landmarks for regulatory change and enforcement in the anti-money laundering (“AML”) space. The beginning of 2021 saw the enactment of the Anti-Money Laundering Act of 2020 (the “AML Act”), including the Corporate Transparency Act (the “CTA”), one of the most significant pieces of AML legislation since the USA PATRIOT Act of 2001.<sup>1</sup> During that same time period and since then, numerous regulators have issued a flurry of advisories and other guidance on how to implement AML regulations and contend with the increase of financial activities involving cryptocurrency. Additionally, different regulators have brought significant enforcement actions that demonstrate their regulatory priorities. Simultaneously, while not addressed herein, there have

been significant developments in the sanctions space, including sanctions against Russia following its invasion of Ukraine.

### CORPORATE TRANSPARENCY ACT

Undoubtedly, the CTA is one of the most significant aspects of the AML Act. The CTA creates a federal beneficial ownership registry which will require certain domestic and international corporate entities to file information with the Financial Crimes Enforcement Network (“FinCEN”), a bureau of the U.S. Treasury Department (“Treasury”). On December 7, 2021, FinCEN commenced its much-anticipated rulemaking process to implement the requirements of the CTA by issuing a notice of proposed rule-making soliciting public comments relating to the beneficial ownership information reporting provisions of the CTA (the “CTA

---

<sup>1</sup> AML Act of 2020 (Division F of Pub. L. 116-283).

---

\* *BETTY SANTANGELO is Of Counsel, MELISSA GOLDSTEIN is a Partner, and HANNAH THIBIDEAU is an Associate at Schulte Roth & Zabe LLP. Ms. Santangelo and Ms. Thibideau concentrate their practices in white collar enforcement with specialties in the AML and sanctions areas, and Ms. Goldstein concentrates her practice in the AML and sanctions regulatory compliance areas. Their e-mail addresses are betty.santangelo@srz.com, melissa.goldstein@srz.com, and hannah.thibideau@srz.com.*

Proposed Rule”).<sup>2</sup> This was the first of three proposed rules; the other two proposed rules will address (a) the central database that will be created by FinCEN and (b) revisions to the Customer Due Diligence (“CDD”) Rule.<sup>3</sup> The CTA Proposed Rule was finalized on September 30, 2022 (the “CTA Rule”).<sup>4</sup>

The CTA Rule addressing beneficial ownership information describes who must file beneficial ownership reports, what information must be reported, and when reports must be filed. The CTA applies to broad categories of companies organized in the United States or required to register to do business in the United States *i.e.*, U.S. corporations, limited liability companies, and other similar entities, as well as non-U.S. companies registered to do business in the U.S. The CTA tasks FinCEN with maintaining a nonpublic database of that beneficial ownership information to be available for use by law enforcement agencies, regulators, and financial institutions. Beneficial ownership reporting by such companies is designed to provide greater transparency of organizational structure in order to aid the government in combatting illicit financing, among other harms. The CTA exempts many companies from these reporting

requirements, including, among others, publicly traded companies, banks, money transmitters, broker-dealers, registered investment advisors, and certain pooled investment vehicles.

The CTA Rule mirrors the CTA’s definition of beneficial owner, which includes individuals or entities that either (1) own or control at least 25% of the ownership interest in an entity or (2) exert “substantial control” over that entity. Substantial control is defined broadly, but includes actions such as serving as a senior officer in the entity or having decision-making authority over important matters. Unlike the CDD Rule, which limits beneficial ownership reporting information to one individual or entity, all beneficial owners who fit either of these categories must be reported.

The CTA requires reporting companies to file reports with FinCEN disclosing certain identifying information regarding the reporting company’s beneficial owners, such as name, date of birth, address, and unique identifying numbers from identifying documents. Under the CTA Rule, entities are expected to file these reports within 30 days for newly formed or newly registered entities, but existing reporting companies have until January 1, 2025 to file their reports. FinCEN expects these reports to be updated as beneficial ownership information changes.

## OTHER ASPECTS OF THE AML ACT AND ITS IMPLEMENTATION

The AML Act also outlines a broad range of new AML obligations for various financial institutions and certain private investment entities.<sup>5</sup> The AML Act also expands the government’s extraterritorial reach. For example, Section 6308 of the AML Act permits the Department of Justice and Treasury to subpoena foreign bank records in support of government investigations if the foreign bank maintains a correspondent account in

---

<sup>2</sup> FinCEN, Proposed Rule: Beneficial Ownership Information Reporting Requirements, 89 Fed. Reg. 69920 (Dec. 8, 2021), available at <https://www.govinfo.gov/content/pkg/FR-2021-12-08/pdf/2021-26548.pdf>; see also FinCEN, *Fact Sheet: Beneficial Ownership Information Reporting Notice of Proposed Rulemaking* (Dec. 7, 2021), available at <https://www.fincen.gov/news/news-releases/fact-sheet-beneficial-ownership-information-reporting-notice-proposed-rulemaking>.

<sup>3</sup> See AML Act Title LXIV Sections 6401-6403, which spells out the three stages of the proposals. The CDD Rule was originally issued in 2016. FinCEN, Final Rule: Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016), available at <https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf>.

<sup>4</sup> The CTA Proposed Rules was finalized by FinCEN after the authors drafted this article. See FinCEN, Final Rule: Beneficial Ownership Information Reporting Requirements, 87 Fed. Reg. 59498 (September 30, 2022), available at <https://www.govinfo.gov/content/pkg/FR-2022-09-30/pdf/2022-21020.pdf>.

<sup>5</sup> For further analysis of the AML Act by SRZ, see *Passage of Anti-Money Laundering Act of 2020 Includes Comprehensive BSA/AML Reform Measures* (Jan. 7, 2021), available at <https://www.srz.com/images/content/1/7/v2/177496/010721-SRZ-Alert-Passage-of-AML-Act.pdf>.

---

the U.S.<sup>6</sup> The government’s subpoena power isn’t limited to the correspondent account information, as the USA PATRIOT Act of 2001 allowed, but encompasses records related to any account at the foreign bank, including records maintained outside the U.S.

The AML Act expands the Bank Secrecy Act (“BSA”)<sup>7</sup> to include another industry that faces potential risks of money laundering: the arts and antiquities industry. Notably, the AML Act did not require FinCEN to issue an AML rule applicable to SEC-registered investment advisers (“RIAs”), which would impose obligations on RIAs similar to those imposed on BSA-regulated financial institutions, such as banks and broker-dealers. While FinCEN has already proposed an AML rule for RIAs in various forms throughout the years, support for it has recently renewed. For example, in March 2022, six democratic senators have urged Treasury to dust off this proposed RIA rule and require RIAs to implement AML programs, among other requirements.<sup>8</sup>

As required by the Act itself, implementation of the AML Act has been rolled out over time. On June 30, 2021, FinCEN, in consultation with Treasury and other regulators, issued the first set of government-wide priorities for AML and counter-terrorist financing policy (the “Priorities”), consistent with the obligations set forth in the AML Act.<sup>9</sup> The Priorities include, in no particular order: (1) corruption, (2) cybercrime, including cybersecurity and virtual currency, (3) foreign and domestic terrorist financing, (4) fraud, (5) transnational criminal organization activity, (6) drug trafficking organization activity, (7) human trafficking and human smuggling, and (8) proliferation financing. These priorities are designed to assist covered institutions in designing and calibrating their risk-based AML programs.

FinCEN goes into extensive detail as to each of these priorities, including highlighting prior advisories issued on many of the relevant topics, and the threat to

democracy and human rights each of these areas of concern implicate. While none of these priorities are particularly surprising, FinCEN highlighted new focus areas, such as domestic terrorism, as well as re-emphasizing the continued risks of long-standing areas of concern, such as corruption and fraud. While FinCEN has not yet issued regulations specifying how financial institutions should address the Priorities, these regulations are expected to be forthcoming soon.

More recently, further implementing the AML Act, in January 2022, FinCEN issued a proposed rule soliciting comments on the establishment of a limited-duration pilot program for sharing suspicious activity reports (“SARs”) with overseas affiliates, branches, and subsidiaries of U.S. institutions.<sup>10</sup> The program would terminate, consistent with the AML Act, on January 1, 2024, unless extended. Financial institutions that wish to participate in the pilot program must submit an application to FinCEN identifying certain information about the U.S. institution and the foreign affiliates or institutions with which the U.S. institution hopes to share its SAR information. There are certain limitations set forth in this SAR sharing proposed rule, including that SAR information cannot be shared with any overseas affiliates in China, Russia, or other jurisdictions highlighted by federal regulators. This is a first step in the long-advocated approach of sharing SARs with U.S. entities’ foreign affiliates, although the burdensome requirements and limited duration of this program may stymie participation.

## INCREASED FOCUS ON RANSOMWARE

FinCEN and Treasury’s Office of Foreign Assets Control (“OFAC”) have also focused on certain specific subject areas that have become more relevant in recent years. On October 15, 2021, FinCEN released a report examining trends related to ransomware payments in SARs from the first half of 2021.<sup>11</sup> Ransomware is malicious software that encrypts a victim’s files and holds the data hostage until a ransom is paid. This report is one of many expected reports forecasted by the AML

---

<sup>6</sup> AML Act § 6308.

<sup>7</sup> 31 USC § 5311 et seq.

<sup>8</sup> Senators Reed, Wyden, Durbin, Menendez, Brown, and Warner, *Letter to Janet Yellen, Treasury* (March 30, 2022), available at [https://www.reed.senate.gov/imo/media/doc/letter\\_to\\_ust\\_fince\\_n\\_anti-money\\_laundering.pdf](https://www.reed.senate.gov/imo/media/doc/letter_to_ust_fince_n_anti-money_laundering.pdf).

<sup>9</sup> FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (June 30, 2021), available at [https://www.fincen.gov/sites/default/files/shared/AML\\_CFT%20Priorities%20\(June%2030%2C%202021\).pdf](https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf).

---

<sup>10</sup> FinCEN, Proposed Rule: Pilot Program on Sharing of Suspicious Activity Reports and Related Information with Foreign Branches, Subsidiaries, and Affiliates, 89 Fed. Reg. 3719 (January 25, 2022), available at <https://www.govinfo.gov/content/pkg/FR-2022-01-25/pdf/2022-01331.pdf>.

<sup>11</sup> FinCEN, *Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (Oct. 15, 2021), available at [https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis\\_Ransomware%20508%20FINAL.pdf](https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf).

---

Act's mandate to periodically publish trends and threats identified in SARs. The report highlights that the number of SARs relating to ransomware significantly increased in comparison with prior years, with the total dollar value of the suspicious activity reaching almost \$600 million during the first six months of 2021. Notably, FinCEN identified bitcoin as the most common ransomware payment method.

Among other focal points, FinCEN's ransomware report outlined the increase in the number and severity of ransomware attacks in the U.S. since 2020. These attacks have occurred in any number of industries, including manufacturing, legal, and health care. In addition to identifying various trends in the way ransomware suspicious activity has been reported, FinCEN noted the importance of reporting ransomware-related activity to FinCEN and other regulators. The report also noted a number of ransomware variants used in attacks, as well as other common attributes of the ransomware-related SARs. Unsurprisingly, ransomware is specifically identified as part of the cybercrime priority outlined by FinCEN in the Priorities, described further in Section II above.

Prior to FinCEN's ransomware report, OFAC issued a similar ransomware advisory that highlighted the importance of developing strong cybersecurity protocols to prevent ransomware attacks, as well as flagging other key risks of providing payments in response to ransomware demands, including funding activities adverse to national security and incentivizing malicious actors to initiate additional attacks.<sup>12</sup> In the advisory, OFAC advises that companies may violate sanctions by potentially issuing ransomware payments to one of the malicious cyber actors that have been designated by OFAC as specially designated nationals. OFAC notes that certain prevention strategies, such as maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols, may reduce the risk of extortion by a sanctioned actor, as well as serve as mitigating factors in the event of a sanctions' violation.

---

<sup>12</sup> OFAC, *Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments* (Sept. 21, 2021), available at [https://home.treasury.gov/system/files/126/ofac\\_ransomware\\_advisory.pdf](https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf).

## DECENTRALIZATION RAISING AML CONCERNS

Another area that regulators have had to contend with of late is the ever-evolving cryptocurrency landscape. While regulators continue to regulate activities involving cryptocurrency, the technology simultaneously develops and new issues emerge. One of the more recent trends in the crypto space is the move toward decentralization applications. Decentralized autonomous organizations ("DAOs") are a relatively new type of organization found in this space, characterized by decentralized control; instead of a corporate structure, the organization's members make and implement collective decisions regarding the organization's operations.<sup>13</sup> DAOs are characterized by the lack of leadership that one typically expects to see in organizations, such as through executives and other governing members controlling the organization's actions, relying instead on the members' management. For example, members submit proposals to the group, which then votes on the proposals and codes into the system those proposals that receive majority support.

DAOs present a number of AML issues for financial institutions, including how to identify and verify the identity of members of the DAO, conduct sanctions screening on members, and, for higher-risk members, perform AML-related due diligence. Typically, financial institutions are obligated to collect certain information on their customers, like names, and monitor the transactions in which customers engage. DAOs present numerous challenges in implementing these sorts of processes. Importantly, the anonymity of the decentralized structure and the global reach of the organization's members imposes significant practical limitations on what a DAO could collect.

## MICROCAP SECURITIES

Regulators continue to be focused on low-priced, or microcap, securities. In November 2020, the Securities and Exchange Commission ("SEC") issued a bulletin on risks associated with omnibus accounts transacting in low-priced securities.<sup>14</sup> This bulletin fits into the long-

---

<sup>13</sup> See generally James Holbein and Justin Holbein, *Legal Issues Confronting Formation and Operation of a Decentralized Autonomous Organization (DAO)* (Dec. 6, 2021), available at <https://www.braumillerlaw.com/legal-issuesconfronting-formation-operation-decentralized-autonomous-organization-dao/>.

<sup>14</sup> SEC, Division of Trading and Markets, *Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced*

---

standing expressed concern from the SEC and other regulators as to how omnibus accounts can be misused. In this bulletin, the SEC emphasizes that foreign financial institutions engaging in low-priced securities trading through omnibus accounts present a high risk of, and possibility for, illicit activity.

The SEC further advises broker-dealers to consider their AML obligations when engaging in low-priced securities transactions effected through omnibus accounts. The bulletin emphasizes the importance of broker-dealers recognizing the obligation to establish risk-based, written AML programs that detect and report suspicious activity, and to file SARs relating to microcap securities when necessary, even if the ultimate beneficial owner is not considered the broker-dealer's client. In addition, the SEC reminds broker-dealers of their obligation to establish risk-based, written due diligence programs for correspondent accounts held for foreign financial institutions. In implementing AML programs, financial institutions should recognize the potential need to obtain necessary information about customers trading through certain omnibus accounts, depending on the level of risk that the broker-dealer identifies. While there is generally no obligation to obtain CIP or CDD information regarding a foreign institution's intermediary customers, the SEC cautions that broker-dealers should consider obtaining information on the ultimate beneficial owners of such funds or securities when due diligence identifies heightened risks.

Firms should continue to tread carefully when applying the SEC's historic omnibus guidance in the context of low-priced securities.<sup>15</sup> Managing the particular issues presented in heightened risk activities may require evaluating or modifying existing AML compliance programs, as well as identifying and reacting to the additional risks posed by transactions that come from foreign omnibus accounts.

## SIGNIFICANT ENFORCEMENT ACTIONS AND TRENDS

In addition to the expansion of regulations and the issuance of related guidance, there have also been

significant enforcement actions over the last several years, which highlight certain trends in enforcement relating to AML. A few of the notable enforcement actions in the AML and sanctions space are discussed below.

**Wells Fargo Advisors.** On May 20, 2022, the SEC settled an enforcement action with Wells Fargo Advisors (a/k/a Wells Fargo Clearing Services, LLC) for \$7 million, finding the broker-dealer failed to timely file at least 34 SARs.<sup>16</sup> According to the SEC's Order, these failures stemmed from the firm's failures in its transaction monitoring and alert system, including a failure to reconcile country codes used to monitor foreign wire transfers and a failure to appropriately process wire transfer data. This enforcement action highlights the importance of making sure automated systems work properly in identifying and tracking activity, and may signal a regulatory focus on this issue in the AML space.

**Bittrex.** In October 2022, FinCEN and OFAC entered into a settlement agreement with Bittrex, Inc., a crypto trading platform, requiring the payment of a civil money penalty in the amount of \$29 million to settle liability for AML and sanctions violations.<sup>17</sup> OFAC found Bittrex conducted thousands of transactions valued at over \$260 million with entities and individuals located in jurisdictions subject to comprehensive sanctions. FinCEN's investigation found that Bittrex failed to maintain an effective AML program because it failed to appropriately address the risks associated with the products and services it offered, including anonymity enhanced cryptocurrencies. In addition, Bittrex failed to file any SARs for a period of over three years.

**Bitmex.** In August 2021, the Commodity Futures Trading Commission ("CFTC") and FinCEN levied a \$100 million fine against Bitmex, a crypto derivative trading platform that offers futures, options, and swap trading in digital assets.<sup>18</sup> Bitmex failed both to establish an AML program with adequate AML policies and procedures and to register with the CFTC. The

---

*footnote continued from previous page...*

*Securities* (Nov. 12, 2020), available at <https://www.sec.gov/tm/risks-omnibus-accounts-transacting-low-priced-securities>.

<sup>15</sup> SEC and Treasury, *Question and Answer Regarding the Broker-Dealer Customer Identification Program Rule (31 CFR 103.122)* (Oct. 1, 2003), available at <https://www.sec.gov/divisions/marketreg/qa-bdidprogram.htm>.

---

<sup>16</sup> *In the Matter of Wells Fargo Clearing Services, LLC*, Rel. No. 94-955 (May 20, 2022), available at <https://www.sec.gov/litigation/admin/2022/34-94955.pdf>.

<sup>17</sup> Treasury, *OFAC Settles with Bittrex, Inc. for \$24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs* (Oct. 11, 2022), available at [https://home.treasury.gov/system/files/126/20221011\\_bittrex.pdf](https://home.treasury.gov/system/files/126/20221011_bittrex.pdf); *In the Matter of Bittrex, Inc.*, No. 2022-03 (Oct. 11, 2022), available at [https://www.fincen.gov/sites/default/files/enforcement\\_action/2022-10-11/Bittrex%20Consent%20Order%2010.11.2022.pdf](https://www.fincen.gov/sites/default/files/enforcement_action/2022-10-11/Bittrex%20Consent%20Order%2010.11.2022.pdf).

regulators noted Bitmex’s failure to, among other things, conduct sufficient CDD or use transaction monitoring or blockchain analytics tools, such as those that use address-clustering or other techniques to identify patterns of suspicious activity. This enforcement action highlights regulatory expectations that digital assets entities utilize blockchain analytics for their AML program compliance, supported by internal transaction monitoring systems.

**BitGo.** In December 2020, OFAC settled an enforcement action with BitGo, an institution offering secure digital wallet management, for almost \$100,000 for failures in BitGo’s sanctions compliance.<sup>18</sup> BitGo failed to prevent persons located in countries subject to comprehensive sanctions programs, such as Cuba and Iran, from using its non-custodial secure digital wallet management services, despite having access to IP address information that would identify those users’ locations. This enforcement action highlights the importance of digital currency providers implementing risk-based sanctions compliance programs. In the settlement announcement, OFAC also noted the swift corrective measures put in place by BitGo, highlighting the benefit that cooperation can engender in investigations.

In addition to enforcement actions against institutions, regulators are signaling a continued willingness to bring cases against individual actors behind a firm’s AML program failings if the deficiencies are particularly egregious. One such action is highlighted below.

**Arnold J. Feist.** In February 2022, FINRA fined Arnold Feist, the AML Compliance Officer at Interactive Brokers LLC, finding him personally liable

for failing to oversee an ineffective AML program.<sup>19</sup> Feist was suspended for two months and personally fined \$25,000. This fine follows on a \$38 million combined fine levied by FINRA, the SEC, and the CFTC in 2020 against Interactive Brokers LLC related to failures in its AML program. FINRA identified numerous failures by Feist, including the failure to implement and establish a reasonably designed AML program, failure to supervise analysts, and failure to file SARs, among others.

**CONCLUSION**

The developments described herein are just some of the recent focus areas of regulators as they apply AML regulations to financial institutions. This year will continue to see significant changes, as regulators continue to implement the AML Act, and enforcement continues to signal focus areas in AML and related areas. Further developments are also expected in the cryptocurrency space, as regulators continue to act on their growing knowledge base of this recently developed industry. ■

\*\*\*\*\*

*The substance of this article tracks the Industry Hot Topics panel, moderated by Justin Mendelsohn (Fidelity Digital Asset Services), on which Ms. Santangelo participated at the 2022 SIFMA AML and Financial Crimes Conference. Ms. Santangelo expresses her appreciation to Mr. Mendelsohn and the other panelists for their contributions to the panel.*

*This article is prepared by Schulte Roth & Zabel LLP for informational purposes only and does not constitute legal advice or establish an attorney-client relationship.*

<sup>18</sup> Treasury, *OFAC Enters into \$98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Dec. 30, 2020), available at [https://home.treasury.gov/system/files/126/20201230\\_bitgo.pdf](https://home.treasury.gov/system/files/126/20201230_bitgo.pdf).

<sup>19</sup> *Arnold J. Feist*, FINRA Letter of Acceptance, Waiver and Consent No. 2015047770302 (Feb. 11, 2022), available at <https://media2.mofo.com/documents/1464000-1464582-order-arnold-feist.pdf>.