UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:	)	
	)	**Number 2026-01**
Canaccord Genuity LLC	)	

CONSENT ORDER IMPOSING CIVIL MONEY PENALTY

The Financial Crimes Enforcement Network (FinCEN) conducted a civil enforcement investigation and determined grounds exist to impose a Civil Money Penalty against Canaccord Genuity LLC (Canaccord or the Firm) for violations of the Bank Secrecy Act (BSA) and its implementing regulations.[1] Canaccord admits to the Statement of Facts and Violations set forth below, consents to the issuance of this Consent Order, agrees to pay the civil money penalty imposed in this Consent Order, and agrees to comply with the Undertaking and other provisions of this Consent Order.

I. JURISDICTION AND RELEVANT REGULATIONS

A. Jurisdiction

Overall authority for enforcement and compliance with the BSA lies with the Director of FinCEN, and the Director of FinCEN may impose civil penalties for violations of the BSA and its implementing regulations.[2]

---

[1] The BSA is codified at 12 U.S.C. §§ 1829b, 1951–1960, 31 U.S.C. §§ 5311–5314, 5316–5336 and includes other authorities reflected in notes thereto. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.

[2] 31 U.S.C. § 5321(a); 31 C.F.R. § 1010.810(a), (d); Treasury Order 180-01 (July 1, 2014, reaff'd Jan. 14, 2020).

At all times relevant to this Consent Order, Canaccord was a "broker or dealer in securities," as defined by the BSA and its implementing regulations.[3] As such, Canaccord was required to comply with applicable BSA laws and regulations.

B. Relevant Regulations

AML Program: The BSA and its implementing regulations require broker-dealers such as Canaccord to implement and maintain an anti-money laundering (AML) program, including policies, procedures, and internal controls reasonably designed to achieve compliance with the applicable provisions of the BSA and its implementing regulations. Canaccord is also required to: (i) conduct independent testing for compliance; (ii) designate an individual or individuals responsible for implementing and monitoring the operations and internal controls of the program; (iii) conduct ongoing training for appropriate persons; and (iv) implement appropriate risk-based procedures for conducting ongoing customer due diligence including, but not limited to, (a) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile and (b) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[4]

Due Diligence on Correspondent Accounts for Foreign Financial Institutions: The BSA and its implementing regulations require all "covered financial institutions," including broker-dealers such as Canaccord, to establish a due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to enable the covered financial institution to detect and report, on an ongoing basis, any known or

[3] 31 U.S.C. § 5312(a)(2)(G), (b)(1); 31 C.F.R. § 1010.100(h), (t)(2).

[4] 31 U.S.C. § 5318(h); 31 C.F.R. § 1023.210(b).

suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by such covered financial institution in the United States for a foreign financial institution.[5]

FinCEN's regulations require that such due diligence programs include specific requirements, specifically: (i) determining whether any such correspondent account is subject to enhanced due diligence; (ii) assessing the money laundering risk presented by such correspondent account, based on a consideration of all relevant factors, which shall include, as appropriate: (a) the nature of the foreign financial institution's business and the markets it serves, (b) the type, purpose, and anticipated activity of such correspondent account, (c) the nature and duration of the covered financial institution's relationship with the foreign financial institution (and any of its affiliates), (d) the anti-money laundering and supervisory regime of the jurisdiction that issued the charter or license to the foreign financial institution, and, to the extent that information regarding such jurisdiction is reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered, and (e) information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record; and (iii) applying risk-based procedures and controls to each such correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose, and anticipated activity of the account.[6]

---

[5] 31 U.S.C. § 5318(i); 31 C.F.R. § 1010.610.

[6] 31 C.F.R. § 1010.610(a).

Suspicious Activity Reporting: Broker-dealers must identify suspicious transactions relevant to a possible violation of law or regulation in Suspicious Activity Reports (SARs) filed with FinCEN.[7] Specifically, the BSA and its implementing regulations require broker-dealers to report transactions that involve or aggregate to at least $5,000, are conducted or attempted by, at, or through the broker-dealer, and that the broker-dealer "knows, suspects, or has reason to suspect" are suspicious.[8] A transaction is "suspicious" if a broker-dealer "knows, suspects, or has reason to suspect" that the transaction (or a pattern of transactions of which the transaction is a part): (i) involves funds derived from illegal activities, or is intended or conducted to disguise funds derived from illegal activities; (ii) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations implementing it; (iii) 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 broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction; or (iv) involves the use of the broker-dealer to facilitate criminal activity.[9] A broker-dealer is generally required to file a SAR no later than 30 calendar days after the initial detection by the broker-dealer of the facts that may constitute a basis for filing a SAR.[10]

The reporting and transparency that financial institutions provide through these reports is essential financial intelligence that FinCEN, law enforcement, and others use to safeguard the U.S. financial system and combat serious threats, including money laundering, terrorist financing,

---

[7] 31 U.S.C. § 5318(g); 31 C.F.R. § 1023.320.

[8] 31 C.F.R. § 1023.320.

[9] 31 C.F.R. § 1023.320(a)(2).

[10] 31 C.F.R. § 1023.320(b)(3).

organized crime, corruption, drug trafficking, and massive fraud schemes targeting the U.S. government, businesses, and individuals.[11]

II. STATEMENT OF FACTS

The conduct described below took place from on or about March 2, 2018, through June 30, 2024 (the Relevant Time Period), unless otherwise indicated.

A. FinCEN

FinCEN is a bureau within the U.S. Department of the Treasury and is the federal authority that brings civil enforcement actions for violations of the BSA by investigating and imposing civil money penalties on financial institutions and individuals for willful violations of the BSA.[12] As delegated by the Secretary of the Treasury, FinCEN has "authority for the imposition of civil penalties" and "[o]verall authority for enforcement and compliance" with the BSA and its implementing regulations.[13]

B. SEC

The Securities and Exchange Commission (SEC) is the primary federal regulator of Canaccord and has both delegated authority from FinCEN[14] and separate authority under Title 15 of the United States Code for examining broker-dealers, including Canaccord, for compliance with the BSA and its implementing regulations and similar rules under Title 15 of the United States Code.

---

[11] FinCEN, FIN-2014-A007, FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (Aug. 11, 2014).

[12] 31 U.S.C. § 5321(a). In civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose. Canaccord admits to "willfulness" only as the term is used in civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1).

[13] 31 C.F.R. § 1010.810(a), (d).

[14] 31 C.F.R. § 1010.810(b)(6).

C. FINRA

The Financial Industry Regulatory Authority (FINRA) is a self-regulatory organization with delegated authority from the SEC for examining its member firms, including Canaccord, for compliance with the BSA and its implementing regulations. FINRA also issues rules that govern the conduct of its members, including minimum standards for AML programs.[15]

D. Canaccord

Canaccord is a Delaware limited liability company and SEC-registered and FINRA-member broker-dealer headquartered in New York, New York.[16] It is a subsidiary of Canaccord Genuity Group Inc., a financial services firm incorporated in British Columbia and publicly traded on the Toronto Stock Exchange.[17] Throughout the Relevant Time Period, Canaccord had two lines of business relevant to this Consent Order: (i) a wholesale market making business, which made markets and provided execution services in, among other things, over-the-counter (OTC) securities; and (ii) a trade execution business for Canaccord's institutional customers, which included money managers, hedge funds, financial institutions, and other legal entity customers.[18] As described in more detail below, during the Relevant Time Period, Canaccord was among the most active market makers in OTC low-volume and low-priced securities (including what are

---

[15] FINRA Rule 3310 requires that "[e]ach member shall develop and implement a written anti-money laundering program reasonably designed to achieve and monitor the member's compliance with the requirements of the Bank Secrecy Act (31 U.S.C. 5311, *et seq*.), and the implementing regulations promulgated thereunder by the Department of the Treasury." FinCEN's regulation requiring broker-dealers to implement an AML program requires, among other things, that broker-dealers comply with "the rules, regulations, or requirements of its self-regulatory organization governing such programs." 31 C.F.R. § 1023.210(c).

[16] FINRA, *BrokerCheck Report – Canaccord Genuity LLC – CRD# 1020* (accessed Feb. 16, 2026).

[17] *See* CANACCORD GENUITY GROUP INC., *Fiscal 2025 Annual Report* (for the fiscal year ending March 31, 2025, published May 22, 2025) at 15.

[18] FINRA, *BrokerCheck Report – Canaccord Genuity LLC – CRD# 1020* (accessed Feb. 16, 2026) at 12.

often referred to as "microcap" or "penny" stocks).[19] As of November 2025, Canaccord has exited and no longer operates its U.S. OTC wholesale market making business and significantly reduced the size and scope of its trade execution business.

E. Canaccord Failed to Implement and Maintain an AML Program

Canaccord willfully failed to implement and maintain an AML program that met BSA requirements during the Relevant Time Period. The failures, described in the subsections below, related to each of the regulatory requirements (commonly referred to as "pillars") of the AML program.

Canaccord's violations involved several different issues, but at its core, Canaccord failed to devote adequate resources to ensure compliance with the BSA. Throughout the Relevant Time Period, Canaccord relied extensively on trade surveillance reports that—if properly designed, calibrated, and reviewed—could have enabled the Firm to detect and report the types of potentially suspicious activity that the Firm recognized were most likely to arise in its OTC market making business, which the Firm had identified as a higher-risk business line. However, Canaccord failed, until at least late 2021, to make the relevant reports effective for this purpose, including sufficiently investing in the hiring, training, and oversight of AML personnel tasked with implementation and review of the trade surveillance reports. Even the deficient reports that Canaccord used for portions of the Relevant Time Period often went unreviewed for months or years at a time by AML personnel. Moreover, once a FINRA examination began to focus specifically on the review of such reports, two

[19] A "market maker" is a firm that stands ready to buy or sell a stock at publicly quoted prices. *See* SEC, *Market Centers: Buying and Selling Stock* (Oct. 15, 2012).

compliance employees at Canaccord falsified records to give the false impression that they were completing reviews of trade surveillance reports when they were not.[20]

As a result of these failures involving the Firm's trade surveillance reports—along with deficiencies in the Firm's customer due diligence (CDD) and other SAR-related processes—Canaccord willfully failed to implement and maintain a program that would, as required under the BSA, include policies, procedures, and internal controls reasonably designed to, among other things, detect and report suspicious activity, including multiple instances of securities fraud in the securities for which Canaccord acted as a market maker. Canaccord also willfully failed to investigate and report a high volume of suspicious transactions in its high-risk lines of business during the Relevant Time Period, including transactions tied to securities fraud and other market manipulation schemes. Based on preliminary results from a SAR Lookback, Canaccord failed to file at least 160 SARs relating to dozens of different OTC securities, the trading of which involved a high volume of underlying suspicious transactions that FinCEN estimates to be in the thousands.

1. Unreasonable Policies, Procedures, and Internal Controls Inappropriate for Canaccord's Business During the Relevant Time Period

Throughout the Relevant Time Period, Canaccord willfully failed to implement reasonably designed policies, procedures, and internal controls tailored to the risks the Firm faced, particularly given the heightened risks of fraud and similar illicit activity associated with OTC securities. Canaccord acknowledged these deficiencies as early as 2013 and repeatedly represented to regulatory examiners that it would remediate them; although Canaccord took certain steps to remediate some of these deficiencies, it ultimately failed to adequately address those, preventing the Firm from

[20] Canaccord subsequently terminated these employees after completing an investigation of the issue.

implementing policies, procedures, and internal controls reasonably designed to identify and report suspicious transactions, as required by the BSA and its implementing regulations.

a. Background on Canaccord's Higher-Risk Lines of Business

During the Relevant Time Period, Canaccord was among the most active participants in the trading of OTC securities, including "microcap" and "penny" stocks. As regulators have stated, these securities can pose elevated risks, including because they often lack public information, have no minimum listing standards, lack liquidity, and have high volatility—all factors that make them potentially more susceptible to manipulative trading and fraudulent schemes.[21] FinCEN, the SEC, and FINRA have repeatedly highlighted heightened risks and "red flags" associated with these types of securities, both for potential investors and broker-dealers like Canaccord.[22] Between 2018 and 2022, Canaccord ranked among the top five largest market makers (by trading volume) for OTC low-priced securities, executing nearly $70 billion in transactions where the stock traded for less than five dollars.

b. Prior Exam Findings Regarding AML Program Deficiencies

During regular exams that FINRA performed prior to the Relevant Time Period, FINRA cited several deficiencies in the Firm's AML program, including the design and implementation of trade

---

[21] *See, e.g.,* FINRA, *Avoid Fraud: Low-Priced Stocks Can Spell Big Problems* (Jan. 19, 2024) (highlighting increased potential for fraud and market manipulation in connection with "microcap" and "penny" stocks, with penny stocks defined as those issued by very small companies that trade at less than $5 per share).

[22] *See, e.g.,* FINCEN, *The SAR Activity Review Trends Tips & Issues, Issue 15*, "In Focus: The Securities and Futures Industry" (May 2009) at 24 (describing, among other things, "red flags" for the sale of unregistered securities, fraud, and market manipulation in connection with transactions involving low-priced securities); FINRA, *Notice to Members 19-18* (May 6, 2019); FINRA, *Notice to Members 21-03*, Feb. 10, 2021; SEC, *Risk Alert: Compliance Issues Related to Suspicious Activity Monitoring and Reporting at Broker-Dealers* (March 29, 2021) at 3-5; *see also* SEC, *Microcap Stock: A Guide for Investors*, (Sept. 17, 2013).

surveillance reports that the Firm purported to rely on to monitor the higher-risk lines of business described above, particularly in light of the volume of the Firm's trading activity.[23]

As described in more detail below, Canaccord utilized several trade surveillance reports to monitor for suspicious activity in both its market making and institutional execution businesses. At a high level, each automatically generated report was intended to capture transactions executed by or through Canaccord that contained one or more red flags for a particular type of potentially suspicious activity. For example, a report intended to identify potential instances of "wash sales"—trading involving no change in beneficial ownership that is intended to produce the false appearance of trading[24]—may have captured transactions where the same beneficial owner rapidly purchased and then sold the same security at the same price.

As early as 2013, FINRA identified deficiencies in Canaccord's AML program, including Canaccord's failure to implement an adequate program for detecting and reporting suspicious activity. Citing Canaccord's "high trade volume as a market maker in low-priced securities," FINRA recommended that Canaccord, among other things, increase its use of electronic and automated reports, including adopting a mechanism for identifying "abusive patterns in wire and trading activity." In response to these findings, Canaccord committed in writing to corrective action relating to adoption and implementation of automated trade surveillance reports for low-priced securities.

---

[23] The individual who served as Canaccord's AML Compliance Officer for most of the Relevant Time Period was aware that FINRA had cautioned Canaccord in 2014, 2017, and 2018 that it needed to implement automated AML trade surveillance; improve its review for suspicious trading activity, including timely review and documentation of surveillance and investigations; and review the activity of correspondent accounts for foreign financial institutions. *See,* FINRA, *Letter of Acceptance, Waiver, and Consent No. 2020066079904* (June 16, 2025) at 3-4.

[24] Wash sales (*i.e.*, trading involving no change in beneficial ownership that is intended to produce the false appearance of trading) continue to be strictly prohibited under both the federal securities laws and FINRA rules. *See, e.g.*, 15 U.S.C. 78i(a)(1); FINRA Rule 6140(b). FINRA, *Regulatory Notice 15-09* (May 26, 2015), n.4.

In 2016, FINRA once again identified deficiencies in Canaccord's AML program relating to, among other things, Canaccord's failure to "establish an adequate process for the detection and reporting of suspicious activity related to its market making business." In particular, given that Canaccord traded nearly 4,500 "low-priced Pink Sheet securities which typically trade under $1"—which, as noted above, can present heightened risks for investors and broker-dealers—the exam found the Firm's controls inadequate in reviewing for red flags relating to: (i) matched trades, (ii) pre-arranged trades, (iii) wash trades, (iv) deposit and almost immediate liquidation of securities, (v) dominating the volume of a security, and (vi) marking the close. Further, while Canaccord policy required compliance employees to review trades flagged by the Firm's proprietary monitoring system, a FINRA review of more than 50 sampled transactions found that, based on the materials the Firm had retained, "the subsequent investigation of flagged securities did not appear to be adequate." In response, the Firm committed in writing to enhance its trade surveillance capabilities. Canaccord made certain enhancements to such capabilities, but, as explained below, many deficiencies remained unaddressed within the Relevant Time Period.

c. Deficiencies in Canaccord's Trade Surveillance Reports

Consistent with the time period covered by the FINRA exams described above, throughout the Relevant Time Period, Canaccord relied on trade surveillance reports as its primary mechanism to monitor for potentially suspicious activity involving its trading businesses.

Many of the Firm's trade surveillance reports went unreviewed for extended periods of time or were reviewed by employees who did not have sufficient guidance, training, and AML experience to properly use the reports. In multiple instances, they set unreasonable parameters, including to reduce the volume of activity captured in the reports, rather than applying a risk-based approach to identify suspicious activity. These employees also failed to timely address design flaws and data

errors that created additional deficiencies with respect to certain of these reports. When FINRA requested evidence of the review of these reports, two compliance employees at Canaccord falsified records to give the false impression that they were completing reviews of trade surveillance reports when they were not. Because of these deficiencies, Canaccord failed to detect a high volume of suspicious transactions during the Relevant Time Period.

i. The Firm's Willful Failure to Review Trade Surveillance Reports

Until late 2021, just four Canaccord employees—each of whom maintained responsibilities other than trade surveillance—were tasked with reviewing more than 100 unique reports, many of which were daily reports and some of which produced thousands or millions of combined line items to review each year. Canaccord's deficient staffing was a significant factor in certain of these reports going unreviewed for long stretches during the Relevant Time Period.

Across its trading lines of business (including its market making business), for stretches of time ranging from months to four years, Canaccord entirely failed to review its low-priced, low-volume, pump and dump, self-trading, and wash sales reports. In addition to extended periods of time that reports were not reviewed, some reports were never meaningfully reviewed until late in the Relevant Time Period. This included, for example, a report that a compliance employee did not understand how to review.

ii. Willful and Fundamental Design Flaws and Longstanding Data Issues Related to Trade Surveillance Reports

As described below, several trade surveillance reports were also flawed in their original design and/or improperly used by Canaccord staff.

Low-Priced Reports: In addition to not being implemented until mid-2019 (years after a FINRA examination found the need for this report as a part of the Firm's AML program), the Low-

Priced Reports were not fit for the purpose of identifying potentially suspicious activity until at least late 2021. Prior to that time, these reports—which often went unreviewed during the Relevant Time Period—were generated daily and could include as many as 50,000 lines of data. Until at least late 2021, the employee responsible for reviewing the Low-Priced Report applied a manual filter that limited the reports to executions where (i) over 1 million shares were traded, and (ii) the execution amounted to more than 50% of the daily market volume for that security. The employee conceded that they selected the filter to "manage" the scope of the review, without regard for whether it meant the Firm was reviewing the suspicious activity that the report was designed to detect.

Moreover, the employee responsible for reviewing the report was aware that, due to a data issue, the report at times failed to include data for all relevant fields, including incorrectly reflecting the daily market volume for a security as "null," even though the security had in fact been traded that day.

Low-Volume Reports: Prior to at least late 2021, Canaccord's Low-Volume Report, which was reviewed only a limited number of times during this portion of the Relevant Time Period, was manually filtered to "get the total number [of in-scope transactions] down" and make the report "manageable." More specifically, the employee tasked with reviewing the Firm's Low-Volume Reports explained that, in their first "couple weeks on the desk"—and without any guidance from their supervisor—they adopted a "trial and error" process to arrive at "arbitrary numbers" of what the reviewing employee thought would be considered low volume without consideration for the actual risk profile of transactions captured by the report.

Pump & Dump Report: Canaccord's monthly Pump & Dump Report was similarly not reasonably designed or implemented. At the beginning of the Relevant Time Period, the report used by Canaccord's market making business only reflected transactions with a ***25% price movement that***

occurred in a single day. Such a threshold was not reasonable given that the patterns of activity that this report was intended to identify frequently take place over longer periods of time, and Canaccord had not conducted research or testing in establishing the parameters.[25] Despite some improvement, a second iteration of the report had criteria that were inconsistently applied and still failed to capture relevant trading activity.

Wash Sales: This report—which often ran more than 50 pages each day—was described by compliance personnel as simply "too long" to review. Moreover, the employee reviewing the report received no training on it and did not understand how to differentiate illegitimate trading activity, such as wash sales, from legitimate trading activity; one of the employees responsible for this report stated that they stopped reviewing it because they did not "know[] what it was [management] wanted me to look at," and ultimately determined that they could not review "53 pages" per day anyway.

iii. Misrepresentations to FINRA and Persistent Deficiencies in the Firm's Policies, Procedures, and Internal Controls

For much of the Relevant Time Period, Canaccord failed to timely or adequately remediate the deficiencies described above. In late 2020, as a regulatory examination began to focus on Canaccord's AML program, two compliance employees at Canaccord falsified records to give the false impression that they were completing reviews of trade surveillance reports when they were not. More specifically, in response to formal requests from FINRA regarding the Firm's review of particular trade surveillance reports, a Canaccord employee falsified nearly 400 documents to create the false impression that they were performing their assigned reviews. A second employee likewise (i) falsified records to indicate that they or their colleagues had reviewed certain reports that, as the

[25] This report did not include contextual information that would help the reviewer to assess the context of the price movement (*e.g.*, comparisons to historical baselines, market-wide developments).

employee was aware, had not been reviewed; and (ii) backdated versions of certain Firm policies and procedures to suggest they were implemented earlier than they were. [26]

As the extent of the AML compliance issues described above was revealed through FINRA's supervisory process, the Firm implemented some enhancements but still failed to address certain continuing issues in its AML compliance program, as well as issues relating to the specific reports described above. A report drafted by a third party that Canaccord voluntarily engaged to assess its AML program as of November 2023 (the Third-Party Report) found, for example, that Canaccord still lacked: (i) written guidance or procedures for trade surveillance or transaction monitoring; (ii) specific requirements regarding reviews of potentially suspicious activity, investigation steps, and supporting documentation standards; and (iii) any quality assurance to ensure consistency and quality of investigations. Further, the Third-Party Report stated that Canaccord's documentation contained inconsistent and vague requirements for completing and documenting automated and semi-automated reviews, instead relying heavily on the expertise of its trade surveillance staff to use discretion in their investigations.

The Third-Party Report also found issues with the design and review of certain trade surveillance reports, including that the two individuals charged with reviewing the Firm's Low-Priced and Low-Volume Reports documented their work inconsistently.

2. Inadequate Independent Testing

Through 2022, Canaccord did not conduct adequate independent testing to identify potential gaps in its controls related to suspicious activity monitoring. Although independent AML testing was conducted annually during the Relevant Time Period, the independent audit reports reflect an

[26] Canaccord subsequently terminated these employees after completing an investigation of the issue.

inadequate understanding of the risks presented by the relevant aspects of Canaccord's business. Moreover, the independent testing did not identify apparent gaps in the design and implementation of Canaccord's trade surveillance reports, including the issues described above regarding how several of these reports were utilized by Canaccord's compliance employees. Lastly, the independent testing failed to adequately test the remedial measures that Canaccord implemented, including in response to prior concerns that FINRA raised in its regular exams.

3. Failures Related to the Designated Individual Responsible for Implementing and Monitoring Canaccord's AML Program

Canaccord was required to designate an individual to be responsible for coordinating and monitoring the Firm's day-to-day compliance with the BSA—a "BSA Officer." Longstanding regulatory guidance has made clear that this requirement is central to the effective function of an AML program and that the mere act of appointing an individual to the role of BSA Officer is insufficient to assure and monitor compliance with the BSA;[27] thus, the existence of an individual with this title does not alone fulfill this requirement. Similarly, regulatory guidance also states that to have an effective AML program, a broker-dealer's board of directors must ensure that the designated BSA Officer has appropriate authority, independence, and access to resources to administer an adequate BSA compliance program.[28]

Throughout the Relevant Time Period, Canaccord and its BSA Officer failed to ensure that its compliance department had sufficient resources and competence to ensure compliance with the BSA. As described above, Canaccord's ability to monitor for suspicious activity hinged, in large part, on the effectiveness of its trade surveillance program, and in particular, on the review of daily or monthly

---

[27] *See* FINCEN, *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance, FIN-2014-A007* (Aug. 11, 2014).

[28] *See id*.

trade surveillance reports. Despite the importance of these reports to Canaccord's AML program, throughout the Relevant Time Period, the Firm's review process was hindered by (i) a lack of resources that caused critical reports to go unreviewed—and suspicious activity undetected—for extended periods of time; (ii) inexperienced and untrained employees; and (iii) oversight failures.

The resources Canaccord dedicated to its AML program—and in particular, its Trading Compliance Group—were inadequate to manage the risks the Firm's business model entailed. For much of the Relevant Time Period, the team responsible for reviewing Canaccord's full suite of reports consisted of just four employees, all of whom had additional responsibilities.

The Firm's resourcing issues were compounded by Canaccord's staffing of the Trading Compliance Group with employees who lacked the requisite knowledge, experience, and training to perform their duties. Although Canaccord designated a BSA Officer, beginning in 2017 and continuing in to the Relevant Time Period, the BSA Officer delegated authority for oversight of Canaccord's trade surveillance program to a newly hired Head of Trading Compliance who lacked prior AML experience and who did not receive training or guidance regarding his new role, other than sitting with a departing employee for a few days. The Head of Trading Compliance, in turn, tasked three employees with reviewing most of the reports that Canaccord used to monitor for suspicious trading activity, while retaining some of the reports for his own review. These line-level compliance employees also lacked prior AML experience. In addition, they were hired for job postings that did not list AML as part of their roles and responsibilities and did not receive appropriate training or guidance on how to perform the reviews.

Moreover, the BSA Officer and Head of Trading Compliance failed to oversee this aspect of the Firm's AML program by not confirming that the reviews were being completed or perform quality control reviews to ensure they were being completed effectively. Neither the BSA Officer nor Head

of Trading Compliance questioned why, over the course of several years, many of the trade surveillance reports—several of which were not, in fact, being reviewed—had never led to a single escalation of potentially suspicious activity.

4. Training

For much of the Relevant Time Period, Canaccord's management failed to properly ensure that employees in the Firm's Trading Compliance Group—including the Head of Trading Compliance—received appropriate, tailored training, particularly regarding the review of trade surveillance reports. Canaccord had ***no*** formal AML compliance training in place prior to November 2021. Front-line compliance employees lacking prior AML experience were not trained, for example, on how to identify red flags (including how they might appear on a trade surveillance report and require further investigation) or the AML risks inherent to Canaccord's business. These employees were left to exercise considerable judgment in determining (i) how and what to review in each report and (ii) whether any of the reviewed activity should be further investigated or escalated as potentially suspicious.

During this period, instead of AML compliance training, the Firm opted for an approach that resulted in compliance employees teaching themselves—without proper guidance or supervision—how to review a particular report. In the words of one former Canaccord compliance employee, this was "trial-by-fire." Similarly, Canaccord's Head of Trading Compliance—who as noted above, also lacked relevant AML experience—was only shown the reports he was now responsible for during a two-day period as part of two weeks when he overlapped with his predecessor.

Canaccord later implemented some AML training, but the Third-Party Report stated that the trade surveillance team continued to "lack[] technical knowledge of the BSA/AML requirements to execute controls in line with regulatory expectations." This review also found that multiple

Canaccord employees failed to complete annual AML training as required with no apparent consequences to such individuals, and that Canaccord lacked any training tailored to address known issues with personnel completing review of alerts and investigations of potentially suspicious activity, accurately and consistently. Finally, Canaccord's AML training was not tailored to the risks that it faced, as the Firm failed to consider the findings of its AML risk assessment in designing or revising required training.

5. Customer Due Diligence

As part of its obligation to implement and maintain an effective AML program, Canaccord was required to maintain risk-based procedures to conduct ongoing customer due diligence. Canaccord failed to implement processes that fulfilled this aspect of its AML program.

To comply with this regulatory requirement, a financial institution's CDD processes must, among other things, allow it to: (i) understand the nature and purpose of the customer relationship for the purpose of developing a customer risk profile, (ii) conduct ongoing monitoring of the accounts to identify and report suspicious transactions, and (iii) on a risk basis, maintain and update customer information (including beneficial ownership information of legal entity customers).[29] Appropriate CDD at onboarding also aims to, among other things, assess the applicant's risk profile and to consider any red flags the applicant might present.[30] In constructing the risk profile of a customer, CDD may involve, among other things, understanding the customer's source of wealth and source of funds, as well as certain related-party and counterparty relationships.

---

[29] 31 C.F.R. § 1023.210(b)(5).

[30] Red flags commonly observed at onboarding include, among other things, inconsistent identification details, complex ownership structures, and reluctance to provide necessary information. *See,* FINRA, *Notice to Members 19-18* (May 6, 2019); *see also*, FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (FFIEC), *BSA/AML Manual, Appendix F: Money Laundering and Terrorist Financing "Red Flags";* SEC, *Risk Alert – Division of Examinations, Observations from Anti-Money Laundering Compliance Examinations of Broker-Dealers* (July 31, 2023).

Canaccord's CDD processes failed to accomplish these objectives. The Firm's written procedures only set forth a requirement to collect documents (including, for example, completion of a new account form) without requiring further evaluation of those documents. The Firm failed to establish processes to achieve its CDD obligations or to provide staff with guidance or standards for conducting CDD.

Appropriately risk-based CDD processes involve collecting more customer information for those customers that have a higher risk profile.[31] Examples of CDD for higher-risk customers include more extensive background checks, verifying the source of the customer's funds (rather than simply requesting the customer describe it), and enhanced ongoing monitoring.[32] In determining when such measures are required, risk profiles and assessments might take into account the customer's identity, location, type of business, and the expected activity for the account.[33] Customer risk profiles are

---

[31] *See, e.g.*, FINCEN, *Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions, FIN-2020-G002* (Aug. 3, 2020), (explaining that, where a financial institution assesses that a customer presents a "higher risk" profile, it may "collect more information to better understand the customer relationship"); FINCEN, *Guidance on Obtaining and Retaining Beneficial Ownership Information*, FIN-2010-G001 (Mar. 5, 2010) ("With respect to accounts that have been identified by an institution's CDD procedures as posing a heightened risk, these accounts should be subjected to (EDD) that is reasonably designed to enable compliance with the requirements of the BSA. This may include steps, in accordance with the level of risk presented, to identify and verify beneficial owners, to reasonably understand the sources and uses of funds in the account, and to reasonably understand the relationship between the customer and the beneficial owner."). *See also* FFIEC, *BSA/AML Manual, Customer Due Diligence- Overview* ("Collecting additional information about customers that pose heightened risk, referred to as enhanced due diligence (EDD), for example, in the private and foreign correspondent banking context, is part of an effective due diligence program.").

[32] *See, e.g.*, FINCEN, *Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions, FIN-2020-G002* (Aug. 3, 2020), (heightened risk can be mitigated by, among other things, enhanced monitoring and collecting information regarding expected account activity); *see also* FFIEC, *BSA/AML Manual, Customer Due Diligence- Overview* (listing additional information that can be collected as part of EDD).

[33] *See* FINCEN, *Guidance: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions, FIN-2018-G001* (Apr. 3, 2018) at 22–23 ("Understanding the nature and purpose of a customer relationship—the information gathered about a customer at account opening—is essential to developing a customer risk profile. This information should be used to develop a baseline against which customer activity, such as the customer's expected use of wires or typical number of deposits in a month, can be assessed for possible suspicious activity reporting. If account activity changes, particularly with regard to what should be anticipated based on the original nature and purpose of the account, risk-based monitoring may identify a need to update customer information, including, as appropriate, beneficial ownership."); FINCEN, *Final Rule, Customer Due Diligence Requirements for Financial Institutions,* 81 Fed.

often critical aspects of a broker-dealer's AML program, including because they determine the required level of due diligence. As detailed in the examples set forth below, Canaccord failed to meaningfully account for the presence of higher risk customers in its customer base.

Finally, beyond onboarding, broker-dealers must also conduct appropriate, risk-based Ongoing Due Diligence (ODD) to maintain and update customer information, and conduct ongoing monitoring to identify and report suspicious transactions.[34] Until December 2022, Canaccord did not maintain ***any*** process to require consistent updates to CDD and customer risk profiles, with any such updates to CDD and customer risk profiles occurring on a limited, *ad hoc* basis. As illustrated by the examples set forth below, this resulted in Canaccord failing to maintain and update customer information on a risk basis. Even though its policies now require such updates, this recent change has yet to be implemented for many of Canaccord's existing customers.

The following subsections provide further details regarding Canaccord's failures in conducting CDD at onboarding and on an ongoing basis, as well as examples of specific customer

---

Reg. 29398, 29422 *(*May 11, 2016) ("[W]e observed that under the existing requirement for financial institutions to report suspicious activity, they [securities broker-dealers] must file SARs on a transaction that, among other things, has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage. To understand the types of transactions in which a particular customer would normally be expected to engage necessarily requires an understanding of the nature and purpose of the customer relationship, which informs the baseline against which aberrant, suspicious transactions are identified." (internal citation omitted); *id.* ("And as FinCEN stated in the proposal, in some circumstances an understanding of the nature and purpose of a customer relationship can also be developed by inherent or self-evident information about the product or customer type, or basic information about the customer, and such information may be sufficient to understand the nature and purpose of the relationship. We further noted that, depending on the facts and circumstances, other relevant facts could include basic information about the customer, such as annual income, net worth, domicile, or principal occupation or business, as well as, in the case of longstanding customers, the customer's history of activity."). *See also* FFIEC, *BSA/AML Manual, Customer Due Diligence- Overview* ("As with the risk assessment, the bank may determine that some factors should be weighted more heavily than others. For example, certain products and services used by the customer, the type of customer's business, or the geographic location where the customer does business, may pose a higher risk of money laundering or terrorist financing. Also, actual or anticipated activity in a customer's account can be a key factor in determining the customer risk profile.").

[34] 31 C.F.R. § 1023.210(b)(5)(ii).

relationships that posed heightened AML risk but were not identified or monitored as such, as a direct result of Canaccord's CDD-related failures.

a. Canaccord's Deficient Onboarding CDD Processes

Canaccord did not implement reasonable processes that would allow it to conduct risk-based due diligence upon onboarding its customers. During the Relevant Time Period, the Firm applied the same, basic diligence for ***all*** customers without consideration of the risk the customer posed. Canaccord also did not consistently include information regarding beneficial owners as part of its CDD process and, in many instances, failed to resolve inconsistencies in customer-supplied information.[35] As a result, Canaccord's CDD onboarding processes were inconsistent with the risk-based approach set forth in the relevant pillar of the AML program rule and a violation of the BSA and FinCEN's implementing regulations.

Until late 2023, Canaccord risk rated account types, rather than individual customers. As a result, Canaccord lacked a process to perform individualized, differentiated CDD, meaning that higher-risk applicants were subject to the same level of CDD as lower-risk customer applicants. Similarly, Canaccord lacked processes to reasonably address red flags that could arise during the onboarding process. As illustrated in the examples below, Canaccord personnel made no effort to resolve or even explain inconsistencies in customer-provided information. In the case of legal entity applicants, Canaccord failed to consistently verify information regarding beneficial owners, despite the requirement to do so as part of CDD. Canaccord's policies did not define control persons (for purposes of determining beneficial ownership), much less set forth procedures to identify beneficial

[35] The applicability date for FinCEN's CDD rule was May 11, 2018. *See* 81 Fed. Reg. 29,398 FINCEN *Customer Due Diligence Requirements for Financial Institutions* (May 11, 2016).

owners, including control persons. In March 2023, Canaccord began consistently conducting documentary verification of beneficial owners and control persons.

These onboarding CDD failures were apparent for a foreign financial institution customer whose ownership was fully held through bearer shares, a practice regulators have long identified as posing elevated AML risks.[36] The customer provided information at onboarding that identified its "100% ownership in bearer shares," but personnel involved in the onboarding process were unaware of this indication of elevated risk and did not conduct additional due diligence to assess or mitigate this elevated risk.

b. Canaccord's Lack of Ongoing CDD Processes

As of at least November 2023, Canaccord had not implemented a process to consistently update customers' due diligence files after the customer's initial onboarding. Although the Firm subsequently began taking steps to address this failing, Canaccord's revised process, which required updating CDD files every three years regardless of the customer's risk profile, had not been retroactively applied to existing customers. As a result, even under the revised process, existing Canaccord customers, including high-risk customers, would continue to have outdated customer risk profiles for several years.

Even where Canaccord's written AML compliance procedures historically provided for ODD, the Firm frequently failed to implement ODD requirements through established processes. For

[36] As of 2021, the United States prohibits legal entities formed under State law from issuing bearer shares. 31 U.S.C. § 5336(f). Companies that use "bearer share" structures do not maintain records of their beneficial owners; rather, ownership is based on physical possession of the stock certificates. Regulatory guidance has long identified the risks associated with customers that use this ownership structure, and financial institutions have been encouraged to apply CDD processes that pay "particular attention" to this type of ownership structure, including having the financial institution itself maintain the bearer share for the customer as a way to mitigate this elevated risk. FFIEC, *BSA/AML Manual, Business Entities (Domestic and Foreign) – Overview* ("Particular attention should be paid to articles of association that allow for nominee shareholders, board members, and bearer shares.").

example, Canaccord's AML program required that diligence relating to a particular customer be updated when certain triggering events, including a change in settlors, beneficiaries, or authorized representatives, occurred—but the Firm had no documented process to notify the relevant team responsible for performing CDD when such a trigger event took place. Although Canaccord conducted monthly reviews of its foreign accounts' transactions to detect potential anomalies, it nonetheless failed to update customer risk profiles when anomalies were identified. Similarly, Canaccord did not update customer risk profiles after customers appeared on an exception report or triggered an alert. Nor did the Firm require staff investigating alerts to search for prior alerts or investigations involving the same customer.

As detailed above, Canaccord's processes for identifying suspicious activity remained deficient throughout the Relevant Time Period and implicated CDD obligations.

c. CDD Failures Involving Specific Customers

FinCEN identified multiple instances of Canaccord failing to conduct appropriate, risk-based CDD for its customers, including the examples discussed below:

i. Customer A and its Beneficial Owner, Individual 1

Customer A is a Cayman Islands-domiciled partnership with a business described in Canaccord's CDD as "investments, sales, and trading" that opened an account with Canaccord in November 2017. As described below, despite red flags that were apparent during the life of the account over the next approximately three-and-a-half years (including within the Relevant Time Period), Canaccord's CDD on Customer A was subject to only limited and *ad hoc* updates to customer

information that were not conducted on a risk basis, and Canaccord also failed to properly conduct ongoing monitoring of this account until at least July 2020.[37]

Canaccord failed to conduct adequate ODD on Customer A for several years after the account was opened to update Customer A's information on a risk basis and properly conduct ongoing monitoring of this account. The ODD for Customer A that Canaccord collected consisted of one additional industry template for an AML questionnaire dated two years after the template collected during Customer A's initial 2017 onboarding and annual, one-page certifications that Customer A maintained an AML program. However, Canaccord did not investigate the indicia of elevated risk posed by Customer A, including the fact that Customer A's onboarding documentation listed its assets under management as $28 million, but this figure unexpectedly rose by over 1500% to "greater than $500 million" in an AML questionnaire provided roughly two years later.

In July 2020, Canaccord received a law enforcement request that prompted it to perform additional due diligence on Customer A and its owner, Individual 1. This additional due diligence identified media reports published the prior year alleging that Individual 1 was purportedly implicated in investigations involving a Venezuelan individual designated by the Office of Foreign Assets Control (OFAC). Canaccord filed a SAR, and, in a contemporaneous internal memorandum, compliance personnel initially recommended closing the account. Instead, Canaccord ultimately kept open Customer A's account but indicated that its account would be subject to "heightened supervision."[38]

---

[37] During onboarding, Canaccord conducted minimal CDD on Customer A, and there is no record that the Firm conducted due diligence regarding Customer A's beneficial owner, Individual 1. For example, Canaccord's onboarding CDD described Customer A's source of funds merely as "client funds."

[38] Canaccord's record of the decision to maintain Customer A's account stated that the "heightened supervision" would consist of reviews of: (i) Customer A's transactions, (ii) email correspondence with Customer A, and (iii) negative news

Customer A's account was closed in 2021, only after the clearing firm that Canaccord relied on to settle its customers' transactions refused to clear transactions related to Customer A's accounts due to the media reports described above.[39]

ii. Customer B and its Beneficial Owner, Individual 2

In 2017, Canaccord opened an account for Customer B, a Cyprus-based investment firm owned by Individual 2 and his two children. As described below, despite red flags that were apparent during the life of the account (including within the Relevant Time Period), Customer B's account remained open throughout the Relevant Time Period, with only limited and *ad hoc* updates to customer information that were not conducted on a risk basis, and Canaccord also failed to conduct adequate ongoing monitoring of this account.

For example, the records of the due diligence that Canaccord performed included updated financial statements, which indicated substantial changes in Customer B's operations (such as Customer B's total assets growing by over 400% in a three-year period); Canaccord's CDD files for Customer B do not reflect that Canaccord considered such information as part of Customer B's risk profile.

In 2023, a series of articles detailed Individual 2's years-long efforts to shield wealthy Russians' assets through an affiliate of Customer B that is also based in Cyprus. Canaccord's CDD

---

related to Customer A. The record of decision, which was an internal memorandum, also stated that the memorandum would be updated to reflect the completion of the reviews and any action taken. The Firm maintained high-level records relating to its reviews of its email correspondence with Customer A. In connection with the closing of Customer A's account in 2021, the internal memorandum was updated to include a list of bullets regarding the dates and findings of the email and negative news reviews. The updated memorandum does not contain any reference to the Firm having conducted reviews of Customer A's transactions.

[39] Canaccord filed a second SAR contemporaneous with the closure of its accounts for Customer A in 2021.

files for Customer B do not reflect that the Firm considered the impact of this information on Customer B's risk profile and failed to assign a higher customer risk rating or to conduct EDD.[40]

Canaccord also failed to conduct adequate ODD after the United Kingdom added Individual 2 and an affiliate of Customer B to its sanctions list in April 2023. As a result, Canaccord failed to identify this and the underlying reporting that Individual 2 helped Russian oligarchs move money out of Russia.

iii. Customer C and its Beneficial Owner, Individual 3

In 2019, Canaccord opened an account for Customer C, an "asset management" firm organized as a Wyoming LLC that was beneficially owned by Individual 3. Individual 3 was subsequently fined and barred from the penny stock industry by the SEC for his role in several microcap fraud schemes that occurred during the time Customer C's account was open at Canaccord. As detailed in the section that follows on SAR violations, Canaccord facilitated much of the trading for these schemes, including some through the Customer C account.

Canaccord's clearing firm first raised concerns over the trading activity in Customer C's account in early 2020—at least some of which related to Customer C's trading that was later the subject of SEC allegations of manipulative trading—and Canaccord initially decided to close the

---

[40] In particular, Canaccord's CDD records for Customer B do not reflect reporting alleging that Individual 2 aided certain oligarchs in hiding their assets, including Konstantin Malofeyev. In December 2014, OFAC designated Malofeyev as a Specially Designated National (SDN). In sanctioning Malofeyev, OFAC described him as "one of the main sources of financing for Russians promoting separatism in Crimea" and, through its designation, prohibited U.S. citizens from working for or doing business with Malofeyev. OFAC, *Press Release, Treasury Targets Additional Ukrainian Separatists and Russian Individuals and Entities* (Dec. 19, 2014). On April 20, 2022, Malofeyev was sanctioned again for acting, or purporting to act, on behalf of, directly or indirectly, the Government of Russia. OFAC, *Press Release, U.S. Treasury Designates Facilitators of Russian Sanctions Evasion* (Apr. 20, 2022).

Additionally, publicly available information pre-dating this 2023 reporting linked Individual 2's business to Russian oligarchs; as early as 2012, Individual 2 was linked to an oligarch's Cypriot trust. References to this information remained absent from Canaccord's CDD files in the roughly five-year period between account opening and the third quarter of 2022.

account in June 2020. Canaccord subsequently reversed course, however, and allowed the account to remain open while Canaccord purported to respond to this information regarding Customer C's risk through monitoring the customer's concentration in low-priced securities trading activity. However, this form of ongoing monitoring proved to be ineffective: throughout the life of Customer C's account, its trading in low-price securities never dropped below 100%, despite Canaccord's request that Customer C diversify its trading activity by trading securities other than low-priced stocks. Notwithstanding the purported application of enhanced monitoring, from June through October 2020 when Canaccord's clearing firm decided it would no longer clear Customer C's transactions, Customer C engaged in manipulative activity that was later charged by the SEC.

F. Violation of the Requirement for Due Diligence on Correspondent Accounts for Foreign Financial Institutions

Foreign correspondent accounts are gateways to the U.S. financial system that can present heightened AML/CTF risks depending on the unique facts and circumstances of the account.[41] In some instances, Canaccord operated foreign financial institution correspondent accounts without confirming that the customer information satisfied regulatory requirements. Personnel responsible for onboarding customers did not consistently require or request critical information—such as the nature of the foreign financial institution's business and the markets it serves—to properly mitigate the risks associated with such accounts. Canaccord similarly failed to implement a procedure for conducting ongoing periodic reviews of correspondent account activity to determine whether activity was consistent with the type and purpose of the account, as well as the anticipated account activity.

---

[41] *See* 31 C.F.R. 1010.610.

For example, in 2017, a Bahamas-based foreign bank, Customer D, opened a correspondent account at Canaccord. Despite the elevated risk presented by this foreign financial institution,[42] Canaccord conducted diligence that did not comply with applicable requirements. Canaccord did conduct a search against the OFAC SDN list.

In February 2021, Canaccord's Trading Compliance Group raised concerns over Customer D's trading activity, leading the Firm's BSA Officer to determine that Customer D should be subject to "heightened supervision." Notwithstanding that determination, the Firm failed to conduct EDD or take steps to mitigate the increased risk presented by the customer.

Canaccord later received information requests regarding Customer D from both law enforcement and another financial institution indicating that Customer D was associated with suspicious transactions. Nonetheless, the Firm still failed to conduct additional due diligence or EDD on Customer D.

G. Violation of the Requirement to Report Suspicious Activity and Transactions

Canaccord's willful failure to implement controls resulted in Canaccord being used by illicit actors engaged in securities fraud, and Canaccord failing to report suspicious activity—despite readily apparent red flags and certain escalations raised by its own clearing firm over the activity. Based on preliminary results from a SAR Lookback, Canaccord failed to file at least 160 SARs relating to dozens of different OTC securities, the trading of which involved a high volume of underlying suspicious transactions that FinCEN estimates to be in the thousands.[43]

---

[42] *See, e.g.*, FATF, *Mutual Evaluation Report on the Bahamas* (July 2017) (flagging, among other things, vulnerabilities to "financial flows associated with foreign threats, including tax evasion").

[43] Canaccord has subsequently filed SARs with FinCEN on certain of the suspicious activity described in the examples below, including in connection with the SAR Lookback.

1. Oncology Pharma, Inc.

Canaccord failed to report a significant volume of suspicious transactions in Oncology Pharma, Inc.'s common stock between January and August 2021. The transactions had an aggregate value of nearly $100 million. As described in public filings and other open-source information, Oncology Pharma, Inc. was a Nevada corporation that described its business as the licensing, development, manufacturing, and commercialization of therapeutic drugs and medical devices designed to treat many types of cancers. Oncology Pharma, Inc.'s common stock traded on the OTC market under the symbol ONPH.

In March 2023, stock promoters Joseph A. Padilla and Kevin C. Dills were indicted on federal fraud charges for allegedly orchestrating a pump-and-dump penny stock scheme involving ONPH that generated over $150 million in illicit proceeds.[44] Separately, in June 2023, the SEC charged Padilla and Dills for their roles in carrying out a fraudulent stock scheme involving ONPH.

Both of these cases brought in 2023 revealed that during the period when Canaccord was trading ONPH, Padilla and Dills participated in a market manipulation scheme involving ONPH. Based on these cases, the scheme proceeded as follows: first, Padilla and Dills caused nearly all of ONPH's free-trading shares to be transferred to multiple brokerage accounts for the benefit of Padilla's clients at a Cayman Islands broker; second, beginning in January 2021, Padilla then engaged in manipulative trading to artificially drive up the price of ONPH; and finally, Padilla then began

[44] Padilla subsequently pleaded guilty to securities fraud and other charges; Dills pleaded guilty to securities fraud. The SEC found that Padilla manipulated stock prices through trading activities in his own account and accounts belonging to family and friends that he controlled during periods of heightened investor demand driven by promotional activities such as email newsletters and online articles. The SEC's cases against Padilla and Dills were resolved through judgments imposing disgorgement totaling over $1 million and, in the case of Dills, a civil penalty of over $200,000.

selling the ONPH shares (which were then trading at inflated prices due to Padilla's manipulative activity) to unsuspecting victims.

Despite its role as a market maker buying and selling millions of shares of ONPH, Canaccord failed to detect the following red flags of suspicious activity related to ONPH, including red flags related to manipulative trading.[45]

First, ONPH had the appearance of a shell company. Publicly available information reflects that the issuer's name and business description changed abruptly in 2019, it had no operational history or revenue, and the audit report contained a going concern audit opinion reflecting doubt as to whether the company could continue operating.

Second, publicly available information reflects that ONPH's stock price increased by more than 250% during the month of January 2021 and again by more than 400% during February. Monthly trading volume increased four-fold from January to February 2021 and continued to grow through June. The stock price peaked at $50 on March 1, 2021, up from a low of $0.42 less than two months earlier on January 8, 2021.

---

[45] *See* FINRA, *Notice to Members 19-18* (May 6, 2019)(identifying "Potential Red Flags in Securities Trading," to include "a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security"); FINRA, *Notice to Members 21-03* (Feb. 10, 2021)(identifying "Potential Red Flags of Fraud Involving Low-Priced Securities," to include issuers that are or were "currently or previously a shell company," and "a spike in social media promotions (*e.g.*, on Twitter, Instagram or Facebook), and activity on investor chat rooms or message boards."); SEC, *Risk Alert: Compliance Issues Related to Suspicious Activity Monitoring and Reporting at Broker-Dealers* (March 29, 2021) at 4–5 (incorporating by reference a 2014 SEC Risk Alert and observing that some broker-dealers did not review activity and follow up to consider filing a SAR when certain red flags set forth in the prior 2014 Risk Alert were present, including "[t]rading in thinly traded, low-priced securities that resulted in sudden spikes in price or that represented most, if not all, of the securities' daily trading volumes" and "[t]rading in the stock of issuers that were shell companies.")

No single red flag is determinative of illicit or suspicious activity. Financial institutions consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is suspicious.

Finally, publicly available information reflects that ONPH was the subject of Internet discussions throughout the spring and summer of 2021 indicative of fraudulent promotional activity.

Canaccord failed to investigate these red flags and failed to timely file a SAR regarding this activity.

2. Blue Eagle Lithium, Inc.

Canaccord failed to report a significant volume of suspicious transactions in Blue Eagle Lithium, Inc.'s common stock between January and August 2019. The transactions had an aggregate value of several million dollars.

As described in public filings and other open-source information, Blue Eagle Lithium, Inc., a Nevada corporation, purported to be in the business of lithium and rare earth metal resources. Initially, the company did business under the name Wishbone Pet Products Inc. and had a pet-related business model. As reflected in a contemporaneous public filing, in July 2018, the company changed its name to reflect its purported shift from pet products to rare earth metal resources. Simultaneously, publicly available documents reflect that the issuer conducted a 20-for-1 share split in its common stock—thereby greatly increasing the number of shares outstanding—which traded on the OTC market as BEAG.

Roughly a year later, the SEC issued a two-week trading suspension in the securities of BEAG. In suspending trading, the SEC cited questions regarding (i) the accuracy and adequacy of publicly available information about BEAG and (ii) unusual and unexplained market activity in BEAG common stock. After the temporary suspension terminated, Canaccord resumed trading in BEAG and did not appear to review its own activity in the stock or increase its monitoring of transactions in the stock.

Over two years later, on April l4, 2022, the SEC filed a Complaint against eight individuals alleging a long-running scheme to manipulate the trading of at least seventeen microcap stocks, including BEAG. The SEC complaint alleged the manipulation of BEAG as a pump and dump scheme, through which the conspirators sold roughly five million BEAG shares to generate illicit proceeds totaling over $5 million. The U.S. Attorney's Office for the Southern District of New York issued a series of indictments in a parallel action.[46] Based on these cases, the alleged scheme proceeded as follows: first, the conspirators acquired a controlling interest in the penny stock; second, they concealed their collective control of the security; third, they funded misleading promotional campaigns designed to increase investor interest and demand; and finally, they exploited the buy-side demand they had created by dumping their shares on unsuspecting retail investors.

Canaccord failed to file any SARs concerning BEAG during the Relevant Time Period or after the indictments. Canaccord also failed to appropriately investigate and act upon the following red flags, including:[47]

First, BEAG had the appearance of a shell company, including its change in name and significant revision to its business description. Similarly, publicly available information reflects that

---

[46] One defendant subsequently pleaded guilty to conspiracy to commit securities fraud and was sentenced to twenty months imprisonment and forfeiture of over $4 million.

[47] *See,* FINRA, *Notice to Members 19-18* (May 6, 2019) (identifying "Potential Red Flags in Securities Trading," to include "a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security"); FINRA, *Notice to Members 21-03* (Feb. 10, 2021) (identifying "Potential Red Flags of Fraud Involving Low-Priced Securities," to include issuers that are or were "currently or previously a shell company," and "a spike in social media promotions (*e.g.*, on Twitter, Instagram or Facebook), and activity on investor chat rooms or message boards."); SEC, *Risk Alert: Compliance Issues Related to Suspicious Activity Monitoring and Reporting at Broker-Dealers* (March 29, 2021) at 4–5 (incorporating by reference a 2014 SEC Risk Alert and observing that some broker-dealers did not review activity and follow up to consider filing a SAR when certain red flags set forth in the prior 2014 Risk Alert were present, including "[t]rading in thinly traded, low-priced securities that resulted in sudden spikes in price or that represented most, if not all, of the securities' daily trading volumes" and "[t]rading in the stock of issuers that were shell companies or had been subject to trading suspensions or whose affiliates, officers, or other insiders had a history of securities law violations.")

the company lacked operational history and revenues and had publicly disclosed a going concern audit opinion.[48]

Second, publicly available information reflects that BEAG's stock price rose sharply throughout the relevant period, increasing 65% throughout January 2019. By June, the price had more than doubled from the initial January price of $0.66, peaking at $1.41 in June. Further, Canaccord's own trading of BEAG substantially increased in June: the Firm's monthly volume rose 1,000% over the BEAG volume that Canaccord had traded in May.

Third, publicly available information reflects that throughout this period of price and volume spikes, BEAG was the subject of Internet discussions indicative of fraudulent promotional activity.

Fourth, the SEC suspended trading in the securities of BEAG. The SEC's notice to the public regarding the suspension raised questions regarding "online promotional materials regarding analyst findings and the extent of the company's mining claims" and "recent unusual unexplained market activity."[49] Canaccord conducted no review of the potentially suspicious underlying trading activity and resumed trading in BEAG after the suspension expired.

Finally, a Canaccord employee recommended that the Firm report suspicious activity involving BEAG. In August 2019, less than one month after the suspension of trading in BEAG securities expired, Canaccord's Head of Trading Compliance noted that "[b]ased on the conclusion

---

[48] *See* Blue Eagle Lithium Inc. Form 10-K, at 7 ("Accordingly, you should consider our prospects in light of the costs, uncertainties, delays and difficulties frequently encountered by companies in their pre-revenue generating stages, particularly those in the exploration and mining of lithium. Potential investors should carefully consider the risks and uncertainties that a new company with no operating history will face.") and 10 ("There is significant doubt regarding our ability to continue as a going concern. If we do not continue as a going concern, investors could lose their entire investment."). Similarly, Blue Eagle's predecessor Wishbone Pet Products Inc. was a non-operating business. *See* Form 10Q filed on September 23, 2016 at 9 ("We are considered to be a 'shell company' . . . with either no or nominal operations or assets, or assets consisting solely of cash and cash equivalents.").

[49] *See SEC, Securities Exchange Act of 1934 Release No. 86271* (July 1, 2019); SEC, *In the Matter of Blue Eagle Lithium, Inc. (File No. 500-1), Order of Suspension of Trading* (July 1, 2019).

of the June Pump and Dump [report], I would recommend filing in BEAG based on the news headline pertaining to potential market manipulation." Despite this recommendation, and notwithstanding the significant red flags presented by BEAG and its trading activity, in the Relevant Time Period, Canaccord never filed a SAR on suspicious transactions involving BEAG or otherwise applied controls to its trading in this high-risk security.

3. Customer C and its Beneficial Owner, Individual 3

In 2019, Canaccord opened an account for Customer C, an "asset management" firm organized as a Wyoming LLC that was beneficially owned by Individual 3. As noted above, Individual 3 was subsequently fined—the civil penalty and disgorgement applicable to Individual 3 exceeded $5 million—and barred from the penny stock industry by the SEC for his role in several microcap fraud schemes that occurred during the time his account was open at Canaccord. More specifically, the SEC's action explains that Individual 3 paid stock promoters to tout the stock of three microcap companies that he controlled. Then, along with associates, Individual 3 convinced investors through false and misleading representations to invest in the stocks. As described below, while Canaccord was well-positioned to identify the red flags associated with this activity,[50] a meaningful amount of these microcap stocks trades flowed through Canaccord, including:

---

[50] *See,* FINRA, *Notice to Members 19-18* (May 6, 2019) (identifying "Potential Red Flags in Securities Trading," to include "a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security"); FINRA, *Notice to Members 21-03* (Feb. 10, 2021)(identifying "Potential Red Flags of Fraud Involving Low-Priced Securities," to include issuers that are or were "currently or previously a shell company," and "a spike in social media promotions (*e.g.*, on Twitter, Instagram or Facebook), and activity on investor chat rooms or message boards."); SEC, *Risk Alert: Compliance Issues Related to Suspicious Activity Monitoring and Reporting at Broker-Dealers* (March 29, 2021) at (incorporating by reference a 2014 SEC Risk Alert and observing that some broker-dealers did not review activity and follow up to consider filing a SAR when certain red flags set forth in the prior 2014 Risk Alert were present, including "[t]rading in thinly traded, low-priced securities that resulted in sudden spikes in price or that represented most, if not all, of the securities' daily trading volumes" and "[t]rading in the stock of issuers that were shell companies or had been subject to trading suspensions or whose affiliates, officers, or other insiders had a history of securities law violations.")

Odyssey Group International, Inc. As described in public filings and other open-source information, Odyssey Group International (ODYY) was incorporated in 2014 and described its business as "surgical & medical instruments & apparatus" and the "development and acquisition of medical products and health related technologies." In the roughly two-and-a-half years prior to the conduct perpetrated by Individual 3, publicly available information reflects that ODYY traded sparingly: it had reported volume on only 25 days and the average volume of shares traded was roughly 350 per day. That changed in the summer of 2019, when, as explained in the SEC's subsequent action, Individual 3 acquired 98% of the shares of ODYY for $100,000.

As explained in the SEC's action, at the start of 2020, Individual 3 and his co-conspirators hired telemarketers to promote ODYY to potential investors using deceptive and high-pressure sales tactics. The SEC's action further explains that Individual 3 later hired a company to conduct a digital promotion campaign of ODYY, resulting in dozens of electronic promotions of ODYY; as these promotions began, Individual 3 started selling his shares, selling more than 20,000 shares in a single day after a promotional email was sent to investors—this volume represented a more than 5,000% increase of ODYY's trading volume prior to Individual 3 obtaining control of the security's public float. The SEC's action explains that, ultimately, Individual 3 generated more than $2.5 million in illicit proceeds from selling shares of ODYY. By the time Individual 3 completed his scheme, the price of ODYY collapsed by more than 80% from its peak during the promotional period.

As an active market participant in ODYY's trading throughout the duration of Customer C's market manipulation scheme, Canaccord was privy to red flags related to the trading in ODYY but failed to reasonably investigate them and failed to file any SAR concerning ODYY with FinCEN.

CannaPharmaRx, Inc. As described in public filings and other open-source information, CannaPharmaRx (CPMD), described itself as "an early stage pharmaceutical company whose purpose

was to advance cannabinoid research and discovery using proprietary formulation and drug delivery technology that was in development." As explained in the SEC's subsequent action, in the spring of 2020—after the scheme involving ODYY was well underway—Individual 3 acquired roughly 3 million shares, or 80% of public float of CPMD, by paying $50,000 to a third party affiliated with CPMD's CEO. Together with a co-conspirator, Individual 3 arranged a digital promotion campaign consisting of a series of deceptive emails to potential investors and an Internet "landing page" to promote CPMD to investors.

In the two-week period coinciding with the launch of the promotional campaign described in the SEC's action, the volume of trading in CPMD increased by more than 200%, and CPMD's share price increased by nearly 25%, compared to the preceding two weeks before the campaign began. For the first month of the promotional campaign described in the SEC's action, the volume of trading in CPMD increased by nearly 600%. As the SEC explained, this scheme ultimately netted Individual 3 and his co-conspirator more than $3 million.

Canaccord processed a significant volume of trades in CPMD during this time. Canaccord did not detect the fraud that Individual 3 and Customer C were perpetrating involving CPMD, although Canaccord did identify other potentially suspicious activity in CPMD and filed SARs in August 2020 and June 2021, respectively.

Scepter Holdings, Inc. As described in public filings and other open-source information, Scepter Holdings, Inc. (BRZL) managed "the sales and brand development of high-performance consumer packaged goods." As with ODYY and CPMD and explained in the SEC's subsequent action, Individual 3 and his co-conspirators manipulated the price of BRZL and generated illicit proceeds of about $3.2 million from sales of BRZL. Through Canaccord, Individual 3 executed more than 130 transactions in BRZL between February and September 2020—contemporaneous with the

period in which, as stated in the SEC's action, Individual 3 and his co-conspirators engaged in a promotional campaign—with an aggregate value of more than $1 million. During the first month of the promotional campaign described in the SEC's action, BRZL's price increased by more than 170% and its volume increased by nearly 900%, compared to the month before the campaign began. While Canaccord took some steps to investigate trading by Customer B in the securities of BRZL, it did not file a SAR.

Canaccord failed to report the suspicious activity in Customer C's account until it received a copy of the SEC's complaint, along with an emergency order to freeze Individual 3's account, almost a year after Canaccord closed Customer C's account based on concerns about his trading of low-priced securities. At that time, Canaccord filed a SAR concerning potentially suspicious activity in Customer C's account, including in the securities of the three issuers described above.

III. VIOLATIONS

FinCEN determined that Canaccord willfully violated the BSA and its implementing regulations during the Relevant Time Period. Specifically, FinCEN determined that Canaccord willfully failed to implement and maintain an AML program that met the minimum requirements of the BSA, in violation of 31 U.S.C. § 5318(h) and 31 C.F.R. § 1023.210. Additionally, FinCEN determined that Canaccord willfully failed to accurately and timely report suspicious transactions to FinCEN, in violation of 31 U.S.C. § 5318(g) and 31 C.F.R. § 1023.320. FinCEN determined that Canaccord also willfully failed to conduct due diligence on correspondent accounts in the United States for foreign financial institutions, in violation of 31 U.S.C. § 5318(i) and 31 C.F.R. § 1010.610.

IV. ENFORCEMENT FACTORS

As summarized below, FinCEN considered all factors outlined in the Statement on Enforcement of the Bank Secrecy Act issued August 18, 2020, when deciding whether to impose a civil money penalty in this matter.[51]

1. **Nature and seriousness of the violations, including extent of possible harm to the public and the amounts involved:** Canaccord's AML compliance failures, which included fundamental aspects of its compliance program, occurred over an extended period of time, and its failure to have an AML compliance program that appropriately took into account its high-risk lines of business resulted in trading through Canaccord involving numerous fraud schemes that ultimately caused significant economic harm to innocent investors. Canaccord's deficient CDD practices allowed high-risk customers with reported ties to illicit actors to obtain access to the U.S. financial system without appropriate controls or oversight. Canaccord was aware, including as a result of examinations conducted by FINRA, that its AML program needed significant reform, but failed to timely or adequately address the deficiencies during most of the Relevant Time Period. As a result of these issues, Canaccord failed to file SARs on a large volume of suspicious transactions with FinCEN: based on preliminary results from a SAR Lookback, Canaccord failed to file at least 160 SARs relating to dozens of different OTC securities, the trading of which involved a high volume of underlying suspicious transactions that FinCEN estimates to be in the thousands. This deprived law enforcement of timely and critical financial information pertaining to suspicious activity.

[51] FinCEN, "Financial Crimes Enforcement Network (FinCEN) Statement on Enforcement of the Bank Secrecy Act," (Aug. 18, 2020).

2. **Impact or harm of the violations on FinCEN's mission to safeguard the financial system from illicit use, combat money laundering, and promote national security:** Canaccord significantly impaired FinCEN's mission. Fraud is a significant AML/CFT concern for FinCEN, and Canaccord's willful failures to adopt and implement reasonable controls to prevent fraud allowed scammers to harm innocent investors. Similarly, Canaccord's facially deficient CDD practices enabled certain high-risk customers—including those with reported ties to illicit actors and a nexus to Russia and Venezuela—to trade in the U.S. financial markets. The gaps in Canaccord's controls allowed illicit actors to effect suspicious transactions through Canaccord, which Canaccord willfully failed to report to FinCEN.

3. **Pervasiveness of wrongdoing within an entity, including management's complicity in, condoning or enabling of, or knowledge of the conduct underlying the violations:** Through repeated regulatory examinations, Canaccord had ample notice of the deficiencies in its AML program but still failed to take meaningful steps to address them. Moreover, management knew that, due to a combination of a lack of resources and insufficient experience and training, AML staff were ill-equipped to mitigate the risks that Canaccord faced. When a regulator uncovered the substantial flaws in Canaccord's controls, Canaccord personnel altered records and provided false information in an attempt to cover up the violations. Senior AML Compliance employees also failed to meaningfully discharge their duties by not questioning for years that critical trade surveillance reports, which employees were not in fact reviewing, had not led to escalations or SAR filings.

4. **History of similar violations or misconduct in general, including prior criminal, civil, and regulatory enforcement actions:** Canaccord has no AML-related enforcement history. Canaccord, however, has been the subject of more than a dozen formal actions by regulatory

authorities since 2010, including for supervisory/oversight failures relating to, among other things, (i) position limits; (ii) trade reporting/recordkeeping; (iii) improper short-selling; (iv) collection/retention of issuer information; and (v) best execution.

5. **Financial gain or other benefit resulting from, or attributable to, the violations:** Canaccord's underinvestment in its AML program allowed it to avoid significant expenses that it otherwise would have incurred to manage the AML risks of a high-risk line of business for many years. Moreover, in the rare instances where customer activity was properly escalated, Canaccord consistently failed to take appropriate action.

6. **Presence or absence of prompt, effective action to terminate the violations upon discovery, including self-initiated remedial measures:** Although Canaccord implemented several remedial measures in response to issues identified during the course of this investigation—including enhancements to its trade surveillances, the initiation of a SAR lookback, increased compliance staffing, and considerable expenses associated with the retention of third-party consultants to oversee remediation—they were not prompt. FinCEN afforded such efforts less weight because Canaccord commenced many of them near the end of the Relevant Time Period (after years of non-compliance with supervisory findings), and, as of the date of this Consent Order, it is not yet clear if the enhancements (some of which are still being implemented) will be effective. However, FinCEN also considered that Canaccord continued to progress remediation even after entering into a definitive agreement to exit its OTC market making business.

7. **Timely and voluntary disclosure of the violations to FinCEN:** Canaccord did not voluntarily disclose the violations to FinCEN.

8. **Quality and extent of cooperation with FinCEN and other relevant agencies, including as to potential wrongdoing by its directors, officers, employees, agents, and counterparties:** Initially, Canaccord's cooperation with FinCEN's investigation was deficient, but it improved over the course of FinCEN's investigation. Although Canaccord provided several productions in response to FinCEN's requests, they were frequently subject to delays and organizational defects, thus hampering the efficiency of FinCEN's investigation. FinCEN also took into consideration false representations by Canaccord employees to another regulator at an earlier stage of the other regulator's parallel investigation. On the other hand, FinCEN took into consideration that Canaccord agreed to enter into multiple agreements tolling the statute of limitations and provided multiple presentations and written submissions concerning the historical facts of the matter and Canaccord's remediation efforts.

9. **Systemic Nature of the Violations. Considerations include, but are not limited to, the number and extent of violations, failure rates (e.g., the number of violations out of total number of transactions), and duration of violations:** As explained above, the violations that FinCEN identified were numerous, substantial in aggregate value, and occurred over an extended period of time. In particular, Canaccord's consistent failure to review critical trade surveillance reports, and its underinvestment in resourcing and training throughout the Relevant Time Period, allowed illicit activity to flow through Canaccord unreported for years.

10. **Whether another agency took enforcement action for related activity. FinCEN will consider the amount of any fine, penalty, forfeiture, and/or remedial action ordered:** Following separate but parallel investigations, Canaccord has agreed to pay $20 million to FINRA and $20 million to the SEC to resolve these investigations.

V. CIVIL PENALTY

FinCEN may impose a Civil Money Penalty of up $71,545 per day for willful violations of the requirement to implement and maintain an AML program.[52] For each willful violation of the SAR reporting requirement, FinCEN may impose a civil money penalty not to exceed the greater of the amount involved in the transaction (but capped at $286,184) or $71,545.[53] For each willful violation of the requirement to implement a risk-based due diligence program for correspondent accounts established, maintained, administered, or managed in the United States for foreign financial institutions, FinCEN may impose a civil money penalty "in an amount equal to not less than two (2) times the amount of the transaction," but not more than $1,776,364.[54]

After considering all the facts and circumstances, as well as the enforcement factors discussed above, FinCEN is imposing a Civil Money Penalty of $80 million in this matter. FinCEN has agreed to suspend $5 million of the Civil Money Penalty pending Canaccord's compliance with the Undertaking set forth below, and to credit against the Civil Money Penalty payments of $20 million to the SEC and $20 million to FINRA. Accordingly, Canaccord shall make payment of $35 million to the Department of the Treasury pursuant to the payment instructions that will be transmitted to Canaccord upon execution of this Consent Order.

---

[52] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

[53] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

[54] 31 U.S.C. § 5321(a)(7); 31 C.F.R. § 1010.821.

VI. UNDERTAKING

By execution of this Consent Order, Canaccord agrees to the following Undertaking:

SAR LOOKBACK UNDERTAKING

1. In connection with this resolution, Canaccord has engaged a qualified independent consultant (SAR Lookback Consultant) at its own expense to conduct a SAR Lookback Review. The SAR Lookback Consultant has been determining whether certain activity effected by Canaccord's customers during the Relevant Time Period, as agreed to between FinCEN and Canaccord, was properly identified and reported under 31 U.S.C. § 5318(g) and implementing regulations (Covered Transactions).

2. Upon completion of the SAR Lookback Review, and by no later than 180 days from the date of this Consent Order, Canaccord will deliver a detailed report (SAR Lookback Report) to FinCEN that summarizes the methodology and findings of its review and identifies the Covered Transactions that may require a SAR to be filed pursuant to 31 U.S.C. § 5318(g) and its implementing regulations. Canaccord will make, and will cause the SAR Lookback Consultant to make, interim reports, drafts, work papers, or other supporting materials related to the SAR Lookback Review available to FinCEN upon request. To the extent SARs have not already been filed, Canaccord will comply with the findings and recommendations of the SAR Lookback Consultant or FinCEN that Canaccord file SARs on any of the Covered Transactions

3. No later than 90 days from the date of the SAR Lookback Report, Canaccord will complete the filing with FinCEN of SARs regarding all of the Covered Transactions identified by the SAR Lookback Consultant or FinCEN as ones that would have required a report pursuant to 31 U.S.C. § 5318(g) and implementing regulations. Canaccord shall be entitled to one 60-day extension of this

SAR filing deadline as of right. Any additional extensions require the written consent of FinCEN in its sole discretion.

4. Within 30 days of the later of (i) submission to FinCEN of the SAR Lookback Report and (ii) Canaccord completing the filing with FinCEN of SARs regarding all of the Covered Transactions, FinCEN shall respond to Canaccord with a determination of whether Canaccord has complied with this Undertaking for purposes of the suspended penalty described in Section V.

VII. CONSENT AND ADMISSIONS

To resolve this matter and only for that purpose, Canaccord admits to the Statement of Facts and Violations set forth in this Consent Order and admits that it willfully violated the BSA and its implementing regulations. Canaccord consents to the use of the Statement of Facts, and any other findings, determinations, and conclusions of law set forth in this Consent Order in any other proceeding brought by or on behalf of FinCEN, or to which FinCEN is a party or claimant, and agrees they shall be taken as true and correct and be given preclusive effect without any further proof. Canaccord understands and agrees that in any administrative or judicial proceeding brought by or on behalf of FinCEN against it, including any proceeding to enforce the Civil Money Penalty imposed by this Consent Order or for any equitable remedies under the BSA, Canaccord shall be precluded from disputing any fact or contesting any determinations set forth in this Consent Order.

To resolve this matter, Canaccord agrees to and consents to the issuance of this Consent Order and all terms herein and agrees to make a payment of $35 million pursuant to the payment instructions that will be transmitted to Canaccord upon execution of this Consent Order. If timely payment is not made, Canaccord agrees that interest, penalties, and administrative costs will accrue.[55]

---

[55] 31 U.S.C. § 3717; 31 C.F.R. § 901.9.

Canaccord understands and agrees that it must treat the Civil Money Penalty paid under this Consent Order as a penalty paid to the government and may not claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any payments made to satisfy the Civil Money Penalty. Canaccord understands and agrees that any acceptance by or on behalf of FinCEN of any partial payment of the Civil Money Penalty obligation will not be deemed a waiver Canaccord's obligation to make further payments pursuant to this Consent Order, or a waiver of FinCEN's right to seek to compel payment of any amount assessed under the terms of this Consent Order, including any applicable interest, penalties, or other administrative costs.

Canaccord affirms that it agrees to and approves this Consent Order and all terms herein freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever have been made by FinCEN or any employee, agent, or representative of FinCEN to induce Canaccord to agree to or approve this Consent Order, except as specified in this Consent Order.

Canaccord understands and agrees that this Consent Order implements and embodies the entire agreement between Canaccord and FinCEN, and its terms relate only to this enforcement matter and any related proceeding and the facts and determinations contained herein. Canaccord further understands and agrees that there are no express or implied promises, representations, or agreements between Canaccord and FinCEN other than those expressly set forth or referred to in this Consent Order and that nothing in this Consent Order is binding on any other law enforcement or regulatory agency or any other governmental authority, whether foreign, Federal, State, or local.

Canaccord understands and agrees that nothing in this Consent Order may be construed as allowing Canaccord, its subsidiaries, affiliates, Board, officers, employees, or agents to violate any law, rule, or regulation.

Canaccord consents to the continued jurisdiction of the courts of the United States over it and waives any defense based on lack of personal jurisdiction or improper venue in any action to enforce the terms and conditions of this Consent Order or for any other purpose relevant to this enforcement action. Solely in connection with an action filed by or on behalf of FinCEN to enforce this Consent Order or for any other purpose relevant to this action, Canaccord authorizes and agrees to accept all service of process and filings through the Notification procedures below and to waive formal service of process.

VIII. COOPERATION

Canaccord shall fully cooperate with FinCEN in any and all matters within the scope of or related to the Statement of Facts, including any investigation of its current or former directors, officers, employees, agents, consultants, or any other party. Canaccord understands its cooperation pursuant to this paragraph shall include, but is not limited to, truthfully disclosing all factual information with respect to its activities, and those of its present and former directors, officers, employees, agents, and consultants. This obligation includes providing to FinCEN, upon request, any document, record, or other tangible evidence about which FinCEN may inquire of Canaccord. Canaccord's cooperation pursuant to this paragraph is subject to applicable laws and regulations, as well as valid and properly documented claims of attorney-client privilege or the attorney work product doctrine.

IX. RELEASE

Execution of this Consent Order and compliance with all of the terms of this Consent Order settles all claims FinCEN may have against Canaccord for the conduct described in this Consent Order during the Relevant Time Period. Execution of this Consent Order, and compliance with the terms of this Consent Order, does not release any claim FinCEN may have for conduct by Canaccord

other than the conduct described in this Consent Order during the Relevant Time Period, or any claim FinCEN may have against any current or former director, officer, owner, or employee of Canaccord or any other individual or entity other than those named in this Consent Order. In addition, this Consent Order does not release any claim or provide any other protection in any investigation, enforcement action, penalty assessment, or injunction relating to any conduct after the Relevant Time Period as described in this Consent Order.

X. WAIVERS

Nothing in this Consent Order shall preclude any proceedings brought by, or on behalf of, FinCEN to enforce the terms of this Consent Order, nor shall it constitute a waiver of any right, power, or authority of any other representative of the United States or agencies thereof, including but not limited to the Department of Justice.

In consenting to and approving this Consent Order, Canaccord stipulates to the terms of this Consent Order and waives:

A. Any and all defenses to this Consent Order, the Civil Money Penalty imposed by this Consent Order, and any action taken by or on behalf of FinCEN that can be waived, including any statute of limitations or other defense based on the passage of time;

B. Any and all claims that FinCEN lacks jurisdiction over all matters set forth in this Consent Order, lacks the authority to issue this Consent Order or to impose the Civil Money Penalty, or lacks authority for any other action or proceeding related to the matters set forth in this Consent Order;

C. Any and all claims that this Consent Order, any term of this Consent Order, the Civil Money Penalty, or compliance with this Consent Order, or the Civil Money Penalty, is in

any way unlawful or violates the Constitution of the United States of America or any provision thereof;

D. Any and all rights to judicial review, appeal or reconsideration, or to seek in any way to contest the validity of this Consent Order, any term of this Consent Order, or the Civil Money Penalty arising from this Consent Order;

E. Any and all claims that this Consent Order does not have full force and effect, or cannot be enforced in any proceeding, due to changed circumstances, including any change in law;

F. Any and all claims for fees, costs, or expenses related in any way to this enforcement matter, Consent Order, or any related administative action, whether arising under common law or under the terms of any statute, including, but not limited to, under the Equal Access to Justice Act. Canaccord agrees to bear its own costs and attorneys' fees.

XI. VIOLATIONS OF THIS CONSENT ORDER

Determination of whether Canaccord has failed to comply with this Consent Order, or any portion thereof, and whether to pursue any further action or relief against Canaccord shall be in FinCEN's sole discretion. If FinCEN determines, in its sole discretion, a failure to comply with this Consent Order, or any portion thereof, has occurred, or Canaccord has made any misrepresentations to FinCEN or any other government agency related to the underlying enforcement matter, FinCEN may void any and all releases or waivers contained in this Consent Order; reinstitute administrative proceedings; take any additional action it deems appropriate; and pursue any and all violations, maximum penalties, injunctive relief, or other relief FinCEN deems appropriate. FinCEN may take any such action even if it did not take such action against Canaccord in this Consent Order and notwithstanding the releases and waivers herein. In the event FinCEN takes such action under this

paragraph, Canaccord expressly agrees to toll any applicable statute of limitations and to waive any defenses based on a statute of limitations or the passage of time applicable to the Statement of Facts in this Consent Order, until a date 180 days following Canaccord's receipt of notice of FinCEN's determination that a misrepresentation or breach of this agreement has occurred, except as to claims already time barred as of the Effective Date of this Consent Order.

In the event that FinCEN determines that Canaccord has made a misrepresentation or failed to comply with this Consent Order, or any portion thereof, all statements made by or on behalf of Canaccord to FinCEN, including the Statement of Facts, whether prior or subsequent to this Consent Order, will be admissible in evidence in any and all proceedings brought by or on behalf of FinCEN. Canaccord agrees that it will not assert any claim under the Constitution of the United States of America, Rule 408 of the Federal Rules of Evidence, or any other law or federal rule that any such statements should be suppressed or are otherwise inadmissible. Such statements shall be treated as binding admissions, and Canaccord agrees that it shall be precluded from disputing or contesting any such statements. FinCEN shall have sole discretion over the decision to impute conduct or statements of any director, officer, employee, agent, or any person or entity acting on behalf of, or at the direction of Canaccord in determining whether Canaccord has violated any provision of this Consent Order.

XII. PUBLIC STATEMENTS

Canaccord agrees it shall not, nor shall its attorneys, agents, partners, directors, officers, employees, affiliates, or any other person authorized to speak on its behalf or within its authority or control, take any action or make any public statement, directly or indirectly, contradicting its admissions and acceptance of responsibility or any terms of this Consent Order, including any fact finding, determination, or conclusion of law in this Consent Order.

FinCEN shall have sole discretion to determine whether any action or statement made by Canaccord, or by any person under the authority, control, or speaking on behalf of Canaccord contradicts this Consent Order, and whether Canaccord has repudiated such statement.

XIII. RECORD RETENTION

In addition to any other record retention required under applicable law, Canaccord agrees to retain all documents and records required to be prepared or recorded under this Consent Order or otherwise necessary to demonstrate full compliance with each provision of this Consent Order, including supporting data and documentation. Canaccord agrees to retain these records for a period of 6 years after creation of the record, unless required to retain them for a longer period of time under applicable law.

XIV. SEVERABILITY

Canaccord agrees that if a court of competent jurisdiction considers any of the provisions of this Consent Order unenforceable, such unenforceability does not render the entire Consent Order unenforceable. Rather, the entire Consent Order will be construed as if not containing the particular unenforceable provision(s), and the rights and obligations of FinCEN and Canaccord shall be construed and enforced accordingly.

XV. SUCCESSORS AND ASSIGNS

Canaccord agrees that the provisions of this Consent Order are binding on its owners, officers, employees, agents, representatives, affiliates, successors, assigns, and transferees to whom Canaccord agrees to provide a copy of the executed Consent Order. Should Canaccord seek to sell, merge, transfer, or assign its operations, or any portion thereof, that are the subject of this Consent Order, Canaccord must, as a condition of sale, merger, transfer, or assignment obtain the written agreement of the buyer, merging entity, transferee, or assignee to comply with this Consent Order.

XVI. MODIFICATIONS AND HEADINGS

This Consent Order can only be modified with the express written consent of FinCEN and Canaccord. The headings in this Consent Order are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Order or its individual terms.

XVII. AUTHORIZED REPRESENTATIVE

Canaccord's representative, by consenting to and approving this Consent Order, hereby represents and warrants that the representative has full power and authority to consent to and approve this Consent Order for and on behalf of Canaccord and further represents and warrants that Canaccord agrees to be bound by the terms and conditions of this Consent Order.

XVIII. NOTIFICATION

Unless otherwise specified herein, whenever notifications, submissions, or communications are required by this Consent Order, they shall be made in writing and sent via first-class mail and simultaneous email, addressed as follows:

To FinCEN: Associate Director, Enforcement and Compliance Division, Financial Crimes Enforcement Network, P.O. Box 39, Vienna, Virginia 22183

To Canaccord: Chief Compliance Officer, Canaccord Genuity LLC, One Pennsylvania Avenue, Pennsylvania Plaza, 29th Floor, New York, NY 10119

Notices submitted pursuant to this paragraph will be deemed effective upon receipt unless otherwise provided in this Consent Order or approved by FinCEN in writing.

XIX. COUNTERPARTS

This Consent Order may be signed in counterpart and electronically. Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

XX. EFFECTIVE DATE AND CALCULATION OF TIME

This Consent Order shall be effective upon the date signed by FinCEN. Calculation of deadlines and other time limitations set forth herein shall run from the effective date (excluding the effective date in the calculation) and be based on calendar days, unless otherwise noted, including intermediate Saturdays, Sundays, and legal holidays.

By Order of the Director of the Financial Crimes Enforcement Network.

/s/_____

Andrea Gacki Date:
Director

Consented to and Approved By:

/s/_____

Jeffrey Barlow
Canaccord Genuity LLC