K2 Intelligence
Investigations · Compliance Solutions · Cyber Defense

FINANCIAL INTEGRITY NETWORK

POLICY ALERT /// August 31, 2020

Recent U.S. Enforcement Targeting Online Broker Signals Growing Regulatory Focus on Capital Markets

This month's coordinated U.S. multi-agency enforcement action against online broker Interactive Brokers (IBKR) signals authorities' ongoing concerns about anti-money laundering/combating the financing of terrorism (AML/CFT) risk in the securities and commodities sectors and underlines the need for capital markets participants to design and implement comprehensive AML/CFT programs. The U.S. Securities Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), and Commodities Futures Trading Commission (CFTC) fined IBKR a total of $38 million for failure to implement an effective AML/CFT program.[1,2,3] The CFTC noted that "this case marks the first CFTC enforcement action charging a violation of Regulation 42.2, which requires registrants to comply with the Bank Secrecy Act (BSA)."[4]

- The supervisors found that IBKR's transaction monitoring system and rules did not adequately mitigate risk in the products and services it offered and that IBKR failed to file suspicious activity reports (SARs) on customer transactions even when the firm's own monitoring software alerted on the transactions. They also found that IBKR's compliance function was understaffed, and its suspicious transaction analysts were unable to effectively perform their duties because the firm lacked comprehensive databases, including databases of previous investigations.
- FINRA described systematic failures to appropriately manage the risks created by relationships with foreign customers, and specifically with foreign financial institutions (FFIs). FINRA further noted that more than half of IBKR's customers were not U.S. residents. IBKR assumed that foreign wires that lacked full originator data, even those from high-risk jurisdictions, were first-party wires, and thus subjected them to lower scrutiny. It specifically instructed its compliance staff not to investigate many alerts arising from third-party wires to customers located in China, Hong Kong, and Macau. Although IKBR acknowledged that relationships with FFIs posed increased risk, it used purely manual monitoring to surveil transactions, even as its FFI customer base nearly doubled to more than 370 institutions.
- FINRA found many of the same deficiencies in its October 2019 enforcement action against BNP Paribas's securities businesses.[5] That action similarly highlighted the importance of designing a firm's compliance program—particularly transaction monitoring rules—to effectively manage the risks of the firm's products and services mix, and of applying appropriate preventive measures to foreign clients and to wire transfers in foreign currencies.
- In May, a former broker with UK brokerage Beaufort Securities was sentenced to three years' probation after pleading guilty to conspiracy to commit securities fraud and to evade

the Foreign Account Tax Compliance Act.[6,7] The defendant had assisted an undercover FBI agent to manipulate the market for a particular stock. The investigation also resulted in the collapse of Beaufort Securities.[8]

Recent government risk assessments and international media reports clearly illustrate the vulnerability of capital markets to abuse at all stages of the money laundering process and to actors seeking to launder the proceeds of a wide variety of offences, not just those related to market abuse. Official risk assessments also found that market participants are vulnerable due to unique features of the sector and to their weaker understanding of risk.

- The 2020 U.S. *National Strategy for Combating Illicit Finance* included securities broker-dealers on a list of the U.S. financial system's most significant vulnerabilities to illicit finance.[9] The strategy noted that securities markets and brokerage accounts provide many opportunities for layering and integration of criminal proceeds, and that certain features of securities markets—including the lack of beneficial ownership information for some account structures—limit brokers' ability to fully know their customers.
- The UK Financial Conduct Authority's recent review of money laundering (ML) risks in the capital markets found that market participants were "generally at the early stages" of thinking about their illicit finance risks and did not fully understand their exposure, particularly to risks beyond market abuse.[11] The review includes multiple ML typologies that exploit loopholes or extended transaction chains to launder criminal proceeds—no matter their origin—through securities markets.

U.S. Regulatory Gaps Increase Vulnerability of Some Capital Markets Participants

U.S. investment advisers (IAs), including hedge funds, are not required to comply with the requirements of the BSA, including the requirement to maintain an AML/CFT program and to conduct customer due diligence (CDD) on customers.[10] Because IAs frequently act as intermediaries between financial institutions and the ultimate customer, this inconsistency between U.S. and global standards could allow criminals to abuse the services of IAs to conduct sophisticated laundering operations. IAs involved in these transactions could be actively complicit (acting as professional third-party money launderers); willfully blind; or could simply fail to recognize the ML risks associated with their customers or with the investments they manage on their customers' behalf.

Financial institutions holding accounts for IAs, particularly accounts that contain pooled customer funds, should be aware that the IA is not the ultimate beneficial owner of the funds and may in fact have little understanding of its customer's identities, business activities, and source of funds or wealth. Financial institutions should consider treating IAs as correspondent financial institutions and subjecting them to enhanced due diligence, including an assessment of their AML/CFT programs and their CDD policies. Investment advisers should consider proactive efforts to institute AML/CFT programs that will protect them from the real illicit finance risk in the sector and help safeguard their banking relationships and reputations.

- Recent media reports have alleged that the Italian criminal group the 'Ndrangheta was able to sell publicly backed debt owed to its front companies to special purpose vehicles,

which ultimately repackaged the debt as bonds and marketed them through investment banks to customers in European financial centers.[12] This case offers a vivid illustration of the complex and difficult-to-detect techniques that transnational criminal organizations use to exploit even sophisticated consumers of financial services.

Commercial capital markets participants should implement a comprehensive financial crimes compliance (FCC) program that addresses the full scope of products, services, customers, and markets offered or serviced by their businesses. Such a program should be designed to identify and guard against a wide range of malfeasance, including through intermediated relationships that may be covered under specific and enhanced due diligence requirements pursuant to Section 312 of the USA PATRIOT Act. Financial institutions (FIs) that are indirectly exposed to this sector through customer relationships with service providers in the securities and commodities sectors should be aware of risks in these sectors, including risks related to potential noncompliance of participants' developing FCC regimes.

- In implementing a comprehensive FCC program, commercial capital markets participants should:
  - Conduct a full risk assessment of their operations that considers, among other factors, the risk that illicit actors may exploit their products, services, and relationships for criminal purposes, including laundering the proceeds of a variety of criminal offenses unrelated to market abuse or engaging in transactions on behalf of sanctioned parties;
  - Ensure that their automated transaction monitoring systems offer comprehensive coverage and are appropriately designed to identify suspicious activity;
  - Review their sanctions screening and compliance programs to ensure consistency with guidance issued by Treasury's Office of Foreign Assets Control (OFAC), including *A Framework for OFAC Compliance Commitments*;[13]
  - Expand and modify their compliance programs to keep pace with growth or other changes in their operations, such as exposure to new jurisdictions and the launch of new products, services, or relationships with FFIs;
  - Identify intermediated relationships that may present indirect illicit financing risks, including correspondent relationships with FFIs covered by Section 312 of the USA PATRIOT Act, and develop specific controls to address such risks;
- Commercial market participants that engage in correspondent relationships with FFIs should review their systems for monitoring transactions through correspondent accounts to ensure that these are risk-based and appropriate to the volume of activity involved. The IBKR enforcement action sends a clear message that supervisors do not consider manual monitoring of these customers acceptable in situations where FFI customers execute a high volume of transactions.
- FIs with only indirect exposure to the securities and commodities sectors—including those exposed via the broker-dealer and investment advisory arms of their parent company—should be aware that market participants are subject to sharply differing levels of regulation

and oversight depending on their classification and country of origin. FIs should apply enhanced due diligence to market service providers and ensure they are subject to thorough ongoing monitoring. It is particularly critical to apply heightened scrutiny to investment advisers, which are not currently subject to BSA requirements, although even other market participants' AML/CFT programs may lag behind those of FIs.

[1] SEC, "SEC Charges Interactive Brokers with Repeatedly Failing to File Suspicious Activity Reports: Firm Will Pay a Total of $38 Million in Penalties to Settle with Regulators," August 10, 2020, at https://www.sec.gov/litigation/admin/2020/34-89510.pdf.

[2] FINRA, "FINRA Fines Interactive Brokers $15 Million for Widespread AML Failures," August 10, 2020, at https://www.finra.org/media-center/newsreleases/2020/finra-fines-interactive-brokers-15-million-widespread-aml-failures.

[3] CFTC, "CFTC Orders Interactive Brokers LLC to Pay More Than $12 Million for Anti-Money Laundering and Supervision Violations," August 10, 2020, at https://www.cftc.gov/PressRoom/PressReleases/8218-20.

[4] CFTC, "CFTC Orders Interactive Brokers LLC to Pay More Than $12 Million for Anti-Money Laundering and Supervision Violations," August 10, 2020, at https://www.cftc.gov/PressRoom/PressReleases/8218-20; 17 CFR § 42.2, at https://www.govinfo.gov/content/pkg/CFR-2016-title17-vol2/pdf/CFR-2016-title17-vol2-sec42-2.pdf.

[5] FINRA, "FINRA Fines BNP Paribas Securities Corp. and BNP Paribas Prime Brokerage, Inc. $15 Million for AML Program and Supervisory Failures," October 24, 2019, at https://www.finra.org/media-center/newsreleases/2019/finra-fines-bnp-paribas-securities-corp-and-bnp-paribas-prime.

[6] Stewart Bishop, "Ex-Investment Manager Dodges Prison For Stock, Tax Crimes," *Law360*, May 4, 2020, at https://www.law360.com/articles/1270190/ex-investment-manager-dodges-prison-for-stock-tax-crimes.

[7] U.S. Attorney's Office for the Eastern District of New York, "Former Beaufort Securities Investment Manager Pleads Guilty to Conspiracies to Commit Securities Fraud and to Defraud the United States by Failing to Comply With Foreign Account Tax Compliance Act," November 20, 2019, at https://www.justice.gov/usao-edny/pr/former-beaufort-securities-investment-manager-pleads-guilty-conspiracies-commit.

[8] Hannah Murphy and Philip Stafford, "Share pumping and Picassos: $50m scam that killed a London brokerage," *The Financial Times*, March 9, 2018, at https://www.ft.com/content/24db2600-22ff-11e8-add1-0e8958b189ea.

[9] *National Strategy for Combating Terrorist and Other Illicit Financing*, February 2020, at https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf.

[10] K2/Financial Integrity Network, "Client Alert: FATF Upgrades U.S. Customer Due Diligence Regime," April 2, 2020, at https://www.finintegrity.com/uploads/8/7/8/0/87802750/2020.04.02_fatf_us_r10_client_alert.pdf.

[11] Financial Conduct Authority, *Thematic Review 19/4: Understanding the Money Laundering Risks in the Capital Markets*, June 2019, at https://www.fca.org.uk/publication/thematic-reviews/tr19-004.pdf.

[12] Miles Johnson, "How the Mafia infiltrated Italy's hospitals and laundered the profits globally," *The Financial Times*, July 9, 2020, at https://www.ft.com/content/8850581c-176e-4c5c-8b38-debb26b35c14.

[13] OFAC, "OFAC Issues A Framework for Compliance Commitments", May 2, 2019, at https://home.treasury.gov/news/press-releases/sm680 (announcing *A Framework for OFAC Compliance Commitments*, available at https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf).