

**FINANCIAL INDUSTRY REGULATORY AUTHORITY  
LETTER OF ACCEPTANCE, WAIVER AND CONSENT  
NO. 2015047770301**

TO: Department of Enforcement  
Financial Industry Regulatory Authority (FINRA)

RE: Interactive Brokers LLC, Respondent  
Member Firm  
CRD No. 36418

Pursuant to FINRA Rule 9216 of FINRA's Code of Procedure, Respondent Interactive Brokers LLC ("Interactive Brokers" or the "Firm") submits this Letter of Acceptance, Waiver and Consent (AWC) for the purpose of proposing a settlement of the alleged rule violations described below. This AWC is submitted on the condition that, if accepted, FINRA will not bring any future actions against Respondent alleging violations based on the same factual findings described herein.

**I.**

**ACCEPTANCE AND CONSENT**

- A. Respondent hereby accepts and consents, without admitting or denying the findings, and solely for the purposes of this proceeding and any other proceeding brought by or on behalf of FINRA, or to which FINRA is a party, prior to a hearing and without an adjudication of any issue of law or fact, to the entry of the following findings by FINRA:

**BACKGROUND**

Interactive Brokers has been a FINRA member firm since January 1995. It is headquartered in Greenwich, Connecticut. The Firm offers online trading through self-directed accounts. The Firm also clears transactions for retail and institutional customers, as well as for customers introduced to it by approximately 610 foreign and domestic introducing firms. As of June 2020, Interactive Brokers and its affiliates employed more than 1,600 people, including approximately 327 registered individuals at approximately 7 branch offices.

**RELEVANT DISCIPLINARY HISTORY**

Respondent does not have any relevant disciplinary history with the Securities and Exchange Commission ("SEC"), any state securities regulators, FINRA, or any other self-regulatory organization.

**OVERVIEW**

Since 2013, Interactive Brokers' business has grown dramatically. In addition to having grown in size – in terms of numbers of customer accounts and securities and money transactions

executed – it has also grown in scope. In particular, the Firm has significantly expanded its relationships with foreign financial institutions (“FFIs”), for whom the Firm performs clearing services, including hundreds of FFIs located in high-risk jurisdictions. From January 2013 through September 2018 (the “Relevant Period”), however, Interactive Brokers failed to develop and implement an anti-money laundering (“AML”) program reasonably designed to match its growth.

During the Relevant Period, the Firm’s AML program was deficient in many respects, including the following:

**Failure to Reasonably Surveil Certain Money Movements:** Interactive Brokers did not reasonably surveil certain money movements for money laundering concerns. The Firm treated hundreds of millions of dollars of incoming wire transfers as first-party transfers despite the fact that those wires did not identify the names of the remitting persons or entities. It also failed to reasonably surveil thousands of third-party transfers to customers located in China, Hong Kong, and Macau, three jurisdictions deemed “high-risk” by domestic and international anti-money laundering agencies. Additionally, the Firm did not reasonably surveil for AML purposes outgoing wire transfers identified as “first-party” transfers (*i.e.*, transfers where the recipient was the customer itself), because the Firm accepted customers’ designations that they were first-party wire transfers, even when the Firm learned that some purportedly “first-party” wires were, in fact, third-party wires.

**Failure to Develop and Implement Reasonably Designed Surveillance Tools for Certain Money Movements and Securities Transactions:** The Firm’s tool to review securities trading and money movements by customers of FFIs, including in high-risk jurisdictions, was a blotter report that required manual review, provided only summary data, and failed to identify red flags of suspicious activity. The report, moreover, had programming errors, or “bugs,” which often resulted in the Firm failing to review certain money transfers for potentially suspicious activity. Similarly, Interactive Brokers manually monitored its customers’ deposits and withdrawals of money using spreadsheets that did not automatically identify potentially suspicious activity for further review. Moreover, Interactive Brokers did not employ reasonably designed automated surveillance tools dedicated to identifying insider trading and manipulative microcap securities trading.

**Failure to Reasonably Investigate Potentially Suspicious Activity:** Interactive Brokers failed to reasonably investigate certain potentially suspicious activity that occurred through the Firm. Despite the Firm’s growth, it did not sufficiently increase its AML compliance staff during the Relevant Period. The Firm also lacked an effective case management system; analysts, therefore, could not readily learn information about prior AML investigations concerning the same customers or identify patterns and trends. Because of these failures, Interactive Brokers failed to reasonably investigate numerous instances of suspicious activity that appeared on its surveillance reports, and failed to identify that some were Ponzi schemes, market manipulation schemes, and the like.

**Failure to File SARs:** Interactive Brokers failed to file Suspicious Activity Reports

(“SARs”) after detecting that customers had engaged in suspicious activity. For example, the Firm failed to file a SAR even after a customer “contacted [the Firm] to state they were scammed by” an introducing broker. Moreover, the Firm did not file SARs when it learned about potentially suspicious conduct from regulators or law enforcement agencies because the Firm incorrectly believed that it was not required nor useful to do so.

**Inadequate AML Testing:** Interactive Brokers failed to conduct reasonable AML testing throughout the Relevant Period. The Firm’s internal audit group reviewed Interactive Brokers’ AML program, but failed to question whether the Firm applied appropriate criteria to generate surveillance reports; whether analysts reasonably reviewed surveillance reports and properly investigated potentially suspicious conduct; whether analysts memorialized the results of their reviews and investigations; whether supervisors reasonably reviewed analysts’ determinations; and whether SAR filing decisions were reasonable and documented. The Firm’s AML program had deficiencies in each of those areas.

Based on the foregoing, Interactive Brokers violated FINRA Rules 3310(a), (b), and (c), and 2010 during the entirety of the Relevant Period.

### **FACTS AND VIOLATIVE CONDUCT**

Since 2013, Interactive Brokers’ business has grown dramatically. It is currently one of the largest electronic broker-dealers in the United States based on shares traded, executing approximately 800,000 trades per day.

Interactive Brokers has also expanded its relationships with FFIs. In July 2015, Interactive Brokers cleared transactions for 192 FFIs. By December 2018, Interactive Brokers cleared transactions for 373 FFIs, far more than any other broker-dealer in the United States. Indeed, during the Relevant Period, approximately 55% of its 640,000 customers were domiciled outside the United States, many in countries such as Russia, Pakistan, Panama, China, and Cyprus, despite the risks inherent in those jurisdictions.

FINRA Rule 3310 requires member firms to “develop and implement a written anti-money laundering program reasonably designed to achieve and monitor ... 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.” Among other AML program requirements is the mandate set forth in FINRA Rule 3310(a) that firms “[e]stablish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under [the Bank Secrecy Act] and the implementing regulations thereunder.” Broker-dealers are required to report suspicious activity pursuant to 31 C.F.R. 1023.320. Additionally, FINRA Rule 3310(b) requires that member firms “[e]stablish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder.” A violation of FINRA Rule 3310 also constitutes a violation of FINRA Rule 2010.

In April 2002, FINRA issued Notice to Members (“NTM”) 02-21, which reminded broker-dealers of these obligations, and further advised broker-dealers that their AML procedures must

address a number of areas, including monitoring “trading and the flow of money into and out of ... account[s].” NTM 02-21 also advised broker-dealers “to look for signs of suspicious activity that suggest money laundering” – or, “red flags” – and if they detect “red flags,” to “perform additional due diligence.” In August 2002, FINRA issued NTM 02-47, which described the suspicious activity reporting rule promulgated by the Department of the Treasury for the securities industry. NTM 02-47 further advised broker-dealers of their duty to file a SAR for any transaction raising suspicions of illegal activity occurring after December 30, 2002.<sup>1</sup>

NTM 02-21 advised that, “[t]o be effective, [a firm’s AML program] must reflect the firm’s business model and customer base.” Interactive Brokers’ AML program during the Relevant Period was not reasonably designed to do so. Instead, the Firm operated an AML program that, for years, was understaffed and under-resourced and relied on surveillance reports that were both insufficient for a firm of Interactive Brokers’ size and business model and had programming failures; with respect to certain transactions, the Firm’s AML program failed to conduct any surveillance at all. During the Relevant Period, Interactive Brokers failed to engage in a formal assessment of the AML risks of its business or the adequacy of its staffing and technology to perform reasonable AML surveillance. As a result, the Firm failed to detect, investigate, or report numerous instances of suspicious conduct.

## **I. The Firm Failed to Reasonably Surveil Certain Money Movements**

To comply with FINRA Rule 3310 and the Bank Secrecy Act (“BSA”), firms must establish policies, procedures, and internal controls that can reasonably be expected to detect and cause the reporting of suspicious movements of money to and from their customers’ accounts. As set forth below, the Firm failed to reasonably surveil certain types of money movements for money laundering concerns during the Relevant Period.

### **A. Interactive Brokers Failed to Surveil “No-Data” Wires**

Some nations’ wire transfer and electronic payment messages do not include complete information about the originator of the payments. The Firm referred to such wires as “no-data” wires. Interactive Brokers chose not to review no-data wires as third-party wires. As a result, no-data wires were not subject to the additional monitoring and review that the Firm had in place for some third-party wires, but were instead treated as if they were first-party wires. The Firm’s internal reference guide did not address no-data wires, and Firm analysts did not review, or contact customers to determine the origin of, no-data wires.

During the Relevant Period, Firm customers received hundreds of millions of dollars of no-data wires. For example, between January 1, 2015 and April 30, 2016, Interactive Brokers customers deposited into their accounts more than \$165 million they received via no-data wires. Many of those wires originated from countries with a heightened risk of money laundering. In January 2016, alone, Interactive Brokers customers received \$14.3 million via no-data wires, and \$6.3

---

<sup>1</sup> Likewise, in FINRA Regulatory Notice 19-18 (“RN 19-18”), issued in May 2019, FINRA provided broker-dealers with a non-exhaustive list of money laundering “red flags” potentially indicative of suspicious activity. RN 19-18 further explained that “[u]pon detection of red flags through monitoring, firms should consider whether additional investigation, customer due diligence measures or a SAR filing may be warranted.”

million of those no-data wires originated from jurisdictions such as Malta, Hong Kong, Cyprus, China, Liechtenstein, and Estonia, despite the risks associated with those jurisdictions.

### **B. Interactive Brokers Failed to Reasonably Surveil Certain Third-Party Transfers to Customers Located in China, Hong Kong, and Macau**

Interactive Brokers also failed to reasonably surveil certain third-party transfers to customers located in China, Hong Kong, and Macau, three jurisdictions deemed to be “high-risk” by domestic and international anti-money laundering agencies. The Firm’s internal reference guide specifically instructed analysts not to review third-party deposits to customers located in those countries if they had previously received deposits from five or fewer individuals. This instruction was designed to limit the number of “false positives” for AML analysts to review, but the Firm failed to assess the associated AML risks. Indeed, in applying the parameters it did, Interactive Brokers failed to review thousands of deposits as third-party transfers to customers located in China, Hong Kong, and Macau during the Relevant Period. From March 2013 through January 2016, for example, the Firm failed to review as third-party wires more than 1,100 third-party wires that transmitted more than \$64 million to its customers located in China.

### **C. Interactive Brokers Also Failed to Surveil Purportedly “First-Party” Outgoing Wire Transfers**

Interactive Brokers also failed to reasonably review some of its customers’ outgoing wire transfers for AML concerns. The Firm allowed customers to select on wire transfer forms whether the recipient of an outgoing wire was the customer itself (a “first-party” wire) or a third party, but the Firm did not take any steps to verify that the wire transfers self-identified by customers as first-party wires were, in fact, first-party wires. As a result, the Firm did not reasonably review for AML purposes wires that customers identified as first-party transfers to themselves at other financial institutions, including FFIs, even when those transfers were rejected by receiving institutions.

## **II. The Firm Failed to Develop and Implement Reasonably Designed Surveillance Tools for Certain Money Movements and Securities Transactions**

FINRA explained in NTM 02-21 that member firms “should implement systems, preferably automated ones, that would allow firms to monitor trading, wire transfers, and other account activity to allow firms to determine when suspicious activity is occurring.” NTM 02-21 further explained that “[i]f a firm decides to monitor customer accounts manually, it must review a sufficient amount of account activity to ensure the detection of suspicious activity by allowing the member to identify patterns of activity and more importantly, new patterns or patterns that are inconsistent with the customer’s financial status or make no economic sense.”

As set forth below, the Firm used blotter-based spreadsheets that were not automated and had programming “bugs.” The Firm’s few automated trade surveillance tools also had certain limitations that impacted their effectiveness. Consequently, the Firm failed to reasonably surveil certain money movements and securities transactions.

## **A. Interactive Brokers' Surveillance of FFI Accounts Was Ineffective**

By the end of the Relevant Period, more than 300 of Interactive Brokers' customers were FFIs that had established correspondent accounts at the Firm for trading and clearing services. During the Relevant Period, Interactive Brokers recognized that correspondent accounts for FFIs ("CAFFIs") presented unique money laundering risks, and therefore it assigned a risk ranking to each CAFFI account when the account was established. Interactive Brokers' risk ranking determined how frequently an AML analyst reviewed a CAFFI account's securities trading and money movements. The Firm reviewed accounts that posed the greatest risk of illicit activity, known as "CAFFI 2" accounts, each month. It reviewed the accounts that presented the least risk, known as "CAFFI 5" accounts, once a year.

During the Relevant Period, Firm analysts monitored activity in CAFFI accounts manually. CAFFI account activity was listed on separate spreadsheets based on risk rating; each spreadsheet listed thousands of lines of data. During the Relevant Period, each spreadsheet grew as the Firm expanded its trading and clearing business for its FFI customers. The CAFFI 2 spreadsheet, for example, grew so large that it required an analyst to spend between five and ten days each month to review it.

Despite their size, the spreadsheets included only summary data and provided information about only the prior review period's transactions, requiring analysts to access multiple Firm systems to understand a potentially suspicious transaction and inhibiting their ability to identify patterns or trends.

As a result of the design of the CAFFI spreadsheets, Firm analysts failed to identify certain suspicious activity appearing on the spreadsheets. For example, Interactive Brokers failed to investigate a customer ("Customer 1") that appeared on ten CAFFI 2 reports (and three other surveillance reports that monitored deposits and withdrawals of money). Customer 1 was a Panamanian FFI that converted currencies and transmitted money between countries. Although Customer 1 indicated on its Interactive Brokers new account forms that it had \$15 million in total assets, net annual income of \$1 million, and a liquid net worth of \$5 million, it engaged in hundreds of deposits and withdrawals totaling \$358 million, and nearly \$292 million in foreign exchanges, from January 2013 through May 2016. During that time, publicly accessible blogs began to allege that Customer 1 and its principals operated a \$400 million trading scheme and misappropriated investors' money. Despite the blogs, which were published regularly for years, Interactive Brokers analysts failed to detect, investigate, or report Customer 1's suspicious trading activity.

Additionally, the CAFFI spreadsheets contained programming errors, or "bugs," which caused hundreds of high-risk FFI accounts of the Firm to be omitted from the spreadsheets at various times during the Relevant Period. In 2015, a compliance manager reported to his supervisor that he had "identified a bug where accounts that are marked as a CAFFI were not appearing" on the CAFFI 2 spreadsheet, and that the reports were "frequently incorrect and it can take weeks of follow-up with programmers to get a corrected report." The Firm took more than fourteen months to correct that "bug." In April 2018, the Firm identified additional accounts that the "bug" had excluded from the CAFFI spreadsheets. As a result of these programming problems,

at various points during the Relevant Period, the Firm failed to timely review the activity in the FFI accounts that were omitted from the CAFFI spreadsheets.

### **B. Interactive Brokers' Surveillance of Deposits and Withdrawals Was Ineffective**

Similarly, during the Relevant Period, the Firm's analysts manually monitored its customers' deposits and withdrawals of money using spreadsheets that provided only summary statistical information and did not identify potentially suspicious activity for further review, such as the movement of money to or from high-risk countries. Moreover, the Firm arbitrarily selected the parameters it applied to the spreadsheets, resulting in the exclusion of some deposits and withdrawals from review.

In addition to failing to identify potentially suspicious money movements, the Firm's manual review of deposits and withdrawals also caused it to fail to identify potentially suspicious securities trading. As discussed below, Interactive Brokers failed to identify that a customer, Customer 2, was engaged in suspicious microcap securities trading, even though Customer 2's multi-million dollar withdrawal from its account appeared on the Firm's deposits and withdrawals report.

### **C. Interactive Brokers' Surveillance of Certain Customer Securities Transactions Was Ineffective**

Even though Interactive Brokers processed hundreds of thousands of trades a day throughout the Relevant Period, it did not employ automated surveillance tools reasonably designed to identify insider trading and manipulative microcap securities trading.

#### *i. Insider Trading*

The only dedicated tool that Interactive Brokers used to monitor for potential insider trading by its customers was a surveillance report that evaluated primarily those customers who self-identified as insiders of public companies and who then traded in the equities of their own companies. As a result of these limitations, Firm analysts failed to identify certain insider trading by its customers.

For example, during a three-week period in 2016, five Interactive Brokers customers amassed positions, totaling nearly 2.15 million shares, in the stock of one Nasdaq-traded company ("Company A"). The customers' purchases constituted approximately 17% of all market trading in Company A during that three-week period and, in five days during the period, the customers' trading constituted between 21.1% and 34.8% of the trading volume in Company A. The five customers, who were all located in Beijing, China, had not previously traded in Company A, and the cost of their purchases greatly exceeded the annual income and net worth figures that they had disclosed to the Firm in their new account forms. Additionally, the five customers accessed their Interactive Brokers accounts through computers that shared Internet Protocol and media access control addresses. During the three days immediately following the weeks of purchases, the customers sold all of their stock after rumors circulated that another entity might acquire Company A. The customers netted profits of more than \$29 million from their trades. Although

an Interactive Brokers surveillance report identified three of the customers as among those with the highest profits from trading on one of those three days, the Firm decided after a cursory review that the customers' trading was not suspicious. The SEC later filed a civil insider trading suit naming the five Interactive Brokers customers as relief defendants, but the Firm did not conduct an AML review as to these defendants or file a SAR at that time.

## *ii. Manipulative Microcap Securities Trading*

Likewise, certain of the Firm's customers engaged in extensive microcap securities trading, but Interactive Brokers did not reasonably surveil that trading. Rather, the Firm's analysts identified suspicious microcap securities trading only if they noticed it through their more generalized reviews of customer trading.

As a result, Firm analysts failed to identify red flags of manipulative microcap securities trading by its customers. For example, a company located in Belize controlled by Bulgarian and Swiss nationals ("Customer 2") netted approximately \$2.6 million through manipulative trading of an Over-the-Counter ("OTC") listed microcap security. Customer 2 opened an Interactive Brokers account in December 2014 and deposited four million shares of the microcap security in January 2015. Just two weeks later, Customer 2 sold its microcap securities holdings and immediately withdrew the sale proceeds. Shortly before Customer 2 began selling, the microcap security's price and volume each increased by more than 2,000%, a rise that continued while Customer 2 sold its stock. The microcap security's trading volume, for instance, increased from 270,000 shares in December 2014 to 22 million shares in March 2015 as Customer 2 sold its position. Customer 2's trading constituted approximately 45% of the microcap security's trading on 9 of the 19 days that it traded. Customer 2 also purchased small amounts of the microcap security to support the stock's price when it faced downward pressure. Those transactions lacked an economic purpose as Customer 2 immediately liquidated the shares at lower prices.

Interactive Brokers identified Customer 2's multi-million dollar withdrawal from its account on the report, discussed above, that monitored deposits and withdrawals, but the AML analyst closed the review with a template response and without noting Customer 2's trading in the microcap security. The Firm also closed nine reviews that identified Customer 2's sales during the last 20 minutes of trading sessions with template responses that the trading appeared "normal." Interactive Brokers failed to conduct an AML review of Customer 2's trading or file a timely SAR even after receiving a formal inquiry from FINRA in March 2015 regarding Customer 2's trading in the microcap security.

## **III. The Firm Failed Reasonably to Investigate Potentially Suspicious Activity**

The BSA requires broker-dealers to reasonably investigate red flags that suggest money laundering. As Interactive Brokers' trade volume, customer base, and FFI clearing business expanded during the Relevant Period, its blotter-style surveillance spreadsheets captured more data. But, because these reports were not automated and did not specifically identify potentially suspicious activity for further review, they required time-intensive, manual review by Firm analysts.

The Firm, however, failed to add sufficient personnel to review those reports as the Firm's



business grew, and the Firm also failed to provide analysts with the tools and resources needed to conduct reasonably effective reviews. Consequently, Firm analysts were provided with voluminous reports, which they routinely failed to review in a timely fashion, and Interactive Brokers failed to reasonably investigate schemes that raised red flags on its surveillance reports.

#### **A. Interactive Brokers Failed to Reasonably Staff its AML Compliance Department**

Interactive Brokers failed to reasonably staff its AML compliance department. For example, in 2010, Firm analysts conducted approximately 18,000 “account reviews,” a number that ballooned to approximately 80,000 in 2016. Likewise, between January 2013 and May 2016, the number of rows on the monthly CAFFI 2 spreadsheet increased from approximately 2,400 to approximately 7,600.

The Firm, however, added only two AML analysts between 2013 and 2016, increasing its staff from four to six. In 2015, a compliance manager warned his supervisor that “we are chronically understaffed” and “struggling to review reports in a timely manner.” A year later, the manager wrote that the compliance department was “still struggling to review reports in a timely manner” and “barely able to review” some of them. The manager, moreover, noted that he had “little time to conduct supervisory reviews of my staff’s surveillance reports, which is concerning considering most of our staff members are new.”

Interactive Brokers continued to have a backlog of unreviewed surveillance reports for activity occurring during the Relevant Period that lasted until 2020. In December 2018, for example, the Firm’s internal audit department noted that it could not find evidence that analysts had reviewed some CAFFI reports that the Firm generated in 2017, contributing to the Firm’s decision to increase its AML staffing, as discussed below. In January 2020, Interactive Brokers continued to review some CAFFI reports reflecting money transmissions and securities trading by FFIs in 2018.

#### **B. Interactive Brokers Failed to Implement a Reasonable Case Management System or Devote Sufficient Technical Resources to AML**

The Firm’s deficient systems compounded its staffing shortages. The Firm failed to implement a reasonable case management system to record analysts’ initiations of investigations, the status of those investigations, and the steps that analysts took to perform their investigations. The Firm lacked a system to track analysts’ progress in completing investigations and surveillance report reviews, and continued to lack such a system for approximately three years after a compliance manager requested that the Firm purchase or develop one. A Firm analyst reviewing suspicious activity, therefore, could not readily obtain information about prior investigations concerning the same customer or similar suspicious conduct. Likewise, Interactive Brokers did not have a compliance tool that would permit its AML analysts to aggregate information across a customer’s multiple accounts, or see patterns or trends in a single account, without making time-intensive inquiries in multiple, distinct Firm systems.

The Firm also failed to provide sufficient technical support to ensure that its surveillance reports operated effectively. As noted, in 2015, a compliance manager identified numerous surveillance

reports that contained programming “bugs,” and informed his supervisor that the Firm’s programmers had not fixed the “bugs” after repeated requests. By 2016, the compliance manager informed his supervisor that “we often find bugs in our tools and reports and can’t get them to fix them until the situation hits emergency status.” The manager suggested that the Firm assign dedicated programmers to the surveillance department, which would be “an obvious solution to this problem,” but noted that “it seems management has been hesitant to do this in the past.” As an alternative, the manager suggested that Interactive Brokers acquire a non-proprietary trade surveillance system that would relieve “countless hours of researching issues, drafting specifications, programming systems/reports and bug fixing.” The Firm, however, did not approve that request.

### **C. Interactive Brokers Failed to Investigate Suspicious Activity**

The Firm also failed to consistently document and track: investigations it undertook in response to regulatory inquiries; employees’ notifications of potentially suspicious activity or investigations undertaken in response to those notifications; and the reasons it determined not to file a SAR. Instead, the Firm encouraged analysts to insert boilerplate language in surveillance reports when closing their reviews, a practice deemed “efficient” by a compliance manager.

For example, analysts used template language to close more than 460 reviews of surveillance reports during a three-year period about a customer who operated a Ponzi scheme and who dissipated nearly \$16 million of investors’ money through trades executed at Interactive Brokers (“Customer 3”). When Customer 3 opened his Interactive Brokers account, he stated that he was an “at home trader” with annual income of \$150,001 to \$250,000 and a net worth of \$1 million to \$5 million. During the Relevant Period, however, Customer 3 deposited more than \$14 million into his Interactive Brokers account – a figure that should have triggered red flags since it was well beyond his stated income or resources. Additionally, Customer 3 regularly incurred trading losses of more than \$100,000 each month and seemingly replenished his account with fresh deposits that exceeded his stated annual income. According to Interactive Brokers’ surveillance reports, in one month Customer 3 lost nearly \$650,000 and made nine deposits totaling \$900,000, and the following month he lost more than \$845,000 and deposited \$795,000. Customer 3 also withdrew more than \$2.26 million from his account over approximately three years. Several types of surveillance reports identified Customer 3’s deposits, withdrawals, and securities trading, but analysts closed those reports with template language including “No apparent third party deposits. Deposit activity appears to be based on [profit and loss]. Activity does not appear unusual.” The Firm consequently did not investigate Customer 3 or speak with him to understand the source of his deposits or to ask about his apparent lack of concern regarding his significant monthly trading losses. In March 2018, Customer 3 pled guilty to securities fraud and was sentenced to eight years’ imprisonment.

Similarly, Interactive Brokers closed reviews concerning potentially manipulative “matched” trades by China-based accounts in the shares of a publicly traded company (“Company B”). Between July 28, 2017, when Company B’s shares began trading on Nasdaq, and September 21, 2018, Interactive Brokers reported 908 “cross trades” at the Firm, meaning that its customers had purchase and sale orders for the same stock at nearly the same time and for the same price. During the same period, the closing price for Company B’s shares increased from \$8.93 to nearly \$27, and was often highly volatile. On August 21, 2018, for example, Company B stated that it

was “not aware of the reasons for the recent volatility in its stock,” after its shares fell from an intraday high of \$29.69 to an intraday low of \$8.61 on volume of more than 4.3 million shares, a sixteen-fold increase in trading volume from the prior day. In 2018, FINRA staff issued two requests for information to Interactive Brokers about order and trading activity in Company B’s stock. An Interactive Brokers surveillance report identified 66 of the 908 cross-trades as potentially manipulative, but the Firm concluded that the customers “unintentional[ly]” traded against each other, even when customers crossed their trades several times on a single day. The Firm, moreover, summarily closed reviews even when its customers placed cross trades through online accounts that appeared to be related. The Firm did not adequately document its rationale for closing reviews about different customers who traded with each other in Company B’s shares on the same day, at nearly the same time, and at the same price.

#### **IV. Interactive Brokers Failed to File SARs about the Suspicious Activity that it Detected**

BSA regulation 31 C.F.R. § 1023.320(a)(2) requires that broker-dealers file a SAR with the Financial Crimes Enforcement Network (“FinCEN”) to report a transaction (or a pattern of transactions) conducted or attempted by, at, or through the broker-dealer involving or aggregating to at least \$5,000 that the broker-dealer knows, suspects, or has reason to suspect: (1) involves funds derived from illegal activity or is conducted to disguise funds derived from illegal activities; (2) is designed to evade any requirement of the BSA; (3) has no business or apparent lawful purpose and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts; or (4) involves use of the broker-dealer to facilitate criminal activity.

During the Relevant Period, Interactive Brokers failed to establish and implement policies, procedures, and internal controls reasonably designed to cause the reporting of suspicious transactions as required by the BSA and 31 C.F.R. § 1023.320(a)(2). Even when Interactive Brokers identified suspicious activity through its surveillance reports and investigations, it did not always recognize that it was required to report that illegal activity through SARs. For example, in multiple investigations during the Relevant Period, the compliance department found that customers had engaged in manipulative trading, and took actions to close the customers’ accounts or place restrictions upon them, but the Firm failed to file SARs. During the Relevant Period, the Firm also failed to file SARs upon detecting suspicious activity on several other occasions. For example, upon detecting the following suspicious activity, the Firm took the following actions:

- Customers were “executing a manipulative trading strategy.” The Firm “warned” the customers;
- A customer was “scammed” by an introducing broker. The Firm “closed the introducing broker to avoid further conflict;”
- A customer opened 60 accounts in his own name, and dozens of “advisor” accounts for relatives, to arbitrage tender offers. The Firm “worked with the customer to bring the accounts into compliance;”

- A customer's funds were withdrawn without his authorization and sent to a financial advisor. The Firm "reset" the customer's password; and
- A former customer issued a "fraudulent letter" to "defraud overseas investors out of \$3MM." The Firm "closed" any "associated" accounts.

Interactive Brokers did not file SARs regarding any of the misconduct listed above until considerably after the Firm detected the suspicious activity, and after it was prompted to do so by FINRA's investigation into the Firm's AML program.

Additionally, Interactive Brokers failed to investigate and file SARs when appropriate after learning about potentially suspicious conduct from regulators or law enforcement agencies because its senior compliance officers incorrectly believed that it was not useful, nor required, to do so. For example, from February 2014 to March 2016, the Firm filed only 3 SARs in response to 37 regulatory inquiries by FINRA and the SEC. In addition to failing to file SARs, the Firm could not demonstrate that it had even conducted investigations in response to certain of the regulators' inquiries. Indeed, despite Interactive Broker's growth, it filed fewer SARs in 2015 than it did in 2010. The Firm did not materially increase its SAR filings until well after FINRA staff began its investigation of Interactive Brokers' AML program.

By virtue of the foregoing, Interactive Brokers violated FINRA Rules 3310(a) and (b) and 2010.

#### **V. Interactive Brokers Failed to Conduct Independent AML Testing**

FINRA Rule 3310(c) requires member firms that conduct business with the public to undertake annual independent testing of their AML programs, and FINRA has stressed the importance of thorough independent testing to member firms. In the 2017 Report on FINRA Examination Findings, for example, FINRA stated that effective AML programs conduct independent testing that includes "trading and money movement activity to test whether the firm was performing adequate monitoring for and investigations of potentially suspicious activity."

During the Relevant Period, the Firm's internal audit group performed its annual tests. The tests, however, failed to assess whether the Firm utilized reasonable surveillance reports and failed to test the integrity of the data underlying those reports. The tests also failed to assess: whether AML analysts reasonably reviewed surveillance reports and properly investigated potentially suspicious conduct; whether analysts adequately memorialized the results of their reviews and investigations; whether supervisors reasonably reviewed the analysts' determinations; and whether SAR filing decisions were reasonable and adequately documented. The Firm's independent testing, moreover, failed to assess whether Interactive Brokers dedicated reasonable resources to its AML program.

Had the Firm's internal auditors conducted reasonable independent testing, they would have learned that the Firm's AML program had deficiencies in all of those respects.

By virtue of the foregoing, Interactive Brokers violated FINRA Rules 3310(c) and 2010.

## SANCTIONS CONSIDERATIONS

In determining the appropriate sanctions in this matter, FINRA considered, among other factors, that during the course of this investigation Interactive Brokers took proactive steps, invested substantial resources, and began taking meaningful steps, to remediate its AML program. The Firm has developed and implemented new, automated surveillance reports, and a new case management system that improves the type and amount of information available to its analysts. The Firm also has hired many dozens of AML-dedicated staff, including senior personnel with regulatory and law-enforcement backgrounds. The Firm has engaged a number of consultants, including a third-party outside consultant (the “Third-Party Consultant”)<sup>2</sup> to conduct a non-privileged review of its AML processes and systems. The Third-Party Consultant has provided recommendations concerning the Firm’s AML program, which Interactive Brokers has adopted and is implementing. Additionally, Interactive Brokers has retained third-party vendors to assess the AML risks posed by the Firm’s business and to conduct third-party testing of the Firm’s AML program.

Accordingly, the sanctions imposed on Interactive Brokers by this AWC reflect FINRA’s consideration of these factors, and FINRA’s determination that the Third-Party Consultant is qualified and not unacceptable to FINRA.

B. Respondent also consents to the imposition of the following sanctions:

1. a censure;
2. a fine in the amount of \$15 million; and
3. an undertaking to do the following:
  - a. Continue to retain, at its own expense, the Third-Party Consultant to conclude a review of the adequacy of Interactive Brokers’ policies, procedures, and internal controls relating to AML surveillance, investigations, and reporting.
  - b. Cooperate with the Third-Party Consultant in all respects, including providing the Third-Party Consultant with access to Interactive Brokers’ and its affiliates’ files, books, records, and personnel, as reasonably requested for the above-mentioned reviews. Interactive Brokers shall require the Third-Party Consultant to report to FINRA on its activities as FINRA may request and shall place no restrictions on the Third-Party

---

<sup>2</sup> The Third-Party Consultant retained by the Firm was comprised primarily of two individuals. Since the time of the Third-Party Consultant’s retention, the original consulting firm disbanded and one of the individuals from the original consulting firm is continuing the work of the Third-Party Consultant at a new consulting firm. As a result, the term “Third-Party Consultant,” as used in this AWC, refers to the original consulting firm, the new consulting firm, and the individual who has worked at both firms.

Consultant's communications with FINRA. Further, Interactive Brokers, upon request, shall make available to FINRA any and all communications between the Third-Party Consultant and the Firm and documents reviewed by the Third-Party Consultant in connection with this review.

- c. Interactive Brokers shall not terminate the relationship with the Third-Party Consultant without FINRA's written approval<sup>3</sup>; Interactive Brokers shall not be in and shall not have an attorney-client relationship with the Third-Party Consultant and shall not seek to invoke the attorney-client privilege or other doctrine or privilege to prevent the Third-Party Consultant from transmitting any information, reports or documents to FINRA.
- d. At the conclusion of the Third-Party Consultant's review, which shall be no more than 30 days after the date of the Notice of Acceptance of this AWC, Interactive Brokers shall require the Third-Party Consultant to submit a written report ("the Initial Report") to it and FINRA. The Initial Report shall, at a minimum, evaluate and address the adequacy of Interactive Brokers' AML program, and make recommendations regarding how Interactive Brokers should improve its AML program; and
  - (i) Within 30 days after delivery of the Initial Report, Interactive Brokers shall adopt and implement the recommendations of the Third-Party Consultant or, if it considers a recommendation to be, in whole or in part, unduly burdensome or impractical, propose an alternative procedure to the Third-Party Consultant designed to achieve the same objective. Interactive Brokers shall submit such proposed alternatives in writing simultaneously to the Third-Party Consultant and FINRA ("Firm's Proposed Alternative Procedures").
  - (ii) Within 30 days of receipt of any of the Firm's Proposed Alternative Procedures, Interactive Brokers shall require the Third-Party Consultant to: (i) reasonably evaluate the alternative procedure(s) and determine whether it will achieve the same objective as the Third-Party Consultant's original recommendation; and (ii) provide the Firm and FINRA with a written decision reflecting its determination ("Written Report Regarding Alternative Procedures"). In the event the Third-Party Consultant and Interactive Brokers are unable to agree, the Firm must abide by the Third-Party Consultant's ultimate determination with respect to any proposed alternative procedure and must adopt and implement all recommendations deemed appropriate by the Third-Party Consultant.
  - (iii) Within 335 days after the issuance of the later of the Third-Party Consultant's Initial Written Report or Written Report Regarding

---

<sup>3</sup> This provision does not apply to the original consulting firm, which has disbanded.

Alternative Procedures (if any), Interactive Brokers shall provide the Third-Party Consultant and FINRA staff with a written Implementation Report, certified by an officer of the Firm, attesting to, containing documentation of, and setting forth the details of the Firm's implementation of the Third-Party Consultant's recommendations. The certification shall identify the undertakings, provide written evidence of compliance in the form of a narrative, and be supported by exhibits sufficient to demonstrate compliance. FINRA may make reasonable requests for further evidence of compliance, and Interactive Brokers agrees to provide such evidence.

- e. Interactive Brokers has retained the Third-Party Consultant to conduct a follow up review and submit a written Final Report to the Firm and to FINRA within 90 days after the issuance of the Implementation Report. In the Final Report, the Third-Party Consultant shall address the Firm's implementation of the systems, policies, procedures, and training and make any further recommendation it deems necessary. Within 30 days of receipt of the Third-Party Consultant's Final Report, Interactive Brokers shall adopt and implement recommendations contained in the Final Report, and inform FINRA in writing that it has done so.
- f. Require the Third-Party Consultant to enter into a written agreement that provides that for the duration of this engagement and for a period of two years from the completion of this engagement, the Third-Party Consultant shall not enter into any other employment, consultant, attorney-client, auditing or other professional relationship with Interactive Brokers, or any of its present or former affiliates, directors, officers, employees, or agents acting in their capacity as such. Any Firm with which the Third-Party Consultant is affiliated or of which it is a member, and any person engaged to assist the Third-Party Consultant in the performance of its duties pursuant to this AWC, shall not, without prior written consent of FINRA, enter into any employment, consultant, attorney-client, auditing or other professional relationship with Interactive Brokers or any of Interactive Brokers' present or former affiliates, directors, officers, employees, or agents acting in their capacity as such for the period of the engagement and for a period of two years after the engagement.

Respondent Interactive Brokers agrees to pay the monetary sanction upon notice that this AWC has been accepted and that such payment is due and payable. Interactive Brokers has submitted an Election of Payment form showing the method by which it proposes to pay the fine imposed.

Respondent Interactive Brokers specifically and voluntarily waives any right to claim an inability to pay, now or at any time hereafter, the monetary sanction imposed in this matter.

The sanctions imposed herein shall be effective on a date set by FINRA staff.

## II.

### **WAIVER OF PROCEDURAL RIGHTS**

Respondent specifically and voluntarily waives the following rights granted under FINRA's Code of Procedure:

- A. To have a Complaint issued specifying the allegations against it;
- B. To be notified of the Complaint and have the opportunity to answer the allegations in writing;
- C. To defend against the allegations in a disciplinary hearing before a hearing panel, to have a written record of the hearing made and to have a written decision issued; and
- D. To appeal any such decision to the National Adjudicatory Council (NAC) and then to the U.S. Securities and Exchange Commission and a U.S. Court of Appeals.

Further, Respondent specifically and voluntarily waives any right to claim bias or prejudgment of the Chief Legal Officer, the NAC, or any member of the NAC, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including acceptance or rejection of this AWC.

Respondent further specifically and voluntarily waives any right to claim that a person violated the ex parte prohibitions of FINRA Rule 9143 or the separation of functions prohibitions of FINRA Rule 9144, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including its acceptance or rejection.

## III.

### **OTHER MATTERS**

Respondent understands that:

- A. Submission of this AWC is voluntary and will not resolve this matter unless and until it has been reviewed and accepted by the NAC, a Review Subcommittee of the NAC, or the Office of Disciplinary Affairs (ODA), pursuant to FINRA Rule 9216;
- B. If this AWC is not accepted, its submission will not be used as evidence to prove any of the allegations against Respondent; and



C. If accepted:

1. this AWC will become part of Respondent's permanent disciplinary records and may be considered in any future action brought by FINRA or any other regulator against Respondent;
2. this AWC will be made available through FINRA's public disclosure program in accordance with FINRA Rule 8313;
3. FINRA may make a public announcement concerning this agreement and the subject matter thereof in accordance with FINRA Rule 8313; and
4. Respondent may not take any action or make or permit to be made any public statement, including in regulatory filings or otherwise, denying, directly or indirectly, any finding in this AWC or create the impression that the AWC is without factual basis. Respondent may not take any position in any proceeding brought by or on behalf of FINRA, or to which FINRA is a party, that is inconsistent with any part of this AWC. Nothing in this provision affects Respondent's: (i) testimonial obligations; or (ii) right to take legal or factual positions in litigation or other legal proceedings in which FINRA is not a party.

D. Respondent may attach a Corrective Action Statement to this AWC that is a statement of demonstrable corrective steps taken to prevent future misconduct. Respondent understands that it may not deny the charges or make any statement that is inconsistent with the AWC in this Statement. This Statement does not constitute factual or legal findings by FINRA, nor does it reflect the views of FINRA or its staff.

The undersigned, on behalf of Respondent Interactive Brokers, certifies that a person duly authorized to act on its behalf has read and understands all of the provisions of this AWC and has been given a full opportunity to ask questions about it; that it has agreed to the AWC's provisions voluntarily; and that no offer, threat, inducement, or promise of any kind, other than the terms set forth herein and the prospect of avoiding the issuance of a Complaint, has been made to induce it to submit it.

Interactive Brokers LLC

Respondent

By: Elaine H. Mandelbaum

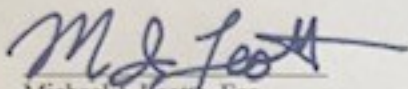
Print Name: Elaine H. Mandelbaum

Title: General Counsel

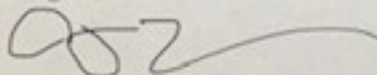
7-28-20

Date

Reviewed by:



Michael J. Leotta, Esq.  
Counsel for Respondent Interactive Brokers LLC  
Wilmer Cutler Pickering Hale and Dorr LLP  
1875 Pennsylvania Avenue, NW  
Washington, D.C. 20006

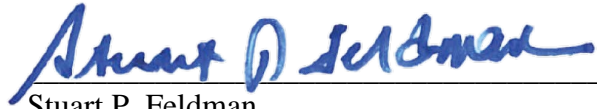


Andrew J. Levander, Esq.  
Counsel for Respondent Interactive Brokers LLC  
Dechert LLP  
Three Bryant Park  
1095 Avenue of the Americas  
New York, NY 10036-6797

Accepted by FINRA:

08/10/2020  
Date

Signed on behalf of the  
Director of ODA, by delegated authority



Stuart P. Feldman  
Senior Counsel  
FINRA  
Department of Enforcement  
Boston District Office  
99 High Street, Suite 900  
Boston, MA 02110

This Corrective Action Statement is submitted by the Respondent. It does not constitute factual or legal findings by FINRA, nor does it reflect the views of FINRA, or its staff.

## **STATEMENT OF CORRECTIVE ACTION BY INTERACTIVE BROKERS LLC**

Interactive Brokers LLC (“IB”) submits this Statement of Corrective Action in connection with the foregoing Letter of Acceptance, Waiver, and Consent (“AWC”) describing the steps it has already taken to correct and substantially reduce the risk of recurrence of the issues addressed by the AWC. As set forth in detail below, IB has invested significant resources to enhance its AML program, and those efforts continue to this day.

**Independent Consultants.** IB has retained several experienced and well-respected consultants and advisors to assist the firm in improving its AML program. In 2018 IB retained Consultant I to conduct a comprehensive review of IB’s AML program and identify areas of focus and improvement for IB’s AML program going forward. IB has accepted all of Consultant I’s recommendations and is in the process of implementing them. IB has also retained Consultant II to conduct assurance work following IB’s implementation of the recommendations resulting from Consultant I’s review. IB retained a third consultant to draft a risk appetite statement and conduct a formal AML risk assessment, and IB has retained an independent firm to conduct its 2019 independent testing of the AML program.

**Hiring and reorganization of AML function.** IB hired new leadership and increased headcount in its AML function. Since the beginning of 2018, the firm has added approximately 80 permanent personnel to its AML and surveillance team (in addition to approximately 35 temporary staff), including many with significant industry and AML experience:

- Chief AML Officer (the function was formerly consolidated with the Chief Compliance Officer) with more than 15 years of relevant experience, including building the Customer Identification Program for a major commercial bank and serving as an AML team lead at another major bank;
- Deputy AML Officer who has been a practicing attorney for fourteen years with four years serving in legal and compliance roles at Nadex, NYSE, and FINRA;
- Head of Sanctions;
- Head of Enhanced Due Diligence;
- Head of Quality Assurance and Training;
- Head of Financial Intelligence Unit;
- Head of AML QA;
- Dedicated AML and Sanctions Counsel;
- Approximately 10 Team Leads (some were promoted from the analyst ranks);
- And dozens of Compliance Analysts.

IB also reorganized its AML program to improve its efficiency and effectiveness. Each AML unit—a QA and Training unit, a Financial Intelligence unit, a Know Your Customer (“KYC”)/Enhanced Due Diligence (“EDD”) unit, a Sanctions and Lists Screening unit, and an AML Risk Assessments unit—now reports to the Chief AML Officer. The Trade Surveillance

unit, which reports to the Deputy Chief Regulatory Officer, also reports to the Chief AML Officer for AML purposes.

**New Case Management System and Surveillance.** IB has developed and is building a customized proprietary case management system, IBKR 360, which allows compliance analysts a holistic view of customer information and activity when they conduct surveillance. The firm has enhanced many of its exception-based surveillance reports and report parameters and is migrating them to IBKR 360. IB LLC retained outside AML consultants to enhance the firm's existing cashiering surveillance reports to address potentially suspicious cashiering typologies. The consultants designed additional report parameters and tuned existing parameters based on their analysis of IB customer data, and IB is in the process of programming and testing the enhancements designed by the consultants.

**Policies and Training.** IB has adopted a new AML policy, completing a risk assessment and risk appetite statement, and developing desktop procedures within each AML team to maintain uniformity in procedure and analysis. These desktop procedures will provide detail on day to day operations aligned with specific tasks, such as conducting investigations and reviewing specific reports. The firm enhanced its standard employee AML training and developed material for additional training of AML and Surveillance Analysts on SAR-filing and AML "red flags." Surveillance Analysts and key New Accounts staff of the firm are becoming CAMS (Certified Anti-Money Laundering Specialist) certified.

**Governance.** Various committee and working groups meet regularly to monitor IB's progress in achieving its goals and to discuss ongoing, future enhancements. These groups include the following:

- AML Advisory Committee – the AML Advisory Committee is comprised of the Chief AML Officer, the Chief Executive Officer, the Chief Financial Officer, the Chief Regulatory Officer, the Deputy Chief Regulatory Officer, the General Counsel, the Global Head of New Accounts, and other in-house counsel. During the quarterly meetings, the Chief AML Officer provides metrics on the AML program and notifies its members of progress made in IB's focus areas for improvement. This committee also discusses regulatory findings and progress made in addressing regulatory matters.
- Account Opening Working Group – the Account Opening Working Group consists of the Chief AML Officer, the Head of New Accounts, and several AML and sales related in-house counsel (as well as members of senior management). This working group meets weekly and makes recommendations as to the acceptance or rejection of any correspondent accounts for foreign financial institutions or other complex clients with material negative news or on which the Head of New Accounts would like further guidance. In addition, the working group discusses potential issues related to AML, potential customer processing, appropriate licensing, and customer risks.
- Data Integrity Working Group – the Data Integrity Working Group is composed of the Chief Data Officer, the Chief Regulatory Officer, and the heads of the major programming groups and meets every other week. This working group discusses issues identified related to the inputs into IB's new AML case management system, IBKR 360, and the surveillance reports that it houses to ensure that such issues are resolved in a timely and efficient manner.

**Risk Ranking and Enhanced Due Diligence.** IB has implemented a Customer Risk Ranking Program designed to capture the overall AML risk posed by individual customers considering a variety of factors. IB has also implemented an EDD program tied to the Customer Risk Ranking Algorithm that subjects certain IB customers to heightened scrutiny both at account opening and on an ongoing basis.

**Restrictions on Certain High-Risk Activity.** The firm is implementing restrictions on money movement designed to mitigate higher risk cross-border and other cashiering activity. The firm has further limited the types of accounts it will accept from high risk countries. The firm also implemented significant restrictions on transfers of U.S. microcap securities in early 2018 and is conducting enhanced surveillance on U.S. microcap securities.