

**Insights**

## **ANTI-MONEY LAUNDERING CONTINUES TO BE AMONG THE HIGHEST REGULATORY PRIORITIES, AS EVIDENCED BY RECENT ENFORCEMENT CASES AND RELEASES**

Jun 04, 2021

For the past decade, anti-money laundering (“AML”) has been at the forefront of securities regulators’ priorities. Indeed, AML enforcement cases have resulted in some of the highest fines imposed by securities regulators, and even the most cursory review of SEC and FINRA annual examination priorities letters reveals AML-related concerns in virtually each of them in the past 10 years.<sup>1</sup> Based on recent enforcement actions and regulatory pronouncements, this focus will continue to be top of mind for regulators<sup>2</sup> and, given the relationship between AML and other headline topics, such as cybersecurity and fraud, broker-dealers should anticipate that future examinations and other regulatory inquiries will heavily focus on AML-related issues. Securities regulators continue to emphasize that any reasonable AML program must be risk-based, and firms should consider periodically conducting a 360° assessment of their AML risks (beyond the annual independent AML testing pursuant to FINRA Rule 3310(c)). At bottom, broker-dealers should be aware of, and be nimble in responding to, cybersecurity and other types of fraud-related developments, and be prepared to modify their AML program in light of their own risk assessments and material developments in the regulatory landscape.

### **Recent SEC And FINRA Enforcement Cases Continue To Result In Significant Fines**

Three recent SEC and FINRA enforcement cases impose significant fines for AML violations. In [GWFS Equities, Inc.](#), a May 12, 2021 SEC settlement, the firm agreed to a censure and \$1.5 million fine. (Read SEC Case No. 3-20298 [here](#).) The case centered on GWFS’ failure to file numerous suspicious activity reports (“SARs”) when it was required to do so during a three-year period. As recounted in the SEC release, and by way of example, in a number of instances employer-sponsored retirement plans contacted the firm to indicate that attempts had been made to withdraw funds from plan participants’ accounts, without authorization. The firm’s AML Compliance Officer (“AMLCO”) and other relevant firm personnel were notified of the underlying attempted account takeovers, but the firm did not file SARs in these instances. In total, the AMLCO and other firm personnel were notified of 130 separate fraudulent transactions necessitating a SAR filing, but the firm failed to file a SAR in any of these instances.

The SEC also found that in 297 additional instances, GWFS filed a SAR concerning attempted account takeovers, but failed to identify relevant information in the filing, such as the “who, what, when, where, and why” (or “the 5Ws guidelines”) of the suspicious activity. Instead, the firm filed a SAR in these instances using only generic, template information, such as stating that an unauthorized person had attempted to access a plan participant's account. GWFS also discovered, but omitted from these SARs, the exact method by which fraudsters intended to intercept certain disbursements. In other words, GWFS had in its possession information identifying relevant parties, bank accounts, IP addresses and other relevant underlying facts, but omitted this information from the SAR filings.

For its part, FINRA has likewise brought notable AML enforcement cases in 2021. In the Score Priority Corp. (“SPC”) Letter of Acceptance, Waiver and Consent (“AWC”) released on April 14, 2021, the firm agreed to a \$250,000 fine and an undertaking to retain an independent consultant. ([Read FINRA's Acceptance, Waiver and Consent \(AWC\) No. 2020067466901 here.](#)) This AWC reflects FINRA's continued focus on suspicious transactional activity (as opposed to money movements), along with the continued emphasis that an AML program must be customized to address the particular AML risks on the firm's business platform. SPC is a small (15 representatives) on-line, introducing broker-dealer that provides customers with a low-cost, self-directed web-based trading platform. The firm's business model was designed to attract active day traders. **First**, FINRA found that firm's AML written procedures were not adequate because they did not provide any additional steps to take **after** suspicious trading was detected. **Second**, and more importantly, SPC relied almost exclusively on a manual review of daily trade blotters, which would not detect patterns of suspicious trading across different accounts on the same day or across multiple accounts in either a single day or multiple days. This manual review was particularly problematic given the high volume of trading through SPC. **Third**, SPC also used a manual review process for daily money movements, which again would not adequately identify patterns or trends over multiple days and/or in multiple accounts.

As a result of these deficiencies, FINRA found that SPC failed to identify and respond to suspicious trading by multiple customers who lived in China. These purportedly unrelated customers placed more than 200,000 orders for a total of more than \$1 billion in shares of certain of the same low-priced securities. The AWC also identified other foreign customers with suspicious trading and money movements during a four-year period. In the end, the use of a manual process for review of high volumes of transactions and money movements simply was not reasonable.

In that same vein, on March 3, 2021, FINRA imposed a \$450,000 fine on ITG, Inc. (“ITG”) for, among other things, failing to customize an AML program around a significant number of customers that were foreign financial institutions (“FFIs”). ([Read FINRA AWC No. 2017054643601 here.](#)) The Bank Secrecy Act requires, among other things, that financial institutions establish due diligence procedures and controls designed to detect money laundering in the correspondent accounts of any FFI. According to the ITG AWC, the firm had some 120 FFIs during the period of January 2014

through April 2018. Although ITG's AML procedures recited, albeit in generic language, that the firm would apply specific enhanced due diligence to correspondent accounts of FFIs, the procedures failed to specify what form such enhanced due diligence should take – similarly to GWFS, ITG failed to identify the “5Ws guidelines” of an enhanced review. More problematic, ITG's books and records contained no relevant due diligence information regarding five FFI customer accounts. Coupled with a manual review of daily trade blotters, these serious deficiencies allowed suspicious activities to go undetected and unchecked: during the period of January 2014 through April 2018, at least 30 different low-priced securities presented significant red flags for market manipulation, but the firm took no significant action in response.

## **Regulators Have Also Recently Identified Significant, And Continuing, AML Concerns From Examinations, But The Regulatory Threshold That Triggers Firms' Reporting Obligation Remains Murky**

At the same time the SEC and FINRA released the recent enforcement cases mentioned above, they also issued regulatory guidance presenting findings and observations from their respective examination programs regarding AML-related issues. Specifically, the SEC's Division of Examinations (“DOE”) issued a Risk Alert on March 29, 2021 on the topic of AML and suspicious activity monitoring and reporting. ([Read SEC's Risk Alert here.](#)) While the Risk Alert provided certain wide-ranging observations derived from “examinations of a number of broker-dealers completed during the past several years,” (p. 1, fn. 2) many of these observations are simply collections of concerns identified by the SEC and FINRA in past releases. However, the DOE's recitation of certain standards in the AML area is particularly noteworthy, as they continue to be troubling for firms. Most important is the SAR-filing standard: “a SAR is required if, on the facts existing at the time, a reasonable broker-dealer in similar circumstances would have suspected the transaction was subject to SAR reporting.” (pp. 2-3) (emphasis added). Notably, the DOE does not suggest that a reasonable broker-dealer would have filed a SAR under the same circumstances – only that such a broker-dealer “would have suspected the transaction was subject to SAR reporting.” In other words, a mere suspicion that a SAR may be required is enough to trigger the reporting obligation. This already-confusing standard becomes further befuddling because the DOE Risk Alert also states “[w]hether a broker-dealer has an obligation to file a SAR depends on the totality of facts and circumstances in a particular situation.” (p. 4, fn. 9.) Insofar as SAR filing obligations for broker-dealers are concerned, it is unclear which of these standards broker-dealers should apply. Regardless, it seems the DOE wants firms to err on the side of filing a SAR in any close case, and, to err on the side of including more details rather than fewer in its description of the “who, what, when, where and why” regarding its suspicions.

Further, the DOE's Risk Alert identifies another long-held frustration regarding broker-dealers failing to follow their own policies and procedures. The DOE states, “A broker-dealer's failure to follow its own AML procedures could also constitute a failure to ‘document accurately’ its AML compliance program in violation of Section 17(a) and Rule 17a-8.” (SEC DOE Risk Alert, p. 2, fn. 4.) In other words, by not following its own procedures, a firm may commit a regulatory violation – and a

failure to affirmatively “document accurately” at that! With respect to actual SAR-related exam findings, the DOE clearly does not favor a manual review of transactions or money movements, and further emphasizes that the parameters for the automated monitoring should be closely tailored to the firm’s risk model.

FINRA’s Regulatory Notice 21-03 issued on February 10, 2021 specifically focused on fraud prevention and AML, relating specifically to low-priced securities.<sup>3</sup> Although the information and “red flags” guidance has been provided in prior Regulatory Notices, it is notable that FINRA sees the need to remind firms of fairly widespread issues regarding low-priced securities – nearly 20 years after FINRA’s AML Rule became effective, and after dozens of AML cases involving six- and seven-figure fines imposed during that time. Issuing this Regulatory Alert (which explicitly “does not create any new requirements or expectations for member firms”) coupled with the issuance of Regulatory Alert 19-18 in May 2020,<sup>4</sup> leaves little doubt that FINRA will prioritize AML in its examination and enforcement efforts in the coming years.

## **Cybersecurity And Account Takeover Incidents Are Intertwined With AML Risks**

Lastly, cybersecurity incidents have continued to be major news events.<sup>5</sup> Relevant to the broker-dealer industry, FINRA has observed, in various releases and contexts, that a cyber or hacking event may, itself, be a suspicious activity necessitating the filing of a SAR.<sup>6</sup> In that regard, Bill St. Louis, FINRA’s Senior Vice President of Retail and Capital Markets Groups, recently stated in an April 2021 podcast that account intrusions, account takeovers, and data breaches “likely will be SAR reportable... And that’s something that we pay quite a bit of attention to...” ([Read transcript here.](#))<sup>7</sup>

Customer account takeover (“ATO”) incidents, which involve bad actors using compromised customer information, such as login credentials (i.e., username and password), to gain unauthorized entry to customers’ online brokerage accounts, were the focus of FINRA Regulatory Notice 21-18 issued on May 12, 2021. ([Read RN-21-18 here.](#))<sup>8</sup> FINRA relates that it has been receiving an increasing number of reports regarding ATO incidents. Moreover, FINRA advised that it has also recently encountered instances in which attackers used synthetic identities to fraudulently open new accounts, and then conduct transactions in that account. FINRA notes that, in the event of an ATO, a SAR may need to be filed and/or a Rule 4530 filing made.

## **Takeaways From 2021 Regulatory Actions And Releases**

In light of the numerous regulatory enforcement cases and continued regulatory focus on AML-related issues, broker-dealers should promptly consider doing the following:

- Conducting, on a periodic basis, a complete assessment of the firm’s business (from a 360° standpoint), evaluating the firm’s AML risks in light of the firm’s existing business model and evolving AML regulatory landscape. This review will be separate from the required annual

independent AML testing pursuant to FINRA Rule 3310(c). Such a holistic review will include, among other things, evaluating the types of exception reports the firm uses, as well as the thresholds that cause a trade or money movement to appear on the reports. Depending on the nature of the firm's business model and regulatory history, a firm may wish to consider conducting such a review under privilege.

- In that same vein, regulators have emphasized that firms must conduct a risk-based analysis in creating, implementing and updating their AML programs. Firms should carefully analyze the AML risks created by their evolving customer base, type of securities business and relationships with affiliated entities.
- Ensure that any analysis involving a questionable activity or customer is clearly documented and the standards on which the firm relies when deciding whether to file a SAR are clearly articulated in writing, even if the firm determines no SAR is necessary.
- More broadly, ensure that the AML and cybersecurity procedures employ the "5Ws guidelines," such that if an incident or "red flag" is identified, the necessary next investigative and reporting steps are clearly articulated. Further, any SAR that is filed should contain this basic type of information.
- Eliminate, to the extent possible, performing manual reviews of transactions and money movements. The continued reference to manual reviews and processes in regulatory actions leaves little doubt that the mere existence of these processes may signal that the firm's supervisory and AML systems may not be reasonable.
- In that same regard, eliminate, to the extent possible, any transactions in low-priced securities. Again, the mere existence of any prevalence of such transactions will certainly lead to heightened scrutiny of the firm's AML and overall supervisory processes.

---

1. Regulators' annual reports have gone by different names over the years, but the SEC and FINRA typically release a communication in the first months of a year, identifying their examination priorities for the coming year. Inevitably, these communications also refer to certain trends and findings from past years, which inform the examination priorities for the coming year. ([Read FINRA's 2021 examination priorities report here](#); [read the SEC's 2021 examination priorities here](#).)

2. President Biden's anti-corruption directive on June 3, 2021 to more than a dozen federal agencies will likely impact AML enforcement activities. (See [Biden's Anti-Corruption Vow Could Supercharge Enforcement](#) on Law360.com; subscription required.) Among the agencies given the directive, and likely to receive additional resources, is the U.S. Department of the Treasury's Financial Crimes Enforcement Network, which shares jurisdiction over broker-dealer AML issues with the SEC and FINRA.

3. The title of this Regulatory Notice is: “FINRA Urges Firms to Review Their Policies and Procedures Relating to Red Flags of Potential Securities Fraud Involving Low-Priced Securities.” ([Read RN 21-03 here.](#))
4. The title of this Regulatory Notice is: “FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations.” ([Read RN 19-18 here.](#))
5. See, e.g., <https://www.usatoday.com/story/tech/2021/05/31/jbs-cybersecurity-attack-top-meat-supplier/5285566001/>; <https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html>.
6. Moreover, depending the scope and nature of a cybersecurity or fraud event, a broker-dealer may have a reporting obligation under FINRA Rule 4530.
7. Greg Ruppert, the head of FINRA's National Cause and Financial Crimes Detection Programs, also recounted popular attacks fraudsters are currently using in an April 20, 2021 podcast. ([Read transcript here.](#))
8. The title of Regulatory Notice 21-18 is: “FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts.”

## **RELATED PRACTICE AREAS**

- Securities Litigation and Enforcement
- Broker-Dealer and Investment Advisor Regulatory Enforcement, Disputes and Investigations



## MEET THE TEAM



**Jeffrey A. Ziesman**

Kansas City

[jeff.ziesman@bclplaw.com](mailto:jeff.ziesman@bclplaw.com)

+1 816 374 3225



**Shea O. Hicks**

St. Louis

[shea.hicks@bclplaw.com](mailto:shea.hicks@bclplaw.com)

+1 314 259 2659



**Shannon M. Wheaton**

St. Louis

[shannon.wheaton@bclplaw.com](mailto:shannon.wheaton@bclplaw.com)

+1 314 259 2296

---

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon ([kathrine.dixon@bclplaw.com](mailto:kathrine.dixon@bclplaw.com)) as the responsible attorney.



Cookiebot session tracker icon loaded