smarsh®

REGULATORY ROUNDUP 2021

A look back at 10 of the most impactful communications oversight violations and penalties

Our Regulatory Update blog series summarizes key FINRA and SEC actions for compliance violations throughout the year. As we review 2021's major fines and infractions, patterns emerge as financial firms across the country solidify their transition to hybrid and remote work.

In this roundup, we highlight:

- **The most impactful fines imposed or actions taken on firms and individuals**
- **Regulatory trends and landscape**
- **Recommendations for supervising digital communications to manage potential risk and liability**

1. CCOs can be held personally liable

- **CCO failed to provide review guidance on digital communication**
- **CCO fined $40,000 and suspended for three months**

A firm's **chief compliance officer was fined $40,000** and suspended by FINRA for "failing to establish a reasonable supervisory system for the review of electronic correspondence and to reasonably review that correspondence."

The findings stated that while at his member firm, the CCO failed to amend the firm's written supervisory procedures (WSPs) and to establish reasonable procedures. This caused the WSPs to fail to specify basic parameters for reviewing digital communications.

The firm's WSPs identified a system to be used for reviewing electronic communications. Unfortunately, the firm didn't provide guidance as to how the system should be used to conduct those reviews. The CCO never reviewed the system containing the firm's Bloomberg messages or chats.

Key takeaway

Chief compliance officers increasingly face personal liability for wrongdoing and regulatory violations as a change of guidelines and a string of enforcement actions have transformed the landscape. Regulators' approach to CCO liability for compliance failures is transforming.

2. Unauthorized outside business activities cause issue for CCO and firm

- **Firm lacked a sufficient WSP on OBAs**
- **Firm fined $50,000**
- **Firm CCO fined and suspended for two months**

FINRA found a firm and its CCO (who was also the firm's president, CEO and only supervisor) failed to establish and maintain a supervisory system. The firm didn't have WSPs designed to achieve compliance with FINRA's outside business activities (OBA) rules.

The findings stated that the firm's WSPs didn't require representatives to provide written notice of their OBAs to the firm. They also failed to address the requirements that the firm review OBAs to determine whether the activity is a private securities transaction — and keep records reflecting the review of OBAs.

The CCO's analysis also failed to provide:

- Criteria for determining if OBAs were appropriate
- Specific conditions or limitations of approved OBAs
- Clarity between OBAs and private securities transactions

FINRA fined the firm $50,000, of which $10,000 is joint and several with the CCO. The CCO was suspended from FINRA for two months.

Key takeaway

Your firm's WSPs must be tailored to the unique risks of the firm and reflect all the activity in which your firm engages. At a minimum, the firm's WSPs should:

- Identify the designated responsible supervisor
- Describe the process the supervisor will follow to conduct each review
- Indicate how frequently such actions will be taken
- Detail how the supervisor will document that the required supervisory steps were taken

3. Regulators continue to crack down on unsupervised social media activity

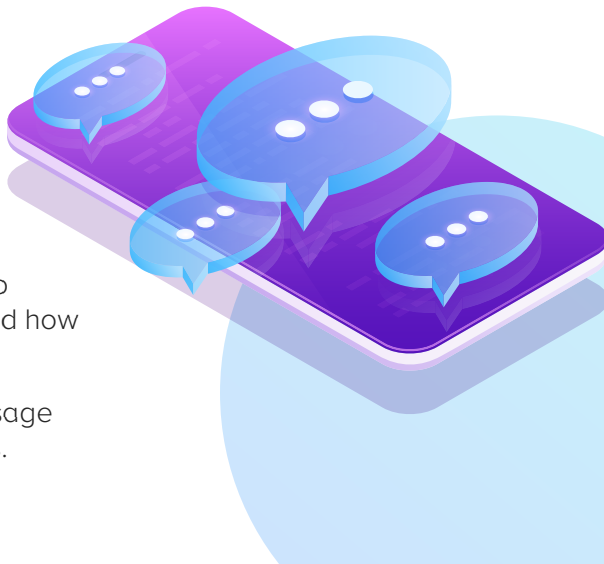
- **Inadequate supervision of registered financial broker's social media use and excessive trading led to meme stock craze**
- **Firm fined $4.75 million**

A U.S. insurance firm agreed to pay a $4.75 million fine to resolve allegations into the social media and trading activity of its employees. The state regulator said the firm failed to detect the activities of their trader, who touted GameStop stock in his spare time while he was working at the company.

State regulators found the firm failed to detect nearly 1,700 trades by the trader, who executed at least two trades in GameStop in excess of $700,000 — beyond the company limit.

Regulators said that while the firm prohibited broker-dealer employees from discussing securities on social media, the company didn't have "reasonable policies and procedures in place to detect and monitor" such activity. Two employees were made aware of his social media activity and the firm didn't take any immediate action, the regulator said.

In addition, the firm inadequately supervised other agents and failed to review their social media usage or catch excessive trading in their personal accounts.



Key takeaway

Regulators are probing how brokerages use social media such as TikTok, Twitter, Instagram, Facebook and other platforms to land new customers. Just last summer, FINRA launched an examination sweep to assess how firms use online "influencers" to promote themselves — and how they protect customer data culled from social media activities.

Firms and advisors should expect regulators to tighten social media usage guidance — along with increased fines and actions taken on violations.

4. Insider trading coordinated with WhatsApp

- **Bank executive and friend used WhatsApp to coordinate insider training**
- **Executive and friend agreed to pay civil penalties of $51,700 and $40,700 respectively**

The **SEC charged a bank executive** and his friend with insider trading. On three occasions, the bank executive tipped off his friend using material, nonpublic information about upcoming acquisitions (two of which involved tender offers).

The executive encouraged communications via WhatsApp because it was encrypted. In a later WhatsApp exchange, the executive urged his friend to buy stock, noting that an upcoming tender offer announcement would be released soon. Responding by WhatsApp, the friend agreed to share the profits of his planned trades.

The executive agreed to pay a civil penalty of $51,700 and the friend agreed to pay a civil penalty of $40,700.

Key takeaway

As employees continue working remotely, compliance concerns inevitably arise. While a prohibition policy may have worked before the pandemic, this is no longer a practical strategy for many businesses. Firms need to proactively stay ahead of recordkeeping and oversight obligations — including capturing and archiving encrypted messages.

5. Unauthorized communications land broker in hot water

- **Broker used personal device and email to forward customer information to work accounts**
- **Broker fined $5,000 and suspended for 45 days**

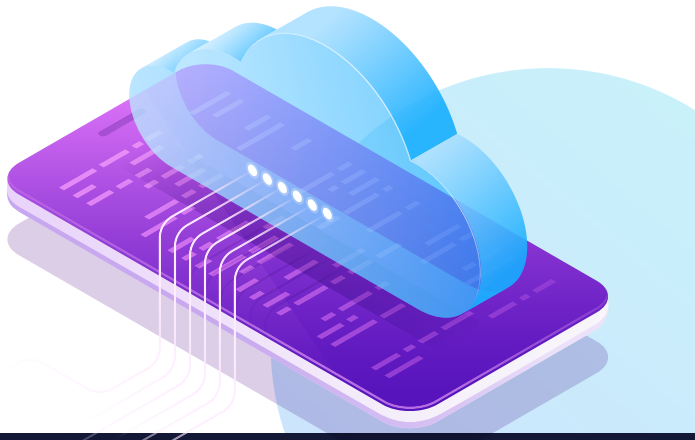
A broker failed to safeguard confidential customer information and was assessed a deferred fine of $5,000 and suspended from association with any FINRA member for 45 days.

With customer consent, a broker used his personal device to capture confidential customer information. The broker then forwarded the information from his personal email account to his firm email account. However, the broker's firm maintained specific policies prohibiting the use of personal email for business purposes and transmitting private client information via email.

The findings also stated the broker exercised discretion in customer accounts without prior written authorization from the customers or approval from his member firm. The findings stated that the customers had verbally authorized the broker to exercise discretion in their accounts.

Key takeaway

This is a clear example of how simply forbidding communication channels in a policy isn't sufficient to protect against recordkeeping rules violations. As we have seen, regulators may fine or suspend a firm and/or broker if they discover a broker uses a communication channel that isn't archived by their firm.



6. Firms continue to get penalized for deficient supervisory systems

- **Firm fined $250,000 for failing to supervise or review solicited transactions**
- **Firm fined $15,000 for failing to supervise and record transactions**
- **Firm fined $450,000 for failing to review MNPIs**

A firm was fined $250,000 for failing to establish and maintain a system to supervise or conduct principal review of solicited transactions. Also, the automated surveillance system, when implemented, wasn't reasonably designed to detect excessive trading and other violative activity.

As a result, the firm failed to supervise a broker who engaged in unsuitable and excessive equity and options trading and used margin in senior customers' accounts. FINRA found that due to an error that occurred when the firm switched internet domain providers, it failed to archive outgoing email communications sent to non-firm email addresses. The emails in question weren't stored in an easily accessible place.

FINRA fined a different firm a total of $450,000, with $90,000 payable to FINRA. The firm failed to reasonably supervise certain types of public and private side employee communications under its policies and procedures. Although the firm had digital communication review procedures in place to detect the disclosure of potential material non-public information (MNPI), those procedures weren't reasonably designed.

In another case, **a firm was fined $15,000** for violating its WSPs by failing to supervise and record on its books and records approximately $1.5 million in private securities transactions. The findings stated that a representative disclosed to the firm that he would be forming a special purpose vehicle for the purpose of making an investment.

The firm didn't request any documents concerning the investment and approved the activity without further supervision of the investment. The firm also didn't update the representative's Form U4.

The representative formed a limited liability company and sold interest in the company to investors — including himself — in the amount of $1,495,438. The firm didn't inquire further about the special purpose vehicle and concluded that the activity didn't constitute a private securities transaction.

As a result of this erroneous conclusion, the firm didn't supervise the private securities transactions or record the transactions on its books and records.

Key takeaway

These enforcement cases are telling examples of how the power of supervision can prevent regulatory infractions. The timely review of digital communications is a first-line defense for firms against improper conduct by employees. It is important to establish a reasonable supervisory system that flags, escalates and enables actions to address potential fraud and violations.

Regulated financial firms must have robust policies and procedures in place — including a policy and system to monitor digital communications — for an effective compliance program. Policies and procedures should be documented to ensure continuing compliance and to serve as a training and reference tool for all employees.

7. Anti-money laundering stays a focus for regulators

- **FINRA lists anti-money laundering as an area of concern in its 2021 Exam Priorities Letter**
- **Firm fined $100,000**
- **General securities principal fined $15,000 and suspended for two months**

FINRA fined a firm $100,000 for failing to establish and implement an anti-money laundering (AML) compliance program to monitor potentially suspicious transactions. The general securities principal was also fined $15,000 and given a two-month suspension.

According to FINRA, the firm and its principal failed to:

1. Take reasonable steps to establish and implement an AML program tailored to the firm's new business line
2. Provide meaningful guidance regarding how the principal was to identify or review red flags specific to the customer account business
3. Take corrective action after becoming aware that the firm's AML compliance officer lacked oversight experience

In addition, FINRA found that the principal "repeatedly" permitted deposits and resales of microcap securities despite missing documentation.

Key takeaway

Anti-money laundering was an area of concern in **FINRA's 2021 Exam Priorities Letter**, and firms can expect this to be a continued focus for 2022.

The retention and supervision of digital communications can proactively flag or provide evidence of AML violations. Compliance teams must be able to monitor employee communications from all channels (email, text message, social media, collaboration and conferencing platforms, etc.), and rely on a supervision solution that will surface only the most relevant content for review.

8. Mobile messages are subject to compliance and supervision regulations

- **Messages sent and received through mobile devices need to be captured and archived**
- **Firm fined $45,000**

The **NYSE fined a brokerage firm $45,000** for failing to supervise the use of personal phones on the NYSE floor. While the phones were properly registered, the firm failed to supervise the use of those phones to communicate by means other than phone calls (e.g., text messages, emails, communication applications).

NYSE found that the firm did not:

- Supervise the use of personal smartphones on the NYSE floor
- Establish and maintain written supervisory procedures and a supervisory system reasonably designed to achieve compliance
- Establish, document and maintain a system of risk management controls and supervisory procedures reasonably designed to manage the financial and regulatory risks of its business activity, including in connection with setting and adjusting credit limits and establishing erroneous order controls
- Demonstrate that its credit limits were reasonable based on customers' financial conditions and trading activity
- Monitor trading for potentially manipulative or otherwise violative activity

Key takeaway

Firms must ensure text messages and other digital records are retained in compliance with applicable recordkeeping and supervision requirements. As firms continue remote work and employees use various messaging applications, compliance risk arises.

Implement archiving technology that can record all smartphone content, including text messages. Archiving software solutions reduce risk for brokers and clients, streamline supervision and compliance activities and protect sensitive firm and client data.

9. Crypto enforcement actions heat up

- **Increasing popularity of cryptocurrency means increased regulatory attention**
- **Cryptocurrency platform fined $6.5 million**
- **SEC filed lawsuit against digital content platform for offering unregistered digital securities**

The Commodity Futures Trading Commission (CFTC) fined a cryptocurrency company $6.5M for delivering false, misleading or inaccurate reports concerning transactions in digital assets

The CFTC alleges that two trading programs operated by company-generated orders traded with each other, which could have misled traders about the trading volume. In addition, the company was fined for "wash trading" Litecoin and Bitcoin transactions conducted by a former employee.

In a separate case, the SEC filed a lawsuit against a digital content platform company for the unregistered offering of securities. The company communicated to investors that the funds raised from the sale of digital assets were to be used to fund business growth and product development.

The SEC seeks a permanent injunction enjoining the company in selling any unregistered securities offerings.

Key takeaways

Recently proposed regulations could present significant compliance burdens for the banks and money service businesses (MSB) that engage in cryptocurrency transactions — especially with FinCEN proposing to impose a reporting and recordkeeping burden on banks and MSBs.

Firms considering the addition of cryptocurrency investment offerings shouldn't overlook the implications for electronic communications regulatory obligations. This entails an assessment of current recordkeeping and supervisory practices to ensure that cryptocurrencies can be controlled, managed and reviewed as an asset class — not just an alternate form of currency.

10. Restricted firms will face increased obligations

- **Rule 4111 became effective January 1, 2022**
- **Rule 4111 follows the same pre-emptive regulatory approach as FINRA's Taping Rule**
- **The public will be able to view which firms are Restricted Firms on the FINRA website**

FINRA adopted Rule 4111 (effective January 1, 2022) to address firms with a significant history of misconduct — or "Restricted Firms."

The new rule allows the self-regulated organization to impose new obligations on broker-dealers with significantly higher levels of risk-related disclosures than other similarly sized peers, based on numeric, threshold-based criteria. A multi-step, annual review process will determine if a Restricted Firm is subject to additional obligations.

Rule 4111 requires Restricted Firms to:

- Deposit cash or qualified securities in a segregated, restricted account
- Adhere to specified conditions or restrictions
- Comply with a combination of such obligations

Key takeaway

This new FINRA rule is positive for the public as it will help protect investors and safeguard market integrity. For brokers, there will be extreme FINRA supervision and examination focused on those on the "naughty list."

Beyond 2022: Supervision is critical for overseeing remote employees

As hybrid and remote work models gain more popularity, digital communication supervision needs to be at the forefront of this transition. Supervisory obligations are only increasing, and FINRA expects member firms to establish and maintain reasonable systems.

Firms must have robust policies and procedures, train employees, engage business leaders and implement a technology solution that includes critical supervision capabilities. This includes flagging keyword lexicons, random sampling, and robust reporting options.

Given that more and more employees are working — and demanding to work — remotely, regulators will take a hard look at firms and individuals who ignore their supervision obligations. Firms and individuals that think of rules and regulations as second tier risk increasingly strict and costly penalties.

Visit our financial services solutions hub to get more information about meeting your specific regulatory obligations.

Subscribe to our blog to keep an eye out for our Regulatory Updates to stay informed of FINRA and SEC updates and actions across the digital communications compliance landscape.

smarsh®

Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals in more than 80 electronic communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

US: 1-866-762-7742 | UK: +44 (0) 20 3608 1209 www.smarsh.com @SmarshInc SmarshInc Company/Smarsh