firm58

The Evolution of Compliance

Why Broker Dealers Need to Renew Their Regulatory Vows

A Firm58 Whitepaper

June 2016

As technology sparks more complexity and versatility in the capital markets, new avenues for unethical and illegal trading practices continue to emerge, while political pressure on Wall Street increases in the wake of the 2008 crisis. Broker dealers' Chief Compliance Officers (CCOs) are coming under increased scrutiny, and for the first time new regulatory proposals threaten to hold them personally accountable for illegal trading activity at their firms.[1]

Over the last two decades, capital markets compliance has evolved from reacting to simple discrete events in a floor-centric world, to addressing intricate, multi-asset, multi-event scenarios in a electronic high-speed, high frequency trading environment. This new paradigm introduces challenges (and opportunities) around big data—and the pressure to search for patterns in a constantly shifting landscape—as well as firms' overall cultural values.

Compliance teams no longer enjoy the benefit of a small pool of compliance concerns, and must simultaneously juggle a variety of competing issues, including:

CYBERSECURITY

Securing digital platforms is a recurring problem, and one that will only become more critical as virtually all business processes are or will soon be digitized.

DATA TRANSPARENCY

Firms don't always collect the right data, and even when they do, broker dealers need to aggregate the data in specific ways in order to be able to parse that information to derive meaning. Mid-market broker dealers generally can't recruit dedicated teams of analysts, but strategic software investments can make the difference between simply retaining and acting on order/execution data.

CULTURE

Institutional culture is a major theme influencing the SEC and FINRA's recent exam priorities; broker dealers must structure incentives and penalties to encourage responsible trading activity. This doesn't necessarily mean trying to keep up with the largest market players in terms of technology, but firms do need to work within their capabilities. Compliance blunders are often costly, and preventative investments easily outweigh punitive fees. In fact, FINRA estimates that since 2010 broker dealers have sunk $300 billion into compliance costs as a result of "cultural failures".[2]

Broker dealers' reputation and success will hinge on their ability to adjust to new industry regulations—through both simple changes and more comprehensive reforms—in the coming months and years. The largest firms with resources to address these issues will have an easier path; however small and mid-sized (SMB) broker-dealers must employ a patchwork of internal resources and external vendors to protect from these growing threats and answer the demands of regulators.

Regulatory compliance is less a matter of educating broker dealers on new or complex rules and processes; most firms already understand what they need to do, or what they cannot do, but struggle to balance effective execution and oversight against budgetary concerns and business conditions. Broker dealers must review their IT security efforts, data management methods and regulatory exam focus, ensuring that compliance is a business priority.

Cybersecurity

On the surface, broker dealers appear well protected against cybersecurity threats, but frequent attacks paint a different story. Analysis from the Office of Compliance Inspections and Examinations found that even though 93 percent of broker dealers conduct internal cyber risk assessments, (and 84 percent review their vendors' security), 88 percent have suffered cyberattacks.[3] Broker dealers are clearly taking steps to address cybersecurity, but too often those measures are incomplete or ineffective. Firms' awareness of cybersecurity risks can only go so far: they have to take meaningful action to address their vulnerabilities and keep up with growing threats. Brian Vazzana, Director of Information Systems & Assurance Services at BDO, sees cybersecurity becoming more crucial, "Cybersecurity has been a hot topic over the past few years and isn't necessarily showing signs of waning among various industries. It's extending beyond simple questions of, 'do you have a firewall,' and 'are you conducting penetration testing?'

"Several widely accepted cybersecurity frameworks are available to companies, including the National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure as well as International Organization for Standardization (ISO), Information Security Management—ISO/IEC 27001. The AICPA's Assurance Services Executive Committee and Audit Standards Board are also currently working on cybersecurity criteria as well as examination engagement guidance in compliance with current attestation standards, which should support various frameworks," Vazzana explained.

Lacking internal expertise, many broker dealers conduct cybersecurity reviews without a solid grasp on the security concepts they investigate. As a result, it's common for firms (large and small) to collect information on features that are irrelevant to a vendor's product while ignoring (whether intentional or not) crucial security considerations. When organizations find defects in their own systems or a partner's defenses, there's often no follow-up to see if those issues were ever addressed. At the risk of reducing the process to a formality (not to mention a waste of time and resources), broker dealers must 'reboot' their cybersecurity review practices.

While the largest broker dealers have the resources to address this issue, middle-market broker dealers simply lack resources to address the concerns—they need a

smarter, cost effective solution. A slim majority (58%) of firms have invested in cybersecurity insurance, but this is just a bandage, not a long-term solution.[4] It's important for firms to invest in relationships with IT consulting organizations familiar with the industry. All of the national and regional accounting firms have cyber-security practices. Firms like BDO are aggressively marketing their services to the industry and have a wide range of solutions for firms regardless of size.[5] Competent security consultants can be the difference between threat recognition and proactive measures that protect your firm, and your clients, from much greater risk.

Data Transparency

In recent months, the SEC and FINRA have voiced concern that broker dealers' surveillance and compliance systems aren't collecting the information organizations need to detect illegal activity.[6] Particularly with regard to anti-money laundering efforts, red flags around wire transfers, name and address changes and more are often lost in the shuffle. This, paired with the industry-wide push toward a consolidated audit trail has forced broker dealers to re-examine their data management practices. Case in point: FINRA recently fined a broker dealer $2.6 million for failing to retain critical records in an immutable format.[7]

Comprehensive data transparency tools, complete with cross-system pattern analyzation and automated reporting, are still new and available at a price point feasible for only the largest firms. The largest, full-service vendors in this category include NASDAQ-Smarts, Nice-Actimize and Sungard-Protegent. These vendors target and are best suited for the largest institutions. SMB broker dealers should continue to pursue conventional, targeted compliance solutions rather than holding out for a silver bullet. Firms specializing in trade surveillance and compliance (such as Firm58), personal trading surveillance, affirmations and certifications, gift tracking, case management (such as Schwab Compliance Technologies), or anti-money laundering (such as Lexis-Nexis), are well suited for the SMB broker-dealer market.[8 9]

Simply hoarding an unorganized data dump might allow for wrongdoing to be discovered via spreadsheets or verified long after the fact, but offers no preventative, or T+1 power. Nor does it address changing industry guidelines or best practices that the vendors mentioned above will provide. Conversely, sparsely collecting data allows for more intensive analysis, but may leave critical records behind. No recordkeeping system will be perfect, but it's important to extract value from what information your organization already collects. Where possible, firms should implement automated controls to monitor and detect irregularities.

Broker dealers should also use the trade analysis tools available to them to identify risks on a per-employee level. Rather than attempting to analyze every record at once, targeted, automated warnings can help direct compliance staff toward the issues that warrant more thorough investigations. It's important that broker dealers invest in surveillance and compliance solutions that can organize data in a meaningful way; no compliance strategy will be effective in the face of terabytes of unstructured data.

A Culture of Compliance

The SEC is reallocating exam resources to focus more on investment advisers, but broker dealers aren't off the hook by any means.[10] To compensate for the SEC's directive, FINRA continues to tighten its brokerage oversight, and its 2016 exam objectives largely mirror the SEC's own. Despite efforts to instill compliance into company culture, many broker dealers undervalue the importance of regulatory exams and certifications. In the past, exams were viewed as a one-time commitment, but an emerging paradigm focuses on continuing education. Many firms don't keep track of employee licenses as well as they should, focusing instead on revenue-generating activity. However, this is easily addressed and doesn't require any special tools; firms can simply use a spreadsheet to keep track of staff.

Broker dealers understand the importance of compliance and market transparency, but many treat regulatory exams as a distraction from business development and client-facing activities. Organizations should view exams from the perspective of reputation management, where tangible benefits are difficult to calculate but costs can become immediately apparent. The reputational and financial damage of a regulatory misstep can be tremendous, while, for example, the costs of tracking and encouraging broker dealers to remain up to date on their exams is miniscule in comparison.

Some firms invest in tracking software, but generally speaking broker dealers aren't lagging behind on their qualification exams due to a lack of resources—this is an HR and culture issue. Broker dealers need to look beyond immediate profitability and incorporate employee training into their approach toward risk management. Many industry-focused compliance-consulting firms can be a key part of a successful strategy. Firms such as Compliance Risk Concepts or Navigator Consulting Group, among others, can provide important insight and introduce processes, bringing a wealth of implementation knowledge and third party solution partners that address these complex requirements.[11] [12] The potential costs of noncompliance (reputational and client attrition) far outweigh the benefits, and firms need to ensure they're not promoting a culture that values short-term gain over long-term profitability.

Nearly two decades later, capital markets are still feeling the impacts of decimalization of spreads, digitization of trading, and fragmentation of markets. Broker dealers must engage third party providers like the ones previously mentioned to not only adapt to organically evolving market conditions, but also address frequently updated regulations. Compliance is a fundamental component of risk management, and broker dealers must learn to adapt their business models to protect against fraud, client disclosure, financial penalties and reputational damage.

Sound compliance does not need to be predicated on sophisticated, cost-prohibitive systems or firm size. Cross-analyzing data from different sources is challenging, but there are available tools to help firms dive deep into the information they collect through their existing surveillance platforms. By combining human expertise with technology, broker dealers can ensure more targeted compliance efforts.

Cybersecurity, data transparency and a healthy culture present both major opportunities and challenges for broker dealers. Organizations largely know what they need to do, but skirt best practices in the drive to remain competitive and profitable. This approach risks firms' financial stability and reputation in exchange for short-term benefits, and will become an increasingly unpalatable avenue as regulatory complexity assuredly increases

Compliance shouldn't be viewed as a cost center; it can provide an advantage over less-prepared competitors. Staying ahead of the curve bolsters your firm's reputation, reduces risk and helps to more easily attract talent. And though the SEC and FINRA may be turning to more stringent individual accountability penalties for compliance pitfalls, capital markets compliance remains a firm-wide responsibility. Broker dealers will find that strong compliance-oriented technology, processes and culture are crucial to future success.

SOURCES

1 Glazer, Emily. "The Most Thankless Job on Wall Street Gets a New Worry," 11 February, 2016. ***http://www.wsj.com/articles/now-in-regulators-cross-hairs-bank-compliance-officers-1454495400***

2 Waddell, Melanie. "FINRA to Examine BDs for Conflicts of Interest," 18 February, 2016. ***http://www.thinkadvisor.com/2016/02/18/finra-to-examine-bds-for-conflicts-of-interest?slreturn=1463608980***

3 Office of Compliance Inspections and Examinations. "National Exam Program Risk Alert, Volume IV, Issue 4," 3 February, 2015. ***https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf***

4 Ibid.

5 BDO, "Cybersecurity Strategy and Solutions," ***https://www.bdo.com/services/consulting/cybersecurity/overview***

6 Goodman, Kevin. "Anti-Money Laundering: An Often-Overlooked Cornerstone of Effective Compliance," 18 June, 2015. ***https://www.sec.gov/news/speech/anti-money-laundering-an-often-overlooked-cornerstone.html***

7 Rosenman, Katten. "Broker-dealer fined $2.6 million by FINRA for failure to retain key records in WORM format," 22 November 2015. ***http://www.lexology.com/library/detail.aspx?g=80a1814f-c3ae-4517-afeb-003c0fc04a41***

8 Firm58, "Compliance and Surveillance," ***https://www.firm58.com/our-products/compliance-and-surveillance/***

9 Schwab Compliance Technologies, "Employee Monitoring," ***http://corporateservices.schwab.com/public/corporate/employee-monitoring/technology***

10 Schoeff, Mark. "SEC to boost Finra oversight as self-regulator takes bigger role in broker exams," 29 March, 2016. ***http://www.investmentnews.com/article/20160329/FREE/160329923/sec-to-boost-finra-oversight-as-self-regulator-takes-bigger-role-in***

11 Compliance Risk Concepts, "Compliance Services," ***http://compliance-risk.com/***

12 Navigator Consulting Group ***http://www.navigatorconsultinggrp.com/home.html***

ABOUT FIRM58

Firm58 helps capital markets firms become more efficient by leveraging the back office for post-trade process improvements. With our solutions, businesses benefit from lower staffing requirements, better compliance and simplified processes for fees and commissions.

To learn more about Firm58, visit our website at **firm58.com**.