GFMI
GLOBAL FINANCIAL MARKETS INSTITUTE

Article **2021**

COVID-19 – A Year Later: The Evolution of Compliance in an Expanding Universe of Know Your Know Yours!

by William Jannace, GFMI Instructor

COVID-19 – A Year Later: The Evolution of Compliance in an Expanding Universe of Know Your Know Yours!

Background

A former U.S. Defense Secretary responded to a U.S. Department of Defense news briefing question in 2002 about the lack of evidence linking the government of Iraq with the supply of weapons of mass destruction to terrorist groups about known knowns; "there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know."[1] One thing we do know; the financial services industry is highly regulated and oversighted; is highly automated and interconnected – making it increasingly vulnerable to cybersecurity threats,[2] and is operating in a world of expanded digitalization, data, and innovation. This perfect storm has and will continue to impact the role of compliance in firms and has changed in many jurisdictions the focus of regulation from prescriptive and reactive to proactive and interactive (i.e., the significant increase post-2008 Credit Crisis in "Sandboxes"[3] and similarly related regulatory innovation hubs).[4]

As discussed in more detail below, this "Regulatory Détente" may be a path forward for the increasingly complex market-regulatory ecosystem to work in a concerted manner to maintain customer protection and market integrity.

While it is still too early to predict how the financial services industry will fully emerge post COVID-19 Pandemic ("the pandemic") one thing is certain-the remit of compliance has expanded from a rules and compliance-based discipline to an evolving hybrid model of Know Your Rules and Know Your Substance with a panoply of "Know Yours" iterations in between -some standalone and some subsets of the traditional ones. The pandemic added an additional dimension of complexity to a broker-dealer's supervisory requirements under FINRA and SEC rules and regulations, but evolving trends in which it operates present increasingly more permanent challenges - the necessity to establish and maintain policies and procedures to comply with rules and regulations in an ever more complex and challenging environment-driven by technological change (e.g., artificial intelligence) and technological challenges (e.g., cybersecurity risks). With the continued use of artificial intelligence and machine learning in conjunction with algorithmic trading strategies,[5] i.e., "Know Your Model" is an emerging regulatory issue as algorithmic trading presents for example the "Black Box problem" for firm's compliance staffs. While human beings can input data into a model and can examine the outputs, the process between the start and finish can be opaque. The lack of model transparency coupled with an algorithm's levels of "explainability," will potentially affect firms, and their compliance officer's ability to understand how a model affects operational risk management. [6] While regulators have issued guidance and promulgated rules[7] with respect to algorithmic trading and the supervision and control practices for firms engaging in algorithmic trading strategies, the guidance was focused more on process, technology, and compliance. [8]

Similarly, Environmental Social and Governance ("ESG") investing and attendant concerns about greenwashing,[9] compliance[10] is being challenged not only to apply the rules and regulations to a firm's supervisory structure but is being tasked with a better understanding of the underlying business product, i.e., "Know Your Substance. [11] ESG regulatory concerns are not limited to financial services firms' customer relationships, but in fact are concerns to these firms' own Enterprise Risk Management ("ERM"),[12] with the "greening" of ERM being driven by shareholder stewardship initiatives and governance proposals[13] and regulatory initiatives such as The Network for Greening the Financial System.[14]

In May 2021, the Biden administration issued an executive order to strengthen the U.S. financial system against climate-related risks. [15] The order instructs the U.S. Treasury Department to work with the other members of the Financial Stability Oversight Council ("FSOC") to report how they plan to reduce risks to financial stability, by improving climate-related financial disclosures to better measure their potential exposure. The order also provides for the development of a "Whole- of-Government Approach"[16] to mitigate climate-related financial risk, by requiring the National Climate Advisor and the Director of the National Economic Council to develop, within 120 days, a comprehensive government-wide climate-risk strategy to identify and disclose climate-related financial risk to government programs, assets, and liabilities. This strategy will identify the public and private financing needed to reach economy wide net-zero emissions by 2050.[17]

While firms have viewed for example, legal, compliance, financial and operational risks as traditional components of their ERM utilizing Value at Risk ("VaR")[18] as a risk management tool, today they are beginning to view (and potentially may be mandated) these traditional indica through a broader prism of ESG and climate risk. For example, the implementation of "Climate VaR"[19] to address the potential to find "Green Swans" in the financial system has been recommended as a means of addressing climate related ERM risk. In addition, there has been increased focus on Data Privacy and Cybersecurity through regulatory guidance[20] and by companies seeking to appoint data and cyber[21]and climate competent boards through the establishment of more diverse boards driven in part by shareholder demands.[22] Companies and boards are recognizing the need to embrace the benefits of diversity at the board level particularly when change is required such as the need to address climate change, and cyber risk[23]. For example, The National Association of Corporate Directors (NACD), commissioned a Blue-Ribbon Commission to explore building and maintaining a strategic-asset board, focusing on issues such as board composition and diversity, succession planning, board-evaluation processes, and ongoing director-skills development.[24] Despite demands for more climate competent boards, progress has been slow and there remains work to be done.[25]

The Convergence of Data and Cybersecurity Risk

The exponential use of data, vendors that generate and sort data, and the increased automation of financial services firms' business and compliance processes, highlights two important and interrelated concerns: cybersecurity[26] and data governance, quality[27] and integrity. The more that data is automated, the more it is susceptible to cyber hacking[28] and cyber ransom. The more

data firms are awash in it, the more concerns there are about its integrity. e.g., false positives on money laundering transaction monitoring.[29]

Regulatory Guidance During the Pandemic

With certain limited exceptions,[30] a broker-dealer is generally provided with some flexibility to design and implement a supervisory system appropriately tailored to and necessary for its businesses and structures.[31] During the pandemic, brokerage firms implemented teleworking arrangements for their staffs. In addition to the added complexity of this situation, the issue of data integrity and cybersecurity – due to the more disaggregated way firms are operating – is also a continuing risk for firms which predates the pandemic.[32] In 2020, FINRA published guidance that addressed, among other things, the supervisory obligations of member firms that used remote offices or telework arrangements" in response to the pandemic.[33] These arrangements may have resulted in registered representatives working in a different environment (e.g., at their homes instead of in their office), and supervising many remote locations may have presented significant challenges or unique considerations that do not exist when supervising non-remote locations. As a result, the use of remote offices or telework arrangements during a pandemic may necessitate a member firm to implement other ways to supervise its associated persons who changed their work locations or arrangements for the duration of the pandemic.[34]

Regulatory guidance also focused on firms assessing whether their remote supervision procedures appropriately address concerns that may be exacerbated when employees are working remotely, such as those involving cybersecurity.[35] Cybersecurity has and continues to be an issue for all financial services firms and their defenses – while being assessed and augmented may still need further funding prioritization.[36] In addition, the 2021 Report on FINRA's Examination and Risk Monitoring Program highlights, among other priorities, cybersecurity.[37]

Further, in 2020, the SEC published a COVID-19 Risk Alert to share observations from its work and provided observations and recommendations to assist firms' pandemic responses.[38] In addition to the cybersecurity recommendations in the COVID-19 Risk Alert, it published two cyber-specific risk alerts in conjunction with its heightened focus in this area since the onset of the pandemic. Its 2020 ***Ransomware Risk Alert*** highlighted the risk and provided observations regarding ransomware attacks, which occur when perpetrators hack into a victim's computer system, seizing control and encrypting data, then demand compensation (a ransom) in exchange for maintaining the integrity and/or confidentiality of customer data, or for the return of control over the firm's system(s).[39]

In addition, in 2020, the SEC issued its ***Credential Compromise Risk Alert*** highlighting observations and responses to credential stuffing attacks, which exploit the tendency for people to reuse their passwords across multiple websites and systems, by cyber attackers who obtain lists of previously compromised usernames, email addresses, and corresponding passwords from the dark web in an attempt to log in and gain unauthorized access to a customer account.[40] These risk alerts built on a special report published in 2020 on ***Cybersecurity and Resiliency Observations*** that highlighted the importance of strong cyber-hygiene and protections.[41] Cybersecurity and related issues continue

to be an SEC priority in 2021 as it advised that it would work with firms to identify and address information security risks, including cyber-attack related risks, and encourages market participants to actively and effectively engage regulators and law enforcement in this effort.[42]

The FINRA 2019 Risk Monitoring and Examination Priorities Letter [43] identified topics that FINRA would continue to review the adequacy of firms' cybersecurity programs to protect sensitive information, including personally identifiable information. FINRA had the prior year published its ***Report on Selected Cybersecurity Practices – 2018,***[44] providing additional information on practices that may help firms strengthen their cybersecurity programs to make their compliance efforts more efficient, effective and risk-based. FINRA also noted that it would engage with firms to understand how they are using RegTech tools and addressing related risks, challenges, or regulatory concerns – including those relating to supervision and governance systems, third-party vendor management, safeguarding customer data and cybersecurity. FINRA published its 2021 ***Report on FINRA's Examination and Risk Monitoring Program*** highlighting it focus on, among other things, cybersecurity, and Anti-Money Laundering ("AML").[45]

Trends in Data

Today data has grown exponentially. The International Data Corporation ("IDC") forecasts that by 2025 the global datasphere will grow to 163 zettabytes (a trillion gigabytes), which is 10 times the data generated in 2016. This necessitates adequate data governance procedures and policies.[46] Data can be a source of significant competitive advantage; if it is timely, relevant, verifiable, and personalized to meet a variety of stakeholder requirements. However, it is easy for firms to become overwhelmed by the volume and complexity of unstructured data, and the inability to understand and interpret it.[47]

Data Integrity

Evolving compliance and operational risk management challenges for financial services firms are related to the governance and control environments specific to the data that is relied upon to ensure that they continue to meet an expanding list of ongoing regulatory and compliance requirements aimed at customer protection, market integrity and increasingly climate risk in the future More transactions equal more data. As transaction volumes have increased exponentially over the last several years, the amount of data being created and stored by broker-dealers has increased accordingly. This data often exists and cuts across many platforms – some sophisticated, some not so much. These can include antiquated proprietary systems, third party vendor systems, End User Computing ("EUC") platforms and spreadsheets, emails, word documents, etc. [48]

Data Governance

Proper data governance is vital for banks and financial services companies, due to increasing frequency of data breaches and increasing regulatory oversight.[49] Data governance also helps financial services organizations understand their data; is essential to protecting that data and to helping comply with government and industry regulations. Financial service companies have a

need for robust data governance due to the nature and volume of the data held.[50] Data governance is also an important aspect of corporate governance and compliance today with KYD as equally important to firms as KYC,"[51] with several iterations in between.

Data governance and loss prevention protocols can be used to protect customer and firm information privacy.[52] If a financial institution has strict controls over who can access and use sensitive data, it can better ensure that it not lost, misused, or accessed by unauthorized users or that its' integrity is compromised. This is particularly important with personal data that is used in AML/KYC reviews.[53] Data governance frameworks should help to make data more consistent, accurate and complete – thereby improving data quality- a vitally important requirement for further integration and acceptability of ESG investing-a source of complaints by various stakeholders in this area. [54] Implemented correctly, a better approach to data management should also lower compliance risk, including the risk of regulatory fines and sanctions.

To promote consistency and uniformity in ESG practices, the Open-Source Climate Initiative (OSCI) was established with the goal of creating an open-source data common, providing easier access for anyone seeking information on companies' environmental performance. It is planning to develop a repository of tools that investors and regulators can use to perform climate risk "scenario analyses" and to help companies establish a path to net-zero emissions.[55] This may be helpful to firms in complying with their Regulation Best Interest (Regulation BI)[56] requirements in connection with the recommendation of ESG products and to regulators in their examinations of firms for compliance with Regulation BI.

There can be a variety of sources of "Bad Data"[57] such as: mergers & acquisitions,[58] additional new databases, EUC risks, new product launches, siloed data sources across an enterprise, legacy systems that don't talk to new systems, a lack of budget to clean up inaccurate data entry, IT transformation and migration, and human error. Proper data governance practices can improve performance, alleviate internal issues pertaining to data, prevent potential data breaches, and mitigate compliance and regulatory exposure.[59] Alternatively, weak data governance can make it difficult to get consistent data for screening for example for OFAC/AML[60] compliance purposes,[61] resulting in duplicate records and duplicate alerts - diverting compliance resources; or, for merged companies, each database was built for its own business purpose and not for compliance, therefore, creating issues when brought together for compliance purposes. The holistic view of data that results from a strong data governance initiative is becoming essential to regulatory compliance. According to a 2017 survey by Erwin Inc. and UBM, 60% of organizations said compliance drives their data governance initiatives.[62] Remember, a firm's compliance and supervisory systems are only as good as the integrity of the data it receives and reviews.

Trends in Surveillance

Increasingly Web and social media data, (including Facebook, Twitter, LinkedIn), and blogs are increasingly the focus of financial services compliance and technology efforts.[63] In this regard, financial services companies now try to integrate this data with other information such as outside business activities and private securities transactions to obtain a more holistic profile of their

employees; and it is part of a trend towards more integrated surveillance. This is part of the evolving trend in the *three lines of defense*[64] of supervision.[65] To the extent that the three lines of defense support ERM, (as noted above there has been a focus on viewing risk through a broader prism of ESG and climate related risk)-perhaps we will soon have the "Green Lines of Defense" or add sustainability to the traditional three lines of defense and have a fourth line, to reflect specific governance features of regulated financial institutions, [66] (which as noted above is becoming more ESG and climate-centric in its focus).

Trends in Alternative Data

In addition, as regulatory requirements and market developments have commoditized aspects of traditional sell-side research, investment firms are repurposing aspects of their business to function as data aggregators and distributors for their hedge fund clients using drones, spatial recognition and mapping tools formulated to take advantage of temporal and price arbitrage opportunities in volatile markets.[67] For example, a hedge fund may use this capability to process information relating to weather and commodity prices. This real-time data needs to be governed. Other examples include following "meme" stocks[68] and trading patterns on social media, such as Twitter and Instagram feeds, commercial market indicia such as "web luminosity" (the number of citations a company receives on its products and brands in reviews, social media and other web content; and its relationship with that company's fundamentals and stock performance.[69] It is worth noting that "meme" stocks have already received their own "Know Your" designation – Know Your Meme Stock ("KYMe") in guidance issued about regulatory trends in this area.[70] It has been reported that the SEC is reviewing existing rules[71] and considering new rules for "Apps" that "Gamify" trading,[72] in addition to actions it has already taken.[73]

While providing benefits to certain market participants, alternative data also poses potential legal and regulatory[74] risks for firms that utilize it including: anti-hacking issues; breach of contract and terms of use; copyright infringement; misappropriation; potentially inappropriate use of nonpublic personally identifiable information; inadequate policies and procedures to prevent violations in connection with the potential use of material non-public information ("MNPI");[75] and reputational risk-risk associated with inappropriate sourcing, vetting, or use of the data. Given such risk, firms should implement third-party due diligence procedures[76] that include due diligence questionnaires and – if necessary – dialogue with vendor(s) to address any potential gaps, including appropriate representations and warranties to address risk mitigation. Such policies on alternative data should permit the use of alternative data only after a vetting and authorization process has been conducted and documented by a firm's legal and/or compliance department.

Evolving Data-Market Trading Ecosystem

The capital markets ecosystem is comprised of several groups: issuers, buy-side and sell-side firms, high-frequency traders ("HFTs") and hedge funds, among others. Increasingly, hedge funds and HFTs utilize machine learning and AI[77] to improve investment results, i.e., generate alpha. AI generates data. Approximately 20 billion Internet of Things (IOT) devices are online currently and by 2025, is expected to reach 75 billion devices. In addition, there are expected to be 4.8 billion

internet users by 2022, up from 3.4 billion in 2017. It is estimated that 80% of data will be unstructured-text centric: dates, numbers, and facts, not in a pre-defined manner.[78] In addition, such funds also utilize alternative data in their investment decision process;[79] and in some instances, this alterative data can be obtained without contacting an issuer – presenting investment ideas for market participants but challenges for the issuers.[80]

Compliance Requirements and Trends

Today, many post-crisis prudential policies have been implemented, and banks for example are better capitalized with more liquidity than they were pre-crisis. Banks and other financial services companies have been increasingly more focused on:

- culture and governance;
- the challenges and opportunities from new technology and innovation generally;[81] and
- emerging economic, market, and operational risks.

They are addressing the above concerns through an expanded universe of Know Your requirements. The Know Yours have evolved from the traditional ones to many that are an outgrowth of technological and financial innovation. The traditional Know Yours have been impacted by the financialization of the world economy and the increased flow of illicit finance.[82]

For example:

- Know Your Customer ("KYC"); and related suitability requirements[83];
- Know Your Country ("KY Country");[84]
    - Know Your Product[85] ("KYP");[86]
    - Know Your Entity ("KYEn"); [87]and related AML concerns[88]

Other traditional ones such as Know Your Rules have been impacted by the expansion of rules and regulations requiring more interaction with regulators, hence:

- Know Your Rules ("KYR");
    - Know Your Regulator ("KYRr");[89]
    - Know Your Needs ("KYN");[90]

Data and technological driven changes have shifted some of the emphasis from the traditional Know Yours to the below subset:

- Know Your Employee ("KYE");
    - Which also has implication for addressing cybersecurity and other related regulatory issues such as insider trading;
- Know Your Data ("KYD");
    - Data Governance[91]

- Know Your Vendor ("KYV");[92]
- Know Your Auditor ("KYA");
- Know Your Model ("KYM");
- Know Your Substance ("KYS");[93]

Lastly, given the depth and breadth of the recent executive order issued to address climate risk, perhaps the next iteration of Know Yours will include:

- Know Your Climate ("KYCe");
- Know Your Environment ("KYEt");
- Know Your Emissions ("KYEs");

Regulatory Détente

As the saying goes, "if you cannot beat them, join them." As the fintech industry continues growing globally, issues continue to come to the forefront of regulation. To address regulatory barriers to the fintech industry - and to take a more proactive approach to regulation - innovation hubs and regulatory sandboxes have been established.[94] By way of background, the first regulatory sandbox was set up in the UK in 2016. Since then, the Financial Conduct Authority (FCA),[95] has interfaced with groups of firms and supported them in reducing the time and cost of getting to market while learning about their technology-driven conduct.[96]

A sandbox is a tool that allows developers to test a technological proof of concept prior to a full-scale public release. This enables a firm the ability to amend and improve a product iteratively based on feedback *before* significant resources are invested in a project. In a regulated sector such as financial services, this iterative approach can be difficult for firms to replicate, particularly for startups which typically lack the regulatory approvals and capital needed to conduct real-world tests. By allowing new firms to experiment with real customers in a regulatory sandbox, regulators expect to disincentivize the tendency of firms to engage in regulatory arbitrage by relying on gaps in rules and regulations or permissive regulatory structures and/or jurisdictions to conduct their business. The sandbox enables firms to enter the financial services market and to experiment with new ideas with a degree of regulatory oversight and support. They also have potential benefits for more established firms that are looking to launch new products that do not fit easily within the structure of existing financial services regulation.[97]

Regulatory Sandboxes are increasingly common since first established by the FCA. The Global Financial Innovation Network (GFIN) was formally launched in January 2019 by an international group of financial regulators and related organizations, including the FCA. Its focus is to discuss and develop policies regarding financial technologies; and to help develop a "global sandbox" that will offer firms an environment in which to trial cross-border solutions. This built upon the FCA's 2018 proposal to create a global sandbox.[98] The US SEC, CFTC, OCC, and FDIC have signed onto the GFIN. [99]

During the Saudi Arabian Presidency of the G20, the Bank for International Settlements (BIS) Innovation Hub launched the G20 TechSprint Initiative to highlight the potential for new technologies to resolve regulatory compliance (RegTech) and supervision (SupTech) challenges. The BIS Innovation Hub - through its Singapore Centre, and the Saudi Arabian G20 Presidency had published high-priority RegTech/SupTech operational problems and invited private firms to develop innovative technological solutions.[100]

In December 2020, the SEC announced that its Strategic Hub for Innovation and Financial Technology, commonly referred to as FinHub, would become a stand-alone office. It was initially established within the Division of Corporation Finance in 2018, and it had spearheaded SEC efforts to encourage responsible innovation in the financial sector, including in evolving areas such as distributed ledger technology and digital assets, automated investment advice, digital marketplace financing, and artificial intelligence and machine learning. Through FinHub, market and technology innovators as well as domestic and international regulators have been able to engage with SEC staff on new approaches to capital formation, trading, and other financial services within the parameters of the federal securities laws.[101]

FINRA's Office of Financial Innovation (OFI) is the central point of coordination for issues related to significant financial innovations by FINRA member firms, particularly new uses of financial technology. To achieve this, OFI initiates outreach with various stakeholders, disseminates research and publications, and collaborates with other regulators on matters related to financial technology by identifying and analyzing emerging trends in the securities industry. [102]

The Financial Crimes Enforcement Network (FinCEN) in 2020 began hosting "Innovation Hours" enabling financial technology/regulatory technology companies, and financial institutions to have the have opportunity to present innovative product, services, and approaches to enhance AML/CFT efforts. The FinCEN Innovation Hours Program is an element of FinCEN's Innovation Initiative, which it is using to enhance national security through the promotion of responsible financial services innovation that furthers the purposes of the Bank Secrecy Act ("BSA"). It is intended that private sector innovation-new ways of using existing tools or by adopting new technologies- can help provide new and more efficient means of providing financial services to consumers and businesses, help financial institutions enhance their AML compliance programs and contribute to more effective and efficient record keeping and reporting under the BSA framework. [103]

What Has Changed and Why Now is the Time to Rethink the Regulatory-Industry Dynamic

Leading up to the financial crisis of 2008 (the "Crisis") to some degree, systemic risk emanated from the interconnectivity of individual firm's idiosyncratic risks arising from the degree of counter party transactions and related extensions of credit between firms and their customers. These customers with other firms-were overlapping risk without any individual firm able to see the entire profile of their customers' transactions and risk exposure- with their industry competitors. While

these firms had in place risk management processes and tools such as VaR, they were, with exceptions,[104] unable to truly gauge potential systemic risk building in the system leading up to the Crisis. Prior to the Crisis, a focus on regulation had been on front-office/sales practice issues. i.e., KYC and suitability. The post-Crisis focus was to a greater extent more concentrated on financial and operational risk, funding and liquidity risk, market structure and operational integrity,[105] continuity, and resiliency, with an acknowledgement to the limits of disclosure to protect investors.[106]

So, what has changed? One can say that the traditional risk paradigm of the financial services industry engaging in overreach and lax ERM poses systemic risk, but today the risk to the industry appears to be more exogenous than endogenous. Unlike the Crisis of 2008, which started in the U.S. financial system and spread globally, the next crisis to the financial system may be the result of an external and unforeseeable shock(s) to system.[107] Climate change, stranded assets,[108] environmental losses, cybersecurity, cyber hacking,[109] and ransomware are threats not solely attributable to the industry's own doing and cannot be addressed without working with industry competitors,[110] regulators,[111] and other stakeholders.[112]

Within firms, the compliance function may be forced to expand its remit by functioning through a more ESG-Sustainability centric prism, whether by regulation or out of necessity. While numerous iterations of potential Know Yours have been discussed there is potentially some issue or risk that may slip through the various apertures of even the most comprehensive ERM program. While expanding the universe of Know Yours in a compliance program may be seen as a granular accretive approach to ensure compliance there are other means to address the burgeoning growth of risk, and regulatory responses to such risks. In addition to climate competent boards and related board committees, the idea of conflating climate risk and compliance into a single role or department may be worthy of further discussion. Today's Chief Compliance Officer ("CCO"), with its stature and visibility is an outgrowth of regulatory issues arising a few decades ago whereby regulators addressed those issues by, among other things, imposing new registration and qualification requirements[113] on CCOs and requiring them to participate in meaningful interactions with their Chief Executive Officers ("CEOs") in connections with certifications they are required to make to regulators. [114] A Chief Climate- Compliance Officer (CCCO) or Chief Sustainably and Compliance Officer (CSCO) designation may be worthy of further discussion by regulators and the financial services industry.[115] This COVID pandemic raised parallel issues of data integrity to support reasonable supervision and compliance particularly during this period. The exponential rise of data has, and will, continue to pose compliance risks and challenges on an ongoing basis – which is the known known. The degree of industry-regulatory cooperation is also to a large extent a known known. The extent that it will *continue to grow* is a known unknown. While not "joining them" the burgeoning growth of Sandboxes and Innovation Hubs *does* indicate that both stakeholders in the financial services ecosystem realize there is more to be gained by cooperating with each other than on working at cross purposes. While this form of "Regulatory Détente" -a known known- may not be the perfect path forward in an increasingly complex market-regulatory ecosystem that is vulnerable to shocks both sides cannot fully predict nor combat, it is a way to work synergistically rather than antagonistically. Perhaps, with the benefit

of time and experience, the next and best Know Yours may be “Know Your Sandbox” and (Really) “Know Your Regulator”-with both responding to industry challenges by firms staffed with more cross-disciplined compliance-climate staffs. Without that, we default to a situation of unknown unknowns-where all stakeholders will be at a disadvantage and unable to even address known knowns, to the detriment of our markets and the investing public.

About the Author: William Jannace

William "Bill" Jannace has over 30 years of professional experience in the securities industry, having held positions at the American and New York Stock Exchanges and FINRA as well as being an adjunct professor, instructor and lecturer at various schools of higher learning, both domestically and abroad. This article represents the views and opinions of the author and does not reflect the views of any organization he is associated with or any banking or securities regulator.

He is an adjunct professor at Fordham School of Law, Baruch College-CUNY, Georgetown Global Education Institute, Wharton Business School, U.S. Army War College, and Metropolitan College. He has delivered courses to 11 schools over the past 20 years. His main areas of expertise include Broker-Dealer, Investment Company, and Adviser Regulation; Efficient Market Theory; Proxy Rules; M & A and Tender Offers; Corporate Governance; Environmental, Social, Governance (ESG) and Impact Investing Sovereign Wealth Funds; State Capitalism, and Geopolitics/Geo-Economics.

Bill was the Director and Counsel of FINRA's (f/k/a NYSE Regulation) Sales Practice Policy department responding to interpretive, policy and disposition requests. He supervised a staff of professionals responsible for writing rules and amendments to rules and providing interpretive guidance to NYSE and FINRA staff and members regarding sales practice rules. Bill also coordinated policy responses to new products and services (e.g., Private IPO market, bank sweeps) and business models (crowd funding). In his FINRA career, Bill participated in the Regulatory Expert program regarding Research, AML, MSRB and Internal Controls violations as well as participated in FINRA-industry committee meetings and industry outreach programs and supporting FINRA-IOSCO initiatives and its MOUs with foreign regulators.

Before joining FINRA, Bill was an Enforcement Attorney with the American Stock Exchange, where he concentrated on broker-dealer regulatory and compliance issues, and options and equity sales practice and trading violations.

Previously, he worked with the Legal-Compliance Departments of TD Securities and Smith Barney providing legal advice on Regulation D/S offerings/144A/144 resales/10b-18 share buybacks; Offering Memorandums/Underwriting and Prime Brokerage Agreements; and ensuring trade reporting/Control Room/employee/firm trading compliance.

When Bill was an account executive at Georgeson & Co. and D.F. King & Co., Inc. – proxy-solicitation firms – he liaised for corporations and institutional shareholders regarding corporate governance issues and proxy fights; and liaised with trading floor and arbitrageurs to provide market color to listed companies.

In addition to his work in the US, Bill has participated in several training programs for foreign stock exchanges and lectured abroad, including seminars for the Russian Securities Commission

and Stock Exchange; Kenyan Capital Markets Authority; East African Securities Regulatory Authority; Saudi Arabian Capital Markets Authority; Taiwan Stock Exchange; and several other international authorities and securities commissions. He is also involved in the social-philanthropy/impact investment market in the Balkans, Caucasus and other countries in East Africa and the Middle East.

Instructional Experience

New York Law School: Adjunct Professor of Law
Securities Training Corporation
NYU: School of Continuing & Professional Studies: Lecturer
Baruch College: Division of Continuing Studies: Instructor
Adelphi University School of Continuing Education: Instructor
New York Society of Security Analysts: Instructor
Pace University: Adjunct Professor

Professional Designations

LL.M Corporate, Banking and Securities Law: Fordham University School of Law - New York
JD: New York Law School
BA, Economics: New York University

Bar Admissions

New York and Connecticut bars

Professional Affiliations

ACAMS - Certified Anti-Money Laundering Specialists
FINRA Certified Arbitrator
Fellow, Charted Institute of Arbitrators

Speaking Engagements

Bill has delivered numerous speaking engagement, covering topics on: Securities Regulation, Market Structure, Clearance and Settlement and Corporate Governance, to these groups:

- Chinese Securities Regulatory Commission
- China Construction Bank
- Iraq Stock Exchange
- Securities and Exchange Bureau of India
- Tokyo Stock Exchange

- Hawkamah Institute for Corporate Governance
- Kenyan Capital Markets Authority
- El Salvador Securities and Exchange Commission
- Ghana Stock Exchange
- Mexican Banking and Securities Commission
- Sarajevo Stock Exchange/Securities Commission
- Saudi Arabian Capital Markets Authority
- Central Bank of Kosovo
- Malaysian Securities Commission
- SEC Annual Institute for Securities Market
- US State Department Foreign Delegation
- Hong Kong Securities Commission
- Philippine Dealing System Holdings
- Treasury Department of Argentina
- Ontario Securities Commission
- Securities Operations Forum
- ALI-ABA Compliance and Enforcement Conference
- ABA Conference

Publications

"A New World Order: The Rule of Law, or the Law of Rulers?" William Jannace and Paul Tiffany, 42 Fordham Int'l L.J. 1379 (2019). Available at: https://ir.lawnet.fordham.edu/ilj/vol42/iss5/2

"Bretton Woods 4.0 Finding New Relevance in a New World Order," By Dr. Paul Tiffany and William Jannace, Bretton Woods@75 Blog and Compendium, February 2019.

"Cautionary Notes for Supply Chain Managers and Others Involved in Global Sourcing & Partnerships (Human Trafficking & Modern Slavery Conditions Raise Reputational Risks)," Governance & Accountability Institute, January 2018.

"Sustainability Disclosures in the EU," Insights, The Corporate and Securities Law Advisor, Volume 31, Number 8, August 2017.

"Sustainability Disclosures in the EU: Implementation of the 2014 EU Non-Financial Reporting Directive," ABA, Spring 2017.

"Accounting for Trade: President Trump and the Geopolitical Balance Sheet," NYU-Global Affairs Perspectives on Global Issues, Spring 2017.

"NASD/NYSE Rule Harmonization: What Do the Changes Mean in Practice, "The Journal of Securities Compliance, Volume One, October 2007.

23 Maytime Ct
Jericho, NY 11753
+1 516 935 0923
www.GFMI.com

References

[1] http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

[2] See Cyber Risk is the New Threat to Financial Stability, for statistics and trends on incidents and the amount of data at risk from such incidents, https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/.

[3] https://dfsobservatory.com/content/regulatory-sandboxes

[4] According to the World Bank ("WBG"), regulators globally have embraced the regulatory sandbox as a "means of providing a dynamic, evidence-based regulatory environment to test emerging technologies." The WBG collated the total sandboxes currently in existence both announced and operational and highlighted some metrics on their design and operations. It noted that there are currently 73 Sandboxes operating globally in 57 jurisdictions. https://www.worldbank.org/en/topic/fintech/brief/key-data-from-regulatory-sandboxes-across-the-globe.

[5] https://www.sec.gov/files/Algo_Trading_Report_2020.pdf.

[6] For example, GPT-3, is a natural-language computer model that learns to write and speak. It is an example of AI that can better understand and interact with the world. While it can mimic human text, it does not understand what it is writing as it has been trained on internet text-misinformation and biases and produces such misinformation and biases. https://openai.com/blog/gpt-3-apps/.

[7] FINRA Rule 1220(b)(4)(A) requires each person associated with a member to register as a Securities Trader if such person is: (i) primarily responsible for the design, development or significant modification of an algorithmic trading strategy relating to equity, preferred or convertible debt securities; or (ii) responsible for the day-to-day supervision or direction of such activities. For purposes of this Rule an "algorithmic trading strategy" is an automated system that generates or routes orders (or order-related messages) but shall not include an automated system that solely routes orders received in their entirety to a market center. https://www.finra.org/rules-guidance/rulebooks/finra-rules/1220. See also https://www.finra.org/sites/default/files/Regulatory-Notice-16-21.pdf.

[8] FINRA provided guidance on effective supervision and control practices for brokerage firms and market participants that use algorithmic strategies. The practices are focused on five general areas: General Risk Assessment and Response; Software/Code Development and Implementation; Software Testing and System Validation; Trading Systems; and Compliance. https://www.finra.org/rules-guidance/notices/15-09. See also https://www.finra.org/rules-guidance/key-topics/algorithmic-trading.

[9] https://www.sec.gov/files/esg-risk-alert.pdf.

[10] Under the Investment Adviser Compliance Rule, it is unlawful for an investment adviser registered with the SEC to provide investment advice unless the adviser has adopted and implemented written policies and procedures reasonably designed to prevent violation of the Advisers Act and the rules thereunder by the adviser or any of its supervised persons. The Compliance Rule requires advisers to consider their fiduciary and regulatory obligations under the Advisers Act and to formalize policies and procedures to address them. Release No. IA-2204, Compliance Programs of Investment Companies and Investment Advisers (Dec 17,2003). https://www.sec.gov/rules/final/ia-2204.htm.

[11] Compliance personnel that are knowledgeable about the firms' specific ESG-related practices. The SEC observed that, where compliance personnel were integrated into firms' ESG-related processes and more knowledgeable about firms' ESG approaches and practices, firms were more likely to avoid materially misleading claims in their ESG-related marketing materials and other client/investor-facing documents. The compliance personnel in these firms appeared to: provide more meaningful reviews of firms' public disclosures and marketing materials; test the adequacy and specificity of existing ESG-related policies and procedures, if any (or assess whether enhanced or separate ESG-related policies and procedures were necessary); evaluate whether firms' portfolio management processes aligned with their stated ESG investing approaches; and test the adequacy of documentation of ESG related investment decisions and adherence to clients' investment preferences (ESG Risk Alert). https://www.sec.gov/files/esg-risk-alert.pdf.

[12] Deloitte's global risk management survey, 12th edition, noted the growing concern over climate risk and increasing attention on the social responsibility of business, with 47% of respondents indicating that it will be an extremely or very high priority for their institutions to improve their ability to manage ESG, including climate risk ("Deloitte Survey"). https://www2.deloitte.com/us/en/insights/industry/financial-services/global-risk-management-survey-financial-services.html.

[13] The proxy advisory firm Institutional Shareholder Services recommends including reference to risk oversight as part of its criteria for choosing when to recommend withhold votes in uncontested director elections. Specifically, in cases where companies are targeted in connection with public "vote-no" campaigns, evaluate director nominees under the existing governance policies for voting on director nominees in uncontested elections. Take into consideration the arguments submitted by shareholders and other publicly available information. Examples of failure of risk oversight include but are not limited to bribery; large or serial fines or sanctions from regulatory bodies; demonstrably poor risk oversight of environmental and social issues, including climate change; significant adverse legal judgments or settlement; or hedging of company stock. https://www.issgovernance.com/file/policy/active/americas/US-Voting-Guidelines.pdf.

[14] In December 2017, eight central banks and supervisors (now currently 83 members and 13 observers) established a Network of Central Banks and Supervisors for Greening the Financial

System (NGFS), to help strengthen the global response required to meet the goals of the Paris agreement and to enhance the role of the financial system to manage risks and to mobilize capital for green and low-carbon investments in the broader context of environmentally sustainable development. https://www.banque-france.fr/en/financial-stability/international-role/network-greening-financial-system.The NGFS published an "Overview of Environmental Risk Analysis (ERA) by Financial Institutions," which provides a list of examples of how environmental risks are transmitted to financial risks, and a review of the tools and methodologies for ERA used by financial institutions: including banks, asset managers and insurance companies. The NGFS also published an Occasional Paper, "Case Studies of Environmental Risk Analysis Methodologies," to provide a comprehensive review of the tools and methodologies for ERA used by some financial institutions including banks, asset managers and insurance companies. https://www.ngfs.net/sites/default/files/medias/documents/case_studies_of_environmental_risk_analysis_methodologies.pdf.

[15] https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/20/fact-sheet-president-biden-directs-agencies-to-analyze-and-mitigate-the-risk-climate-change-poses-to-homeowners-and-consumers-businesses-and-workers-and-the-financial-system-and-federal-government/

[16] In March 2021, the Federal Reserve Board (FRB) announced that it had created a Financial Stability Climate Committee (FSCC) to identify, assess, and address climate-related risks to financial stability. The FRB previously announced the establishment of a new Supervision Climate Committee (SCC) to strengthen the FRB's capacity to identify and assess financial risks from climate change and to develop a program to ensure the resilience of supervised financial institutions to those risks. The SCC's micro-prudential work is intended to ensure the safety and soundness of financial institutions and constitutes one core pillar of the FRB's framework for addressing the economic and financial consequences of climate change. The FSCC, in contrast, will examine the macro-prudential aspects of climate change, including the potential for climate-generated economic shocks and how climate change could exacerbate these shocks and cause broader impacts that could harm households, businesses, and communities. The FSCC will also coordinate with the SCC and FSOC to develop an integrated approach to climate change risk. https://www.federalreserve.gov/newsevents/speech/brainard20210323a.htm. https://www.newyorkfed.org/newsevents/news/aboutthefed/2021/20210125. On March 17, 2021, the Commodity Futures Trading Commission (CFTC) announced the establishment of an interdivisional Climate Risk Unit (CRU) to assess the risks to US financial stability posed by climate change. https://www.cftc.gov/PressRoom/PressReleases/8368-21. On Mar 4, 2021, the SEC announced the creation of an Enforcement Task Force Focused on Climate and ESG Issues to proactively identify ESG-related misconduct, with an initial focus on identifying any material gaps or misstatements in issuers' disclosure of climate risks under existing rules. The task force will also analyze disclosure and compliance issues relating to investment advisers' and funds' ESG strategies. https://www.sec.gov/news/press-release/2021-42.

[17] https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/20/fact-sheet-president-biden-directs-agencies-to-analyze-and-mitigate-the-risk-climate-change-poses-to-homeowners-and-consumers-businesses-and-workers-and-the-financial-system-and-federal-government/

[18] Value at Risk measures the potential loss in value of a risky asset or portfolio over a defined period for a given confidence interval. It is sometimes defined more narrowly as the possible loss in value from "normal market risk" as opposed to all risk, requiring distinctions between normal and abnormal risk as well as between market and nonmarket risk. Value at Risk has been used most often by commercial and investment banks to capture the potential loss in value of their traded portfolios from adverse market movements over a specified period compared to their available capital and cash reserves to ensure that the losses can be covered without putting the firms at risk. http://people.stern.nyu.edu/adamodar/pdfiles/papers/VAR.pdf.

[19] Climate Value-at-Risk (Climate VaR) is designed to provide a forward-looking and return-based valuation assessment to measure climate related risks and opportunities in an investment portfolio. The fully quantitative model offers deep insights into how climate change could affect company valuations. https://www.msci.com/documents/1296102/16985724/MSCI-ClimateVaR-Introduction-Feb2020.pdf/f0ff1d77-3278-e409-7a2a-bf1da9d53f30?t=1580472788213.

[20] In 2018, the SEC published new guidance regarding public company disclosures about cybersecurity risks and incidents. The guidance consolidated and expanded upon the SEC's prior guidance on disclosure obligations relating to cybersecurity. The guidance provided additional insights instructive to public companies regarding: (1) the materiality of a cybersecurity risk or incident, (2) the timing of disclosures relating to a cybersecurity incident, (3) disclosures about board oversight, (4) insider trading, (5) cybersecurity policies and procedures, (6) cybersecurity assessments, and (7) regulatory and litigation risk. https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[21] According to the Gartner 2020 Board of Directors Survey, cybersecurity-related risk is rated as the second-highest source of risk for the enterprise, following regulatory compliance risk. However, relatively few directors feel confident that their company is properly secured against a cyberattack. To ensure that cyber risk receives the attention it deserves, many boards of directors are forming dedicated committees that allow for discussion of cybersecurity matters in a confidential environment, led by someone deemed suitably qualified. According to the survey, by 2025, 40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from less than 10% today, and that by 2025, 50% of asset-intensive organizations will converge their cyber, physical and supply chain security teams under one chief security officer role that reports directly to the CEO. https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-

[22] CalPERS has raised the need for climate change competence in the boardroom. Hedge funds such as TCI Fund Management have indicated its expectations for the Boards of the companies it invests in as well. https://www.calpers.ca.gov/docs/forms-publications/governance-and-sustainability-principles.pdf. https://www.tcifund.com/ESGEngagements. Comptroller Stringer Launches Boardroom Accountability Project 3.0, a First-in-the-Nation Initiative to Bring Diversity to Board and CEO Recruitment. https://comptroller.nyc.gov/services/financial-matters/boardroom-accountability-project/boardroom-accountability-project-3-0/

[23] Why the focus is shifting to boards on cybersecurity. https://www.ft.com/content/c70caa94-2d88-3ece-b802-79e9bac2f32c.

[24]https://www.nacdonline.org/about/press_detail.cfm?ItemNumber=26610.

[25] According to a study by New York University's Stern Center for Sustainable Business, only 7 per cent of board members were "climate competent." The study analyzed the biographies of 1,188 board members at the 100 largest U.S. companies, and three (0.2%) directors had specific climate expertise, and only 6 per cent had broader environmental experience. This dearth of climate competent board members is concerning because since the beginning of 2020, the number of the largest companies with a net-zero emissions target has tripled to at least 1,500-with few firms having a detailed plan for reaching those targets. https://www.ft.com/content/611522b7-8cf6-4340-bc8a-f4e92782567c. See also U.S. Corporate Boards Suffer from Inadequate Expertise in Financially Material ESG Matters, NYU Stern School of Business Forthcoming, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3758584.

[26] The Deloitte Survey noted that while institutions have faced cyberattacks for several years, the threat has grown with many employees working at home. Only 61% of respondents considered their institutions to be extremely or very effective at managing cybersecurity risk, and 87% said that improving their ability to manage cybersecurity risk will be an extremely or very high priority over the next two years. https://www2.deloitte.com/us/en/insights/industry/financial-services/global-risk-management-survey-financial-services.html.

[27] In it 2016 Annual Exam Priorities Letter, FINRA noted that it would be examining firms' data governance, quality controls and reporting practices to ensure the accuracy, completeness, consistency, and timeliness of data reported to firm management and to firms' surveillance and supervisory systems. FINRA has observed that operational problems firms experience can originate from data quality and integrity issues, which can undermine a firm's ability to monitor or report key information that is needed to effectively manage its risk and business activities. For example, FINRA has observed problems with firms' automated AML surveillance systems not capturing complete and accurate data, which can result in missed or poor-quality alerts. https://www.finra.org/rules-guidance/communications-firms/2016-exam-priorities.

[28] In February 2016, hackers targeted the central bank of Bangladesh and exploited vulnerabilities in The Society for Worldwide Interbank Financial Telecommunication (SWIFT)

attempting to steal $1 billion. While most transactions were blocked, $101 million still disappeared. This incident was a wake-up call that systemic cyber risks in the financial system had been underestimated. https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf.

[29] This has also placed an added emphasis on Know Your Employee and Know Your Data, which some believe have overtaken KYC as potentially greater risk to corporations, particularly regarding AML Compliance. Increasingly financial institutions desire to improve their data quality and availability through better data governance is often driven by regulations to implement such program to ensure compliance with the requirements for example of NYDFS Superintendent's Regulations Part 504 (NYDFS Part 504). https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsp504t.pdf.

[30] Broker-dealers are all required to have a supervisory structure in place to prevent the dissemination of material nonpublic information. https://www.law.cornell.edu/uscode/text/15/78o. https://www.sec.gov/divisions/marketreg/brokerdealerpolicies.pdf. See also for general supervisory and related requirements FINRA Rules: 3110, 3120 and 3130, https://www.finra.org/rules-guidance/key-topics/supervision.

[31]https://www.finra.org/rules-guidance/rulebooks/finra-rules/3110. See also NASD NTM 99-45, NASD Provides Guidance on Supervisory Responsibilities, https://www.finra.org/rules-guidance/notices/99-45.

[32] https://www.finra.org/sites/default/files/2019_Risk_Monitoring_and_Examination_Priorities_Letter.pdf

[33] See FINRA Notice 20-08, Pandemic-Related Business Continuity Planning, Guidance and Regulatory Relief (Mar. 9, 2020). https://www.finra.org/rules-guidance/notices/20-08. See also SEC Division of Market Regulation, Staff Legal Bulletin No. 17: Remote Office Supervision (Mar. 19, 2004). https://www.sec.gov/interps/legal/mrslb17.htm.

[34] This guidance is similar to that which FINRA issued in 2009 following the H1N1 (swine flu) pandemic. FINRA Notice 09-59, Business Continuity Planning: FINRA Provides Guidance on Pandemic Preparedness (Oct. 12, 2009). https://www.finra.org/rules-guidance/notices/09-59.

[35] https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.

[36] Esther Shein, 80% of senior IT leaders see cybersecurity protection deficits, TechRepublic.com, March 5, 2021. https://www.techrepublic.com/article/80-of-senior-it-leaders-see-cybersecurity-protection-deficits/ The article notes that a lack of confidence in companies' defenses is

prompting 91% of organizations to boost 2021 budgets, according to a new IDG/Insight Enterprises study.

[37] https://www.finra.org/media-center/newsreleases/2021/finra-publishes-2021-report-finras-examination-and-risk-monitoring.

[38] https://www.sec.gov/files/Risk%20Alert%20-%20COVID-19%20Compliance.pdf.

[39] https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf

[40] https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf.

[41] https://www.sec.gov/files/OCIE-Cybersecurity-and-Resiliency-Observations-2020-508.pdf.

[42] In its 2021 Examination Priorities it noted that the SEC will review whether firms have taken appropriate measures to: (1) safeguard customer accounts and prevent account intrusions, including verifying an investor's identity to prevent unauthorized account access; (2) oversee vendors and service providers; (3) address malicious email activities, such as phishing or account intrusions; (4) respond to incidents, including those related to ransomware attacks; and (5) manage operational risk as a result of dispersed employees in a work-from-home environment. Its division of Examinations will also focus on controls surrounding online and mobile application access to investor account information, the controls surrounding the electronic storage of books and records and personally identifiable information maintained with third-party cloud service providers, and firms' policies and procedures to protect investor records and information. https://www.sec.gov/files/2021-exam-priorities.pdf.

[43] https://www.finra.org/rules-guidance/guidance/exam-priority-letters.

[44] https://www.finra.org/media-center/news-releases/2018/finra-publishes-report-selected-cybersecurity-practices-2018.

[45] https://www.finra.org/media-center/newsreleases/2021/finra-publishes-2021-report-finras-examination-and-risk-monitoring.

[46] IDC, Data Age 2025: The Evolution of Data to Life-Critical: Don't Focus on Big Data; Focus on the Data That's Big. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/workforce/Seagate-WP-DataAge2025-March-2017.pdf. https://www.seagate.com/our-story/data-age-2025/.

[47] https://www.perficient.com/industries/financial-services/data-management.

[48] EUC is a system in which individuals can create working applications beyond the divided development process of design, build, test, and release that is generally followed by professional

software engineering teams. Microsoft Excel is one of the most common examples of EUC. EUCs are essential to many financial operations, allowing users to manage and manipulate data quickly and efficiently making EUC appealing and critical to business structures, but also difficult to manage/control. EUC applications are not subject to the same monitoring as traditional applications, and frequently management does not have visibility over how integral the use of EUCs is within the company. Because of this, many of the advantages of EUCs have begun presenting risks to the businesses that rely so much on them. https://www.clusterseven.com/end-user-computing-risk-management/

[49] In FINRA's 2016 Regulatory and Examination Priorities Letter it noted that areas of focus included: firms' supervision and risk management practices related to their technology infrastructure, including the hardware, software and personnel who develop and maintain a firm's information technology systems. FINRA's focus was on firms' supervision and risk management related to cybersecurity, technology management, and data quality and governance. In addition, it remains focused on firms' cybersecurity preparedness given the persistence of threats and our observations on the continued need for firms to improve their cybersecurity defenses. FINRA's reviews focused on firms' approaches to cybersecurity risk management and depending on a firm's business and risk profile: governance, risk assessment, technical controls, incident response, vendor management, data loss prevention and staff training. As part of these reviews, FINRA considered firms' abilities to protect the confidentiality, integrity and availability of sensitive customer and other information, including compliance with SEC Regulation S-P and Securities Exchange Act (SEA) Rule 17a-4(f), the latter of which requires electronically stored records to be preserved in a non-rewriteable, non-erasable format. https://www.finra.org/rules-guidance/communications-firms/2016-exam-priorities.

[50] For example, the aggregation of data from multiple sources for sanctions screening creates the possibility that data integrity issues may arise. A financial service organization should for example, consider establishing processes to ensure source and list data used in the screening process is both accurate and complete. See Wolfsberg 2019 Guidance 3.5 Data Integrity. https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf.

[51] NYS DFS Part 504 requirement: Validation of the integrity, accuracy, and quality of data to ensure that accurate and complete data flows through the Transaction Monitoring and Filtering Program. https://www.dfs.ny.gov/industry_guidance/transaction_monitoring. According to the Harvard Business Review (HBR), poor data quality costs $3 trillion per year in the U.S. https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year.

[52] The SEC has noted the following practices, among others, with respect to data management: Vulnerability Scanning-establishing a vulnerability management program that includes routine scans of software code, web applications, servers and databases, workstations, and endpoints both within the organization and applicable third party providers; Perimeter Security-

Implementing capabilities that are able to control, monitor, and inspect all incoming and outgoing network traffic to prevent unauthorized or harmful traffic; Detective Security. Implementing capabilities that can detect threats on endpoints; Patch Management-establishing a patch management program covering all software and hardware, including anti-virus and anti-malware installation; Inventory Hardware and Software-maintaining an inventory of hardware and software assets, including identification of critical assets and information; Encryption and Network Segmentation-using tools and processes to secure data and systems; Insider Threat Monitoring-creating an insider threat program to identify suspicious behaviors, including escalating issues to senior leadership as appropriate; and increasing the depth and frequency of testing of business systems and conducting penetration tests. https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[53] Data Governance – Understanding its Importance for AML Compliance, December 14, 2018 by Rama Pappu https://www.acacompliancegroup.com/blog/data-governance-%E2%80%93-understanding-its-importance-aml-compliance.

[54] See https://corpgov.law.harvard.edu/2020/09/21/esg-disclosures-frameworks-and-standards-developed-by-intergovernmental-and-non-governmental-organizations/. See also https://news.bloombergtax.com/financial-accounting/bidens-sec-faces-uphill-battle-to-form-esg-reporting-body.

[55] https://expertinvestoreurope.com/is-open-source-the-answer-to-the-climate-data-problem/ https://www.os-climate.org/news/.

[56] https://www.sec.gov/regulation-best-interest.

[57] Gartner, Inc. estimates that enterprises lose about $15 million every year because of poor data quality. https://www.gartner.com/smarterwithgartner/how-to-create-a-business-case-for-data-quality-improvement/

[58] Deloitte's 2018 Banking and Securities M&A Outlook noted that there is reason to believe the Mergers and Acquisitions (M and A) market would increase for financial technology (i.e., fintech) firms. Such transactions result in more data, new applications and processes that must be harmonized with existing systems in some cases all resulting in complexity. The report noted that integrations can be difficult, and there is an increased likelihood of "data sprawl and data silos." Data governance helps organizations better understand the data, and to t discern gaps and redundancies. https://www2.deloitte.com/br/en/pages/financial-services/articles/banking-securities-mergers-acquisitions-outlook-trends1.html.

[59] According to research by IBM, 45 percent of bankers say partnerships and alliances help improve their agility and competitiveness. Financial services data governance can better enable: The personalized, self-service, applications customers want; The machine learning solutions that automate decision-making and create more efficient business processes; Faster and more accurate

identification of cross-sell and upsell opportunities; Better decision-making about the application portfolio, M&A targets, M&A success and more.
https://www.ibm.com/downloads/cas/DAZBRZLM.

[60] Without proper data governance, firms cannot focus on real risk or identify hidden risk. Since 2009, OFAC has issued 181 penalties; each penalty has averaged over $20 million. Penalties and settlement amounts per OFAC enforcement case in 2018 ranged from $88k to $54 million. Source: Finscam. Challenges and Best Practices of PEP & Sanctions Screening Part 1: Importance of Data. www.innovativesystems.com.

[61] In its 2018 Annual Exam Priorities Letter, FINRA noted that FINRA will assess firms' compliance with FinCEN's Customer Due Diligence (CDD) rule, which became effective on May 11, 2018. The CDD rule requires that firms identify beneficial owners of legal entity customers, understand the nature and purpose of customer accounts, conduct ongoing monitoring of customer accounts to identify and report suspicious transactions and, on a risk basis, update customer information. According to its letter, FINRA focused on ***the data integrity of those suspicious activity monitoring systems, as well as the decisions associated with changes to those systems***.
https://www.finra.org/rules-guidance/communications-firms/2018-exam-priorities.

[62] https://go.erwin.com/2018-state-of-data-governance-report.

[63] FINRA's rules on Communicating with the Public; Books and Records; Supervision; Third-Party Posts/Interactive Electronic Forums, Linking to Third-Party Websites, among other activities, apply.
https://www.finra.org/rules-guidance/key-topics/social-media.
https://www.finra.org/sites/default/files/notice_doc_file_ref/Regulatory-Notice-17-18.pdf.
Many FINRA firms rely on Smarsh to help them comply with books and records rules (SEC 17a-3 and 17a-4), the FINRA Communications Rules (2210, 2212–2216), supervision guidelines and ongoing guidance around websites, blogs, and social media.
https://www.smarsh.com/solutions/industries/financial-services/broker-dealers.

[64] The traditional three lines of defense consisted of: (1)-Supervision by Business Personnel-Risk Owners; (2) Independent Risk Management by Compliance and (3) and Independent Audit.
https://www.bis.org/publ/bcbs292.pdf. https://www.bis.org/publ/bcbs195.pdf.

[65] The original Three Lines of Defense model consisted of the first line (risk owners/managers), the second line (risk control and compliance), and the third line (risk assurance). Each line reported up to senior management, with the third line of internal audit representing the last wall before external audit and regulators. The updated model adopts a six-step, principles-based approach. It encourages the governing body to provide delegation and direction to each line, with the lines providing accountability and reporting in return. The roles of the first line ("provision of products/services to clients; managing risk) and second line ("expertise, support, monitoring and challenge on risk-related matters") both fall under management, while the third line ("independent and objective assurance and advice on all matters related to the achievement of objectives") still

lives under internal audit. The model encourages management and internal audit to coordinate response. https://www.complianceweek.com/risk-management/iias-three-lines-of-defense-updated-to-stress-collaboration/29212.article.

[66] For a detailed discussion of expanding the three-lines-of-defense model further to reflect specific governance features of regulated financial institutions. See Isabella Arndorfer, Bank for International Settlements and Andrea Minto, Utrecht University, Occasional Paper No 11 The "four lines of defense model" for financial institutions, Financial Stability Institute, https://www.bis.org/fsi/fsipapers11.pdf.

[67] https://www.msci.com/www/blog-posts/using-alternative-data-to-spot/01516155636.

[68] Recurring volatility in some "meme" stocks highlight the tension between individual investors and short sellers, months after the volatility in GameStop. https://www.reuters.com/business/new-meme-stocks-swing-shorts-retail-investors-face-off-again-2021-04-30/.

[69] https://www.msci.com/www/blog-posts/more-than-a-feeling-quantifying/01541639111.

[70] https://www.kslaw.com/news-and-insights/from-the-chat-room-to-the-board-room-knowing-your-meme-stock.

[71] https://finance.yahoo.com/news/u-sec-chief-plans-scrutinize-183900055.html.

[72] https://www.wsj.com/articles/secs-new-chairman-set-to-field-questions-on-gamestop-archegos-11620306010.

[73] In February 2021, as part of its efforts to respond to potential attempts to exploit investors during recent stock market volatility, the SEC suspended trading in the securities of 15 companies because of questionable trading and social media activity.

[74] In its 2020 Examination Priorities, the SEC highlighted alternative data issues, stating that examinations will focus on firms' use of these data sets and technologies" and that the SEC would assess the effectiveness of related compliance and control functions. Third party vendor management was also another priority, https://www.sec.gov/news/press-release/2020-4. https://www.sec.gov/news/press-release/2021-35.

[75] Under Section 204A of the Investment Advisers Act of 1940, all investment advisers, are required to "establish, maintain, and enforce written policies and procedures reasonably designed, taking into consideration the nature of such investment adviser's business, to prevent the misuse of MNPI. https://www.law.cornell.edu/uscode/text/15/80b-4a. See also Section 15(g) of the Securities Exchange Act of 1934. https://www.law.cornell.edu/uscode/text/15/78o.

[76] In Regulatory Notice 05-48, FINRA advised that outsourcing an activity or function to a third party does not relieve firms of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and FINRA and MSRB rules regarding the outsourced activity or function. Accordingly, firms may need to adjust their supervisory structure to ensure that an appropriately qualified person monitors the arrangement. This includes conducting a due diligence analysis of the third-party service provider. https://www.finra.org/rules-guidance/notices/05-48. See also FINRA Regulatory Notice 18-31 which provides guidance issued by staff of the SEC's Division of Trading and Markets regarding the use of recordkeeping services provided by third parties to preserve records pursuant to SEA Section 17(a) and SEA Rule 17a-4. https://www.finra.org/rules-guidance/notices/18-31. For additional background information, see also Regulatory Notice 11-14 where FINRA requested comment on Proposed New FINRA Rule 3190 to Clarify the Scope of a Firm's Obligations and Supervisory Responsibilities for Functions or Activities Outsourced to a Third-Party Service Provider, https://www.finra.org/rules-guidance/notices/11-14.

[77] Approximately, one-third of Bloomberg News content is generated by some form of automated technology, which can dissect a financial report the moment it appears and generate news story with pertinent facts. Source: NIRI IR Update, Fall 2020 referencing Think Tank Report: "The Disruption Opportunity," December 2019. https://www.niri.org/NIRI/media/NIRI/IRUpdates/2019%20IR%20Update/001157_NIRI_Fall2019_FINAL.pdf.

[78] Source: NIRI IR Update, Fall 2020 referencing Think Tank Report: "The Disruption Opportunity," December 2019. https://www.niri.org/NIRI/media/NIRI/IRUpdates/2019%20IR%20Update/001157_NIRI_Fall2019_FINAL.pdf.

[79]There are approximately 400 percent more alternative data analysts over the last 5 years; 77% of buy-side firms are seeking to or are already using alternative data to inform investment process and strategies; and approximately $901millionn was spent on alternative data sets by 2021 – a growth of 19.2% every year. https://services.google.com/fh/files/misc/generating_alpha_with_google_cloud.pdf.

[80] For example, Aquantix (an AI Vendor) utilizes satellite imagery, weather-station data and regulatory documents scraped from the internet and it can estimate: How much water a business uses at its various sites; the chances of drought or flooding in surrounding areas; and the financial impact such disasters could have—all without contacting the company. Its tool is useful to investors assessing water risk. It notes that at current rates of consumption, demand for water worldwide will be 40% greater than its supply by 2030, with resulting physical, reputational, and regulatory water risk potentially impacting investment returns especially in industries such as food, mining, textiles, and utilities. https://www.f6s.com/aquantix.ai.

[81] While blockchain technology has been embraced by the financial services industry as the technology permits secure transactions to be made without the involvement of intermediaries, making payment systems more efficient and less costly and thereby supporting financial inclusion as a result, it is not however, an unqualified innovative breakthrough. In this regard, there are several issues pertaining to it which firms may have to increasingly address as cryptocurrencies become more integrated into the traditional investment thesis. First, is its nexus to illicit finance. A Wall Street Journal article cited data from Chainalysis, a crypto security company, indicating that in 2020 illicit entities revived approximately $4.9 billion in crypto payments, with the fats growing category being ransomware payments. https://www.wsj.com/articles/cryptocurrency-has-yet-to-make-the-world-a-better-place-11621519381. See also FinCen guidance and proposed rulemaking on crypto currencies. https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual and https://www.fincen.gov/news/news-releases/fincen-extends-comment-period-rule-aimed-closing-anti-money-laundering Secondly, certain cryptocurrencies consume a significant amount of electricity (in some instances as much as a medium size country) raising issues with respect to the environmental impact of such currencies. https://www.ft.com/content/1aecb2db-8f61-427c-a413-3b929291c8ac.

[82] The estimated annual values of illicit financial flows include approximately a minimum of $2.6 trillion from money laundering; between $1.6 trillion to $2.2 trillion from transnational crime: and approximately $ 1 trillion from corruption and bribery. The Shadowy World of Illicit Finance, ACAMS, December 2020, https://www.acamstoday.org/the-shadowy-world-of-illicit-finance/.

[83] https://www.finra.org/rules-guidance/rulebooks/finra-rules/2111.

[84] For additional information on initiatives to address corruption and money, see "Countering Global Kleptocracy: A New US Strategy for Fighting Authoritarian Corruption," by Nate Sibley and Ben Judah, Hudson Institute, January 2021, https://www.hudson.org/research/16608-countering-global-kleptocracy-a-new-us-strategy-for-fighting-authoritarian-corruption. See also "Defending the United States against Russian dark money, " by Anders Åslund, Julia Friedlander, The Atlantic Council, November 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/defending-the-united-states-against-russian-dark-money/.

[85] https://www.finra.org/sites/default/files/Industry/p359971.pdf.

[86] FINRA provided guidance to firms about the supervision of complex products, which may include a security or investment strategy with novel, complicated or intricate derivative-like features, such as structured notes, inverse or leveraged exchange-traded funds, hedge funds and securitized products, such as asset-backed securities. These features may make it difficult for a retail investor to understand the essential characteristics of the product and its risks. FINRA identified characteristics that may render a product "complex" for purposes of determining whether the product should be subject to heightened supervisory and compliance procedures and provided examples of heightened procedures that may be appropriate.

https://www.finra.org/rules-guidance/notices/12-03. It also recommended best practices for reviewing new products. FINRA urged firms to take a proactive approach to reviewing and improving their procedures for developing and vetting new products. At a minimum, those procedures should include clear, specific, and practical guidelines for determining what constitutes a new product, ensure that the right questions are asked and answered before a new product is offered for sale, and, when appropriate, provide for post-approval follow-up and review, particularly for products that are complex or are approved only for limited distribution. https://www.finra.org/rules-guidance/notices/05-26.

[87] On January 1, 2021, the U.S. Congress passed the Corporate Transparency Act (CTA) as part of the 2021 National Defense Authorization Act and under the scope of the Anti-Money Laundering Act of 2020 (AMLA). The passage of the CTA represents a sweeping change to efforts to combat money laundering, terrorism financing, organized crime, and other financial crimes since the passage of the USA PATRIOT Act in 2001. The AMLA establishes a database to facilitate a voluntary public-private information-sharing partnership among law enforcement agencies, national security agencies, financial institutions, and the Financial Crimes Enforcement Network (FinCEN) for such purposes. The AMLA requires the Secretary of the Treasury to promulgate regulations that establish procedures for the protection of information shared and exchanged between FinCEN and the private sector, including information permitted to be given to financial institutions pursuant to the AMLA in connection with the AMLA's purposes. The CTA requires: the establishment of new federal beneficial ownership reporting requirements for certain U.S. domiciled or active entities, including foreign entities that operate in the U.S.: and FinCEN's maintenance of a federal database for the beneficial ownership information collected. https://www.congress.gov/bill/116th-congress/house-bill/6395.

[88] Although suspended in 2019, FINRA's Risk Control Assessment asked firm to provide information on the following: does the AML function have the opportunity to approve new business opportunities, such as new products, customers, channels; does AML function have Individual veto power over the decision to undertake the new business opportunity; does the AML function participate on a committee to approve new business opportunities. https://www.finra.org/sites/default/files/2017_RCA_PDF.pdf.

[89] The SEC has advised that a CCO can be a "value-add" to the business and by keeping up with regulatory expectations and new rules, CCOs can assist in positioning their firms to avoid costly compliance failures and provide pro-active compliance guidance on new or amended rules. https://www.sec.gov/news/speech/driscoll-role-cco-2020-11-19.

[90] The SEC also noted last year that CCOs should be provided with adequate resources, including training, automated systems, and adequate staff, and that some Investment Advisers expect the CCO to create policies and procedures but fail to give them the resources to hire personnel or engage vendors to provide systems to implement those policies and procedures. https://www.sec.gov/news/speech/driscoll-role-cco-2020-11-19.

[91] This is more vital than ever as the prolific use of alternative data has changed the investing and trading landscape. Examples of alternative data include flight trackers, social media posts, credit card transactions, satellite images (crops, slag piles at mines, etc.), Shopping center traffic, foot traffic coordinates, online communities,

product pricing, and geospatial data.
https://services.google.com/fh/files/misc/generating_alpha_with_google_cloud.pdf

[92] The SEC has noted that practices and controls related to vendor management generally include policies and procedures related to: conducting due diligence for vendor selection; monitoring and overseeing vendors, and contract terms; assessing how vendor relationships are considered as part of the organization's ongoing risk assessment process as well as how the organization determines the appropriate level of due diligence to conduct on a vendor; and assessing how vendors protect any accessible client information.
https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[93] https://www.sec.gov/files/esg-risk-alert.pdf.

[94] https://www.mdpi.com/2199-8531/6/2/43/pdf.

[95]The FCA, in 2015, announced the establishment of the 'Regulatory Sandbox,' with references to innovation, preserving regulatory competitiveness globally, and the need to learn about the new technological innovations by regulators. Specifically, it noted that the sandbox was open to authorized firms, unauthorized firms that require authorization and technology businesses that are looking to deliver innovation in the UK financial services market.

The sandbox seeks to provide firms with: the ability to test products and services in a controlled environment; reduced time-to-market at potentially lower cost; support in identifying appropriate consumer protection safeguards to build into new products and services; better access to finance;
https://www.fca.org.uk/firms/innovation/regulatory-sandbox.

[96] https://www.tandfonline.com/doi/full/10.1080/13563467.2021.1910645.

[97] https://www.sidley.com/en/insights/newsupdates/2017/09/fintech-and-regulatory-sandboxes.

[98] https://www.fca.org.uk/firms/innovation/global-financial-innovation-network.

[99] https://www.sec.gov/news/press-release/2019-221.

[100] https://www.bis.org/hub/g20_techsprint.htm.

[101] https://www.sec.gov/news/press-release/2020-303.

[102] https://www.finra.org/rules-guidance/key-topics/fintech.

[103] https://www.fincen.gov/resources/fincens-innovation-hours-program.

[104] https://www.reuters.com/article/us-wallstreet-primebrokers-analysis/prime-broker-ranks-shaken-up-for-good-by-crisis-idUSTRE5AG42I20091118.

[105] https://www.sec.gov/spotlight/regulation-sci.shtml.

[106] https://www.sec.gov/news/speech/the-sec-after-the-financial-crisis.html.

[107] Some have cautioned that due to the degradation to the world's biosphere, the world could be vulnerable to similar outbreaks. https://en.unesco.org/courier/news-views-online/pandemics-humans-are-culprits. In its 2021 ESG Trends to Watch, MSCI noted among other things, that: policymakers and investors will heed the alarm on biodiversity loss, adapting methodologies established for measuring and managing climate risk; and institutional investors may need to report on new ESG metrics for their portfolio companies (e.g., the European Union's ("EU") Sustainable Finance Disclosure Regulation (SFDR)). https://www.msci.com/www/blog-posts/2021-esg-trends-to-watch/02227813256.

[108] It is estimated that approximately $900bn (one-third of the current value of big oil and gas companies) would disappear if governments more aggressively attempted to restrict the rise in temperatures to 1.5C above pre-industrial levels for the rest of this century, in accordance with the 2015 Paris Climate Accord. This will certainly impact investment banking firms that do business with oil companies and insurance companies for example, that own some of their debt. https://www.ft.com/content/95efca74-4299-11ea-a43a-c4b328d9061c.

[109] It was reported North Korea stole approximately $2 billion from at least 38 countries across five continents over the last five years-greater than 3-times the amount of money it was able to generate through counterfeit activity over the previous four 40 years. The Cybersecurity and Infrastructure Security Agency (CISA), Treasury, FBI and U.S. Cyber Command identified malware and indicators of compromise used by the North Korean government in an ATM cash-out scheme—referred to as "FASTCash 2.0. https://us-cert.cisa.gov/ncas/alerts/aa20-239a. https://carnegieeurope.eu/strategiceurope/81599.

[110] Sheltered Harbor was created to protect customers, financial institutions, and public confidence in the financial system if a catastrophic event like a cyberattack causes critical systems—including backups—to fail. The Sheltered Harbor standard prepares institutions to provide customers timely access to balances and funds in such a worst-case scenario. Sheltered Harbor I s a not-for-profit, industry-led initiative comprising financial institutions, core service providers, national trade associations, alliance partners, and solution providers dedicated to enhancing financial sector stability and resiliency. https://www.shelteredharbor.org/.

[111] The Bank for International Settlements has established its Cyber Resilience Coordination Centre (CRCC) which has published a report, identifying, and comparing the range of observed bank, regulatory and supervisory cyber-resilience practices across jurisdictions. https://www.bis.org/bcbs/publ/d454.htm.

[112] In March 2017, the G20 Finance Ministers and Central Bank Governors outlined an initial road map to increase the cyber resilience of the international financial system. In 2019, the Carnegie Institute partnership with the IMF, SWIFT, FS-ISAC, Standard Chartered, the Global Cyber Alliance, and the Cyber Readiness Institute introduced a cyber resilience capacity-building toolbox for financial institutions. https://carnegieendowment.org/specialprojects/fincyber/.

[113] https://www.finra.org/sites/default/files/NoticeDocument/p003809.pdf.

[114] https://www.finra.org/rules-guidance/rulebooks/finra-rules/3130.

[115] The investment advisory industry is more focused on ESG and may be subject to more requirements (see Financial Factors in Selecting Retirement Plan Investment Act, whereby plans would have to consider ESG factors in a prudent manner consistent with their fiduciary obligations, the same legal standard that ERISA already applies to non-ESG investment factors. https://www.federalregister.gov/documents/2020/11/13/2020-24515/financial-factors-in-selecting-plan-investments. See also the Sustainable Investment Policies Act of 2020, that would amend the Investment Advisers Act of 1940 to require large asset managers to establish Sustainable Investment Policies, https://www.govtrack.us/congress/bills/116/hr8960). While the broker-dealer industry operates under a "suitability" standard (see FINRA Rule 2111), where the integration of ESG factors is not yet required in making suitable recommendations, the potential threat posed by climate change to all securities investments, may necessitate revisiting this standard at some point. It is also worth noting that The Long Term Stock Exchange in the U.S. has principles-based listing standards for its issuers which asks long-term focused companies to consider a broader group of stakeholders and the critical role they play in one another's success, including a policy explaining how the company operates its business to consider all of the stakeholders critical to its long-term success, including: the company's impact on the environment and its community. https://longtermstockexchange.com/listings/principles/