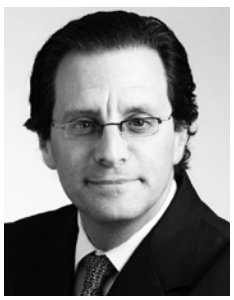
Compliance, technology and data risk: Electronic communications and the modernisation of data governance control structures

Received (in revised form): 4th October, 2024

Therese Craparo



Anthony J. Diana

Philip H. Thomas

Therese Craparo[*]
Partner, Reed Smith, USA

Anthony J. Diana[**]
Partner, Reed Smith, USA

Philip H. Thomas[†]
Partner, Reed Smith, UK

Christian Leuthner[‡]
Partner, Reed Smith, Germany

Samantha M. Walsh[‡‡]
Associate, Reed Smith, USA

Ryan J. Fitzpatrick[¶]
E-Discovery Attorney, Reed Smith, USA

Therese Craparo *is a partner in Reed Smith's Emerging Technologies Group and BankTech practise. She focuses her practise on enterprise data risk management, information governance and record-keeping, technology implementation, cybersecurity and eDiscovery. Therese has worked with some of the world's largest financial institutions to develop strategies for managing the legal and regulatory issues relating to both traditional and innovative technologies, including the developing policies and procedures for data governance and record-keeping, designing and execution data remediation and retention protocols, eDiscovery strategy and management and the use of data analytics and artificial intelligence (AI) for eDiscovery, compliance and risk management. Therese advises clients on how to execute, defensibly implement and defend data strategies from beginning to end, including remediating billions of records safely and defensibly, investigating and addressing record-keeping and surveillance gaps, evaluating and implementing new technologies and defending data governance protocols before regulatory bodies, including the Financial Industry Regulatory Authority (FINRA), the US Securities and Exchange Commission (SEC), the Federal Reserve and the Commodity Futures Trading Commission (CFTC).*

Anthony Diana *is a partner in the Emerging Technologies, Records and eDiscovery and BankTech Groups, and focuses his practise on advising on the legal, regulatory and operational risks associated with implementing, operating and upgrading technology at financial institutions and the management of risks associated with data at financial institutions. Anthony is a recognised leader in eDiscovery and enterprise data risk management issues, nationally ranked in this area by Chambers. Anthony counsels large financial institutions on all aspects of the discovery and management of electronic information, including the development of policies*

Journal of Financial Compliance
Vol. 8, No. 3 2025, pp. 198–214

2398-8053 (2025)

Included in **The Business and Management Collection**

and procedures regarding information governance for various technologies, including artificial intelligence (AI), social media, Wi-Fi and bring your own device (BYOD); and the defence of electronic discovery and information governance policies and procedures before federal regulators and the courts. Anthony has decades of experience advising financial institutions on the implementation and upgrading of technology, with a particular focus on legal, regulatory and operational issues with Microsoft 365 and messaging archives. Anthony has advised on implementing M365 features, including Teams and Copilot, and the migration of data into M365 from legacy data sources (home drives, group shares, exchange, etc). He has advised financial institutions on the implementation and migrations of messaging archives. Anthony has conducted numerous internal investigations for potential liability and violations of laws and/or regulations on behalf of audit committees and general counsel offices in connection with inquiries from regulators, auditors and plaintiffs. Anthony has presented and defended the findings of investigations before regulators, including the Financial Industry Regulatory Authority (FINRA), the Federal Reserve, the US Securities and Exchange Commission (SEC), the Public Company Accounting Oversight Board (PCAOB) and auditors.

Philip Thomas *is a partner in Reed Smith's Emerging Technologies Group, specialising in UK and international privacy and data protection laws, as well as technology and intellectual property. He has a particular interest in the developing cyber and data regulatory landscape and counsels technology service providers and customers operating within Reed Smith's core sectors.*

Christian Leuthner *is a Partner in the Emerging Technologies group. Focusing his practise on technology and data protection, Christian is a trusted advisor to clients seeking help to navigate the ever-changing risk landscape associated with technological development. With a decade of experience as a commercial lawyer in the field, Christian advises on all aspects of IT and data protection law, including cloud computing, online platforms, international data transfers, technology transactions, company integrations and various e-commerce-related projects. Working with clients ranging from multinational company groups and more mature companies to start-ups, Christian has a particular focus on ensuring that his clients are maximising the opportunities available to them through new and emerging technologies while minimising any associated risk.*

Samantha Walsh *is an Associate in the Emerging Technologies group and focuses her practise on enterprise data risk management, information governance, data privacy and artificial intelligence (AI) governance. Prior to Reed Smith, Samantha was in-house counsel at a large US bank.*

Ryan Fitzpatrick *is an E-Discovery Attorney in the Emerging Technologies group. Ryan assists with data remediation as well as legal research on a variety of data privacy and governance matters.*

Christian Leuthner

Samantha M. Walsh

Ryan J. Fitzpatrick

Abstract

Record-keeping and supervision rules regarding electronic communications (eComms) for financial institutions have been in place for as long as eComms have existed. The underpinning of these regulations is the view that the security, reliability, integrity and availability of information reflecting a financial institution's activities are fundamental to the integrity of the financial markets. Over the last few years, the financial regulators have powerfully reminded the financial industry of the importance of the eComms record-keeping rules, launching dozens of off-channel eComms enforcement actions that have resulted in more than US$2bn of fines to date. With the rise in the variety and availability of individual eComms applications and the use of collaboration tools and generative AI (GenAI), the number and variety of channels available to employees for communications purposes are,

however, growing exponentially. Even for sophisticated financial institutions, the resources required to effectively manage the pace of technological development and adapt compliance processes in this space can be overwhelming. This paper explores the regulatory approach to eComms compliance in a changing technology world and how financial institutions can appropriately manage eComms risk. It is possible to establish a robust control structure that meets regulatory expectations, accommodates business needs and keeps pace with changing technology. An effective eComms governance structure must, however, encapsulate processes that engage all key stakeholders, embrace innovation and integrate legal, compliance and IT reasoning that moves beyond reliance on individual employees and detection technology and incorporates data governance as a fundamental principle in business operations and technology development.

Keywords: electronic-communications, off-channel, eComms, broker–dealers, investment advisers, record-keeping, books-and-records, WhatsApp, SEC, CFTC, financial institutions, financial regulators. business-as-such, financial

DOI: 10.69554/TBUH6927

*Reed Smith, 599 Lexington Avenue, 23rd Floor, New York, NY 10022, USA
Tel: +1 212 549 0421; E-mail: tcraparo@reedsmith.com

**Reed Smith, 599 Lexington Avenue, 23rd Floor, New York, NY 10022, USA
Tel: +1 212 549 0332; E-mail: adiana@reedsmith.com

†Reed Smith, 1 Blossom Yard, London E1 6RS, UK
Tel: +44 (0)203 116 3526; E-mail: pthomas@reedsmith.com

‡Reed Smith, OpernTurm Bockenheimer Landstraße 2 – 4, Frankfurt am Main, 60306, Germany
Tel: +49 69 22228 9846; E-mail: cleuthner@reedsmith.com

‡‡Reed Smith, 599 Lexington Avenue, 23rd Floor, New York, NY 10022, USA
Tel: +1 212 549 0315; E-mail: samantha.walsh@reedsmith.com

¶Reed Smith, 599 Lexington Avenue, 23rd Floor, New York, NY 10022, USA
Tel: +1 212 549 4756; E-mail: ryan.fitzpatrick@reedsmith.com

INTRODUCTION

Record-keeping and supervision rules regarding electronic communications (eComms) for financial institutions have been in place for as long as eComms have existed. Beginning with facsimile and e-mail, regulatory focus on the changing landscape of communications and how financial institutions must adapt their control structures to manage those changes has been inexorable. The underpinning of the regulatory focus in this area is the view that the security, reliability, integrity and availability of information reflecting the operations of the financial industry are fundamental to the integrity of the financial markets and essential for regulatory bodies to carry out their mandates. Over the last few years, financial regulators have powerfully reminded the financial industry of these facts through guidance and enforcement actions.

At the same time, the way employees at financial institutions work is also changing. With the rise of the variety and availability of individual eComms applications, the use of collaboration tools and generative AI (GenAI) and the democratisation of advances in technology, the number and variety of channels available to employees for communications purposes has grown exponentially, and the pace of innovation means that new communications tools are constantly emerging. Even for sophisticated financial institutions, the resources required to effectively manage the pace of technological development and adapt compliance processes in this space can be overwhelming. Despite the challenges, the financial regulators have been clear that compliance with record-keeping and supervision regulations are simply the cost of doing business.

Ultimately, the ability to appropriately manage the risks of eComms compliance requires establishing a robust control structure that meets regulatory expectations, accommodates business needs and keeps pace with changing technology. Data governance, including for eComms, presents a cross-disciplinary set of risks, encompassing record-keeping, supervision, privacy, data security and eDiscovery considerations. An effective eComms governance structure must encapsulate processes that consider all of these risks, engage all key stakeholders and embrace innovation. Above all, data compliance processes today require an integration of legal, compliance and IT reasoning that moves beyond reliance on individual employees and detection technology and incorporates data governance as a fundamental principle in business operations and technology development.

ECOMMS ENFORCEMENT: YESTERDAY AND TODAY

The recent fines issued in the USA by the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) to financial institutions across the industry for failure to retain and supervise eComms that took place 'off-channel', through text messaging and instant messaging applications such as WhatsApp, have — by design — caught the attention of the financial industry. Those fines, ranging into the hundreds of millions of dollars (and now totalling well over US$2bn with more fines coming), are the largest the industry has seen for individual record-keeping violations.[1]

The off-channel communications fines are, however, not the first issued by these regulatory bodies for violations of the eComms supervision and record-keeping regulations. In fact, the SEC, the Financial Industry Regulatory Authority (FINRA) and the CFTC have decades of enforcement history relating to eComms compliance. Notably, in the mid-to-late 2000s, following SEC approval of rule changes acknowledging the impact on the industry of the expanding use of eComms such as e-mail and facsimile, the SEC and FINRA engaged in a series of enforcement actions relating to financial institutions' failure to properly retain, store and produce eComms that resulted in millions of dollars in fines.

These early enforcement actions shook the financial industry. They elevated the focus on compliance with the record-keeping and supervision regulations, forced the financial industry to more closely evaluate and invest in compliance technologies relating to eComms and gave rise to an entirely new industry dedicated to developing technology to securely capture, archive, store and retain the eComms of financial institutions; known today as compliance messaging archives. Regulatory scrutiny of compliance with record-keeping and supervision requirements has been steady over the past decades; the recent fines were orders of magnitude larger than past penalties, but the underlying principles were nothing new. Far from being off-the-radar, regulatory attention to eComms record-keeping and supervision has been consistent throughout time.

The more recent off-channel enforcement actions are shaking up the industry today much as the eComms enforcement actions did in the 2000s. All of those actions are remarkably similar and indicate the commonality of the pervasive use of new and nonstandard eComms tools. What is clear from the recent spate of enforcement actions is that the SEC and CFTC have focused on a pattern of conduct across the industry, giving rise to both scrutiny and violations. The typical fact pattern across the multitude of enforcement actions is as follows:

> Each financial institution had written policies prohibiting the use of 'off-channel' eComms tools — meaning eComms tools that were not controlled by the financial institution or captured in the financial institution's compliance messaging archive — for business communications. Nonetheless, regulated business users were using "off-channel" eComms tools for business communications, both internal and external. Those off-channel eComms tools included text messaging and commonly-used applications that are readily available for download and use on mobile devices, such as WhatsApp, iMessage, WeChat, Signal and LinkedIn.
>
> Use of these 'off-channel' eComms tools for business communications was not occasional, one-off or one-time. Such use was wide-spread and prolific across the regulated business. Notably, use of these 'off-channel' eComms tools for business communications frequently included senior-level personnel — including

personnel responsible for ensuring compliance with the policy prohibitions against the use of these 'off-channel' eComms tools for business communications.

In most cases, there was a decided lack of processes or mechanisms to identify, track and monitor the use of these 'off-channel' eComms tools for business purposes. In some cases, the prolific use of these 'off-channel' eComms tools was known to the financial institution, even known to Legal or Compliance personnel, and recommendations or directives relating to these impermissible uses were made but ignored or simply not timely actioned. There was little to no evidence of consequence management, i.e., known and direct consequences to individuals violating the policy prohibitions against the use of 'off-channel' eComms tools for business purposes.

This wide-spread, virtually unchecked, usage is what prompted the extraordinary financial penalties. The regulators viewed this industry-wide, systemic behaviour as, at best, a failure to invest and execute on compliance mechanisms to ensure compliance with the record-keeping regulations and, at worst, a blatant disregard for the importance and purpose of the record-keeping regulations in favour of convenience. Furthermore, the regulators expressed concern that with advances in technology and new eComms tools popping up, the failure to keep pace with technology and to implement comprehensive compliance mechanisms would result in further regulatory violations. Beyond the eye-popping and precedent-setting fines that have been issued, the SEC and the CFTC have used these enforcement actions to send very specific messages to the financial industry.

Fines

The fines issued by the SEC and the CFTC to broker-dealers and investment advisers have ranged from US$325K to US$125m and seem to be commensurate with the regulators' view of the pervasiveness and scope of record-keeping violations. These violations are some of the largest in history for individual record-keeping violations.

Breadth

Historically, regulatory fines for record-keeping violations tended to be one-offs, even where multiple fines were announced at once. Here, the SEC and the CFTC have expanded these investigations across the industry to virtually every major financial institution; encompassing more than 75 different financial institutions to date, with more fines expected to come. The actions target a wide variety of financial institutions ranging in size from the largest financial institutions to smaller institutions not typically targeted for such violations.

Technology

The regulators have reiterated the need for financial institutions to adapt and tailor their compliance programmes to account for the rapid and ever-changing nature of technology. In 2022, in announcing settlements related to 16 financial institutions, SEC Chair Gary Gensler noted '[a]s technology changes, it is even more important that registrants appropriately conduct their communications about business matters within only official channels, and they must maintain and preserve those communications'.[2] The regulators also made it clear that each financial institution is responsible not only for monitoring eComms use but also for investing in compliance structures that have the capacity to detect violations and in technology that meets both business and regulatory requirements by ensuring that new eComms tools can be captured, retained and surveilled.

Enforcement and consequence management

One of the key themes articulated throughout the enforcement orders is the regulators' focus on insufficient, and at times *nonexistent*, enforcement mechanisms within financial institutions' compliance programmes. Inherent in this focus is the notion that policies and procedures, without more, are inadequate to comply with applicable regulatory obligations. Specifically, the regulators highlight that policies and procedures must be accompanied by consistent and robust enforcement structures.

Cooperation and remediation

Recently, the SEC has reinforced the importance of cooperation and remediation, with respect to companies' record-keeping obligations. For example, in a recent enforcement action, SEC Division of Enforcement Director Gurbir Grewal noted, 'firms that self-report and otherwise cooperate with … investigations may receive significantly reduced penalties. Here, despite record-keeping failures that involved communications by senior leadership and persisted after our first record-keeping matters were announced in 2021, [firm] took substantial steps to comply, self-reported, and remediated, and, therefore, received a no-penalty resolution'.[3] As seen from Director Grewal's comments, it is imperative that, to the extent violations are discovered, processes and procedures are in place to facilitate cooperation and remedial action. Furthermore, several of the SEC enforcement actions have noted that lower penalties reflect voluntary self-reporting and cooperation with the Commission.[4]

Expansion

Departing from the almost exclusive focus on broker-dealers, the SEC has recently expanded the scope of its scrutiny and enforcement actions to investment advisers, including stand-alone investment advisers. This is notable as record-keeping enforcement actions, while common for broker-dealers, have historically been rare among investment advisers. By expanding the enforcement sweep to include investment advisers, the SEC made a clear statement that *all* regulated companies must comply with the record-keeping rules.

Overall, these more recent regulatory enforcement actions are a reminder and a warning to the financial industry that the regulators expect the financial industry to *keep pace* with technology, to be *proactive* in enforcing the record-keeping regulations and to take their obligations to *safeguard their data* and protect market integrity seriously.

REGULATORY REQUIREMENTS

The current intense focus on eComms compliance, and the attendant challenges, presents a microcosm of the larger challenges that financial institutions have faced for decades when it comes to data governance. There is a vast labyrinth of regulations with which financial institutions must comply. Record-keeping and supervision, and even more specifically eComms record-keeping and supervision, represent just a few. In tandem, financial institutions leverage thousands, if not tens of thousands, of systems and sources of data in order to efficiently and effectively operate their businesses and deliver quality customer service. In attempting to appropriately allocate finite resources across the organisation, the particular conundrum of eComms governance has not always been top of the list. Regulators, however, are rarely sympathetic to pleas of burden, resourcing or technological challenges.

Financial regulators view record-keeping and supervision, including for eComms, to be fundamental to the integrity of the financial system, ie the regulatory scheme reflects the importance of maintaining complete

and accurate records of a financial institution's business activities. The underlying purpose of these regulations is to support and evidence the reliability of financial data (and thus, the financial system), facilitate supervision of business activities to identify potential regulatory violations or market manipulation and ensure that the financial regulators have sufficient information available to discharge their duty to oversee the financial industry.

In general, financial regulations require financial institutions to store, retain for a defined period and supervise/monitor communications that contain certain content. The requirements mandating supervision and retention of communications are rooted in regulatory regimes promulgated by a variety of regulatory bodies. Although similar in some respects, these regulatory frameworks contain nuanced storage, retention, supervision and content requirements depending on the regulated entity, underlying activity and nature and purpose of the communications.

UNITED STATES

As a general matter, the primary source of compliance requirements around the surveillance and archiving of eComms for financial institutions in the USA flows from the statutory and regulatory mandates of the SEC and the CFTC. These regulatory bodies are supported in their regulatory and enforcement efforts (including as related to eComms) by two self-regulatory organisations, FINRA and the National Futures Association (NFA).

At a high level, the bevvy of rules and requirements related to eComms centre around: (1) the capture of eComms concerning specific *content*; (2) the storage of such eComms for particular retention periods and, in some cases, in a particular *format*[5] and (3) reasonable, risk-based supervision of eComms for both specific activity and to ensure compliance with relevant rules generally.[6] Moreover, depending on the business activity and regulated nature of the entity in question, the scope of eComms required to be captured ranges from expansive (eg Rule 17a-4's 'business as such') to more tailored content focused on specified activity.[7] Importantly, the regulators have consistently made clear that such rules *are not limited to a particular medium or form of communication and are grounded in content irrespective of the mechanism used to communicate*.[8] Consequently, the rules and requirements can focus on a broad scope of potential eComms technologies.

BEYOND THE USA

The USA is not the only jurisdiction that has promulgated regulations for financial institutions that are specific to the retention and supervision of communications. In particular, in the European Union (EU), the Markets in Financial Instruments Directive (MiFID II) and the related Delegated Regulation 2017/565 (DelReg) require covered institutions to retain eComms that meet designated content requirements for five years or, if requested by the regulator, for up to seven years.[9] MiFID II also requires that records, including eComms, are retained in a secure format that assures data integrity by ensuring that the eComm is retained in its original, unaltered form.[10] MiFID-covered entities are obligated to monitor eComms, as appropriate and on a risk basis, to ensure compliance with regulatory obligations, detect market abuse or fraudulent trading practises and evaluate conflicts of interests, etc.[11]

In the UK, the applicable rules regarding the retention and supervision of communications broadly mirror those of the EU. Specifically, MiFiD II has been transposed into UK law through a combination of the Financial Conduct Authority (FCA) Handbook rules, Treasury legislation and various EU Regulations that are directly applicable following Brexit, for example, the Markets in

Financial Instruments Regulation 600/2014 (MIFIR) and DelReg. The FCA Handbook builds focus on the EU requirements by requiring the relevant communications to be accessible to the FCA in the future, by ensuring that such communications are: (a) readily accessible by the FCA; (b) capable of being reconstituted clearly and accurately and (c) maintained in a manner that enables any changes, corrections or amendments to be easily identifiable.

THE COMMUNICATIONS EXPLOSION AND THE REGULATORY APPROACH

The business and technological environment in which financial institutions presently operate is a far cry from the by-gone days when e-mail was seen as the forefront of innovation, and the biggest risk was that individuals using their personal Yahoo! accounts for business-related communications. Today, Internet-based communications channels abound, including both on- and off-channel. Social media sites, such as LinkedIn, TikTok, Instagram and Reddit; collaboration sites such as Teams, Slack and Zoom and chat applications, such as WeChat, WhatsApp and Telegram, are readily accessible to users and present material challenges when it comes to monitoring and controlling off-channel communications use. The ease with which these channels can be downloaded and utilised and the ability to do so on virtually any mobile device (whether company approved or not) have materially changed the communications game.

Beyond those channels that represent clear off-channel use, the variety and breath of communications channels available in company-approved applications designed to improve efficiency, communicate with clients and otherwise increase business value are being rolled out at a dizzying pace. The shift to cloud-based software-as-a-service (SaaS) tools and the recent spotlight on GenAI and other GenAI-powered tools (such as ChatGPT) have resulted in business, competitive and cost pressures that are serving as a further tailwind to procuring and employing the latest technology. This includes functions in tools that otherwise may not be spotlighted as containing eComms functionality, such as in-application chat, comment, co-editing, survey and other collaboration features, to name just a few.

While generally challenging from a governance perspective, these nontraditional communications features are often accompanied by a certain ambiguity regarding their regulatory treatment, particularly considering their absence from regulatory enforcement actions. This is further compounded by the dearth of guidance coming from the regulators on new, nontraditional and emerging communication features.

However, the evolution of regulatory guidance relating to eComms does demonstrate how the regulators approach new technology generally and the challenges of keeping pace with technological development in the modern era. In the USA, the regulatory scheme does not address 'electronic communications' *per se* but generally refers to the retention of 'correspondence' or 'communications' and notes that such definitions apply equally to both physical and electronic formats of such 'correspondence' or 'communications' (referred to hereafter as 'communications'). This lack of specificity is deliberate; the regulations are intended to address *all* types or formats of communication and are not limited by technology or technological development. Rather, financial institutions are expected to monitor and manage the activities of their businesses, to keep pace with the changing nature of business communication and to ensure compliance with the regulations regardless of the technology used.

In the EU, MiFID II requires the recording of electronic communications and telephone conversations that relate to, at least,

transactions concluded when dealing on own account and providing services relating to the reception, transmission and execution of client orders. While MiFID II does not contain a definition of electronic communications *per se*, the European Securities and Markets Authority (ESMA) interprets the term 'electronic communication' broadly and explicitly includes, among others, video conferencing, fax, e-mail, Bloomberg mail, short messaging service (SMS), business-to-business (B2B) devices, chat, instant messaging, and mobile device applications.[12] ESMA, however, also states that because of the continuing innovation and advancement in technology, an exhaustive list of electronic communications would not make sense.

In the UK, the FCA has adopted the very broad definition of 'electronic communications' outlined in s.15(1) of the Electronic Communications Act 2000, namely any communication transmitted from one person to another, from one device to another or from a person to a device or vice versa, either by means of an electronic communications network or otherwise by other means in electronic form. The FCA Handbook has clarified that 'electronic communications' includes (but is not limited to) communications made by way of facsimile, e-mail and instant messaging devices.[13] The breadth of the definition combined with the non-exhaustive list of examples given suggests that (as with the EU) the intention is for the applicable regulations to address all types or formats of communication, irrespective of technology, device or application.

The changeability in the means and methods of electronic communication is not unnoticed or unrecognised by financial regulators. As particular formats become more common or represent more risk to consumers, the regulators do provide written guidance to alert financial institutions that certain formats or technologies are considered communications. The vast majority of this written guidance emanates from FINRA; however, while the electronic communications regulations do vary across different types of financial institutions, the financial regulators generally concur on what constitutes electronic communication.

For example, while unsurprising today, the first generation of recognised electronic communications comprised e-mail and facsimiles. In 1997 and 1998, the SEC and the National Association of Securities Dealers (NASD) (FINRA's predecessor) issued guidance acknowledging that the proliferation of new electronic means of communicating, such as e-mail and facsimile, necessitated modernisation of the existing rules and recognising that these electronic communications were subject to the same record-keeping requirements as any other form of written communication.[14] Just a few years later, in 2003, the NASD issued a notice noting the increased use of instant messaging and warning companies that the 'lack of formality' of instant messaging did not exempt it from the supervision and record-keeping regulations.[15]

In 2007, FINRA issued an advisory notice mentioning that text messaging was also a communication subject to the supervision and record-keeping regulations.[16] Later, FINRA addressed the growing use of social media or other Internet sites for purposes of communication, recognising that social media sites, interactive electronic forums (ie blogs, chat rooms and discussion boards) and even 'likes' and sharing comments may be considered communications subject to the supervision and record-keeping regulations.[17]

More recently, FINRA has turned its attention to 'collaboration' and GenAI tools that may be used for communication purposes. In September 2021, FINRA issued frequently asked questions (FAQs) indicating that visual aids, such as digital whiteboards, dynamic charts, live polling and chat/instant messaging during a live, unscripted meeting may constitute communications subject to the supervision and record-

keeping regulations.[18] In May 2024, FINRA updated those same FAQs to provide similar guidance with respect to the use of chatbot communications.[19]

Similar developments can be seen in the EU. In May 2024, ESMA issued guidance on the use of AI in investment services.[20] While ESMA recognises the potential benefits of AI for customer service and support, investment advice and portfolio management, risk management and many other areas, ESMA emphasises the importance of adhering to MiFID II requirements when using AI in investment services.

The lesson to be learnt in this progression, of course, is that the regulators are monitoring technological development and how financial institutions are using technology to communicate both internally and externally. They expect that the financial industry is doing the same.

COMMON ECOMMS COMPLIANCE CHALLENGES

With 'lessons learned' comes a reflection on how to integrate those lessons into a financial institution's business-as-usual (BAU) eComms compliance processes. That, of course, is not as easy as one might hope. Current compliance structures and limitations present substantial challenges to updating and modernising compliance efforts with respect to eComms.

Responsibility and accountability

One of the all-too-common challenges with eComms compliance is that it tends to fall between the cracks of compliance efforts. This is, in part, because eComms represent only one small portion of a financial institution's compliance efforts and in part because eComms compliance touches on a variety of considerations including records management, supervision, privacy, security, technology and eDiscovery. Because each of these areas has *some* obligations with respect to eComms, none of the areas tends to have *all* obligations with respect to eComms. As a result, eComms compliance often results in a finger-pointing exercise where no one fully accepts responsibility for compliance.

Changing technology and business use

With the proliferation of cloud-based applications and the rise of shadow IT, tracking which applications are in use, much less whether they have eComms features, can be difficult, even for companies with smaller technology footprints. Furthermore, even where an application is a known asset and has gone through an onboarding process, vendors often introduce new features, which may end up in production without passing through any legal or compliance review process. Indeed, most technology vendors view integrating methods of communication within their application as a new fundamental component of the technology, increasing the productivity of the business process that the application supports by replacing more traditional forms of communication like e-mail. Moreover, the introduction of new collaboration features, many of which include some form of eComm, has increased significantly since the start of the COVID-19 pandemic. These features are increasingly central to the way many teams operate and can provide significant business benefits, but unfettered adoption and use of new collaboration technology may be incompatible with financial institutions' regulatory obligations.

Technology integration

Compliance efforts at financial institutions have not necessarily kept pace with technology. Often, legal and compliance are not tied in with technology development or implementation across the organisation, resulting in large gaps in understanding, communication and execution of

compliance requirements. In the current landscape, managing the risk associated with eComms requires compliance and legal departments to closely partner with IT, who can provide much needed subject-matter expertise and can operate as boots on the ground with the business in the compliance effort. Cross-functional cooperation is crucial and frequently lacking.

Adequate resourcing (people and technology)

Staying on top of constantly changing technology requires significant resources. Ensuring measures that address eComms compliance are incorporated into all technology development and third party systems requires significant resources. Executing on compliant capture and storage mechanisms for an increasingly vast number of eComms technologies requires significant resources. Despite the perception of unlimited resources available to financial institutions, many financial institutions simply do not have enough subject-matter experts or funding dedicated to eComms compliance to allow for the level of monitoring required to identify and assess new applications and features. Properly archiving and supervising eComms requires an investment in specialised technology (and people to maintain it) that does not necessarily increase in proportion to the growing needs. While the regulators may not be sympathetic to resourcing complaints, legal, compliance and technology personnel by necessity must work within the constraints of the resources that they are allocated and evaluate where the compliance risks are most acute to make the biggest impact on risk mitigation from those resources.

MODERNISING ECOMMS GOVERNANCE CONTROL STRUCTURES

At the heart of any eComms compliance effort lies the familiar concept of 'governance'. At base, 'governance' refers to the policies, procedures, practises and structures directing an organisation's approach to identifying and controlling risk while maximising and facilitating business and operational goals. Adequate governance necessarily requires a top-down approach — which has been highlighted and emphasised by the regulators in connection with the off-channel communications enforcement actions — that begins with a strong policy that clearly defines roles, responsibilities and expectations, incorporates repeatable procedures and practises and supports cross-functional collaboration throughout the institution. Critically, for any type of data governance, including eComms governance, modern control structures must closely align and incorporate technology strategy, third party risk management and meaningful enforcement regimes to be able to keep pace with changing user behaviour and technology risk.

Centralised governance structure

The multifaceted, ever-changing and complicated nature of eComms, which touches all corners of the institution, requires a governance framework that: (a) clearly defines roles and responsibilities specific to eComms governance; (b) centralises decision making and authority and (c) incorporates insights from all stakeholder groups. There are no pre-defined requirements for this framework and it may take various forms depending on the nature and structure of each financial institution. The key goal is to establish centralised strategic and decision-making authority in a manner appropriate to each institution. This can take the form of a centralised data governance office or a cross-disciplinary working group, council or committee that oversees eComms strategy and compliance efforts. It should incorporate stakeholders from at least technology, legal, compliance, records management, eDiscovery, privacy, security and

the business. This group or body can develop a strategy, set policy, establish standards and guidance, carry out review procedures, make determinations on new applications and/or technology and implement controls and safeguards. Moreover, the operational elements needed to carry out and enforce broader strategy can be defined by, and flow from, this function, serving as the single point of authority for eComms governance, facilitating consistency and continuity across the organisation. In sum, there needs to be a decision-making body with the authority that can say 'no' to the business and IT if the technology does not fitted within the broader eComms strategy, which can set requirements for any implementation of an eComms technology (including forcing the business to bear the costs and burden of implementation, maintenance and compliance if the business wants the technology) and that can establish clear priorities in the eComms governance programme based on its evaluation of risks.

Policies and procedures

Once a governing function is established, policies and procedures are needed to effectuate the institution's strategy, business and compliance mandates. These policies and procedures should clearly set out: (1) expectations; (2) processes and (3) consequences related to eComms. For example, an institution should promulgate a high-level policy laying out its approach to eComms. Such policy should outline regulatory obligations, content requirements, standards for use, capture, storage and retention, approved/unapproved eComms channels and a robust escalation and consequence model. Procedures should be put in place that allow end users and IT personnel to operationalise high-level policy pronouncements, such as procedures for onboarding or developing new technology or applications that include eComms, approval processes for new eComms use, standards for eComms capture/archiving and retention, guidance for defining eComms and appropriate eComms use and monitoring and attestation requirements for production applications.

Beyond directed eComms policies and procedures, institutions must assess their existing policies, practises and procedures relating to eComms to ensure consistency across policies that focus on, but do not direct, eComms compliance. This includes evaluating policies and procedures relating to bring-your-own-device (BYOD), corporate mobile devices, codes of conduct, third party risk management (discussed in more detail next), AI, records and information management policies, supervision and the like. Consistency across data-related policies is necessary to facilitate user compliance and effectively execute the institution's defined eComms strategy.

Monitoring, reporting and tracking

Compliance with eComms regulations requires identifying and tracking eComms functions in use across the institution. This is no small endeavour. It requires not only identifying eComms functions available in *new* technologies but also identifying eComms features that emerge in *existing* technologies and monitoring for new types of eComms features and functions. With the proliferation of new technologies and the instant-upgrade functionality of cloud technologies, this effort can involve thousands of different applications. Consideration should be given to implementing a risk-based approach that focuses on applications that present a higher regulatory risk initially, and as the eComms governance programme matures, develop a broader governance approach that is expanded to accommodate appropriate reviews of lower risk applications.

First, potential new eComms features should trigger an internal review process

to determine whether they are, in fact, eComms that fall under the regulations and must be captured/archived, stored and retained accordingly. This must include both eComms features in new products (third party and proprietary) and new eComms features in existing products. Importantly, this requires trigger mechanisms in different processes within the organisation, eg third party risk management, technology development and life cycle management. Second, eComms governing bodies should document their review of new and existing potential eComms features to demonstrate a thoughtful, clear, compliant strategy to defining and governing eComms use. This may involve, for example, maintaining an inventory of eComms features and applications reviewed and documenting the decisions made regarding compliance requirements, including whether certain types of eComms fall outside the eComms compliance structure. Third, the decisions made as to the approved or unapproved use of select technologies should be clearly communicated and readily available to users to ensure that the institution is facilitating individuals' ability to comply with institutional policy. Furthermore, these decisions, and the underlying reasons, should be disseminated to other groups within the organisation who may be reviewing or monitoring technology and business activities (such as data use boards, supervision teams and procurement) so that they too can identify potential eComms use.

Keeping pace with business use and investing in technology

If the regulators have made nothing else clear in the recent off-channel communications enforcement actions, it is that they expect that financial institutions are keeping pace with technology (irrespective of any direct regulatory guidance on a particular technology) that legal and compliance are directly involved in and overseeing eComms use and compliance and that financial institutions are investing in compliant technology. New or emerging business needs should be identified, and institutional strategies established for investing in compliant technologies that meet those needs. Standards must be set, communicated and enforced that define the requirements for eComms capture/archiving, storage and retention. This means that resources must be incorporated into new technology procurement or development that support eComms compliance where necessary. Such requirements are more critical for applications deemed to meet higher risk criteria, so if there are limited resources, such resources should be allocated to those higher risk applications.

Third party risk

With the rise and continued ubiquity of cloud-based and SaaS solutions, addressing third party risk is a crucial aspect of any data governance programme. Thus, incorporating third party risk management into an eComms governance framework is table stakes. At bottom, third party risk assessment must be interpolated throughout the application life cycle, from onboarding to decommissioning. This can be done by ensuring that proper procedures are in place for onboarding and evaluation of new vendors and applications, conducting periodic reviews — particularly as vendors consistently provide updates and new features that may alter initial risk weighting and eComms identification — and inventorying and tracking use cases. Moreover, safeguards should be put in place to prevent shadow application sprawl, with processes to periodically audit application use throughout the enterprise. In short, procedures for managing eComms promulgated via third party vendors should align with the current pace of technological development, safeguarding against unidentified feature updates that

may constitute eComms subject to policy and regulatory obligations.

Employee training

As with any compliance effort, employee training is fundamental. At base, eComms compliance is dependent on individual business and IT employees understanding and executing on institutional policy. For general end-user employees, eComms training for all employees on eComms policy and procedures should be performed for new hires and for all employees on a periodic basis. Such training can be stand-alone or incorporated into broader data risk management or records management training. That training should run the gamut, incorporating appropriate use, roles and responsibilities, approvals, escalation and reporting channels, as well as consequence models.

For developers and IT teams, granular training on policy-based requirements should be provided, along with guidance on how to address eComms compliance in the application development process. The training may include the specific intricacies found in record-keeping and supervision requirements (ie retention, format and storage requirements) and how those may translate to technical implementation. Moreover, any such training should be directed at equipping technology teams with the requisite knowledge needed to identify potential compliance issues, allowing for a symbiotic relationship among legal, compliance and IT.

To evidence and support compliance efforts, training programmes should incorporate attestations of compliance that are tracked and retained to demonstrate that training occurred and support user understanding of eComms compliance. Training models should also provide clear mechanisms for reporting potential policy violations. An institution may also wish to solicit feedback from personnel as to what forms of eComms are in use or are being requested by clients or service providers. Understanding where communication needs are potentially not being met can help an organisation head off the circumvention of controls around eComms.

Supervisory review and enforcement

Ultimately, the best policies and procedures in the world are not sufficient to ensure and evidence compliance with regulations, including eComms compliance. Many of the financial institutions involved in the off-channel communications enforcement actions *did* have policies and procedures in place and *did* communicate to users that they were not permitted to use off-channel communications tools. In fact, in some cases, legal and compliance recognised a potential gap in eComms enforcement efforts, *but no steps were taken to close those gaps or to act on legal and compliance's recommendations*. Financial institutions must not only actively monitor for eComms compliance but must also take steps to: (a) ensure that known compliance gaps are remediated in a reasonable time period and (b) to actually enforce eComms policies, including appropriately disciplining users for policy violations.

- Incorporate processes to routinely survey the business for institutional eComms use. This will help to ensure that legal, compliance and technology receive adequate business input on eComms use and needs that can be incorporated into eComms compliance efforts.
- Routinely review and update supervision/surveillance procedures and lexicons to target/identify the potential use of non-approved eComms channels, personal devices, personal e-mail, personal websites/social media or other off-channel communications.

Ensure that audit procedures include, as appropriate, compliance with eComms

policies and procedures at both the individual user and the technology level.

Evaluate whether/when new application usage or potential individual violations require remediation to archives, updates to policies/procedures or technology changes and ensure action plans for remediation are defined, documented and incorporated into required business-risk remediation monitoring.

- Take appropriate action when/if potential violations are identified, including disciplining violators. Disciplinary efforts should be consistent with standard policy disciplinary actions; it is not necessary to develop special or unique disciplinary procedures solely for eComms policy violations. Disciplinary standards should be clearly documented and communicated to users and may incorporate escalating discipline for repeat violators.

The need to innovate, modernise operations and leverage the most advanced technologies and tools creates consistent pressure on governance functions within financial institutions, including eComms governance functions. Every onboarded application or novel feature can create incremental risk, pressure-testing the strength and efficacy of eComms governance processes and procedures. Regulators, for their part, expect that financial institutions will keep pace with technology and upgrade their compliance processes, as needed, to do so. As seen from the torrent of enforcement actions (and the expected ongoing nature of those reviews), the risks flowing from violations in this area — even mere foot faults — can be significant, imposing both financial penalties and reputational harms. In the current environment, eComms governance, and indeed all data governance, programmes should be upgraded and modernised. That means moving away from siloed compliance regimes primarily geared towards managing *current* risk and integrated governance programmes designed to anticipate *future* risks and challenges, such as continuously reviewing and revising policies and procedures to account for novel technologies (eg GenAI) while continuously monitoring both the technological and regulatory landscapes. Integrated, cross-functional technology-first compliance programmes are not just the movement of the future, they are quickly becoming a necessity in the ongoing struggle to achieve eComms and data compliance.

References

(1) See for example, U.S. Securities and Exchange (SEC) (August 2024) 'Twenty-Six Firms to Pay More Than $390 Million Combined to Settle SEC's Charges for Widespread Recordkeeping Failures' Press Release 2024-98, available at https://www.sec.gov/newsroom/press-releases/2024-98; U.S. Securities and Exchange (SEC) (February 2024) 'Sixteen Firms to Pay More Than $81 Million Combined to Settle Charges for Widespread Recordkeeping Failures', Press Release 2024-18, available at https://www.sec.gov/newsroom/press-releases/2024-18; U.S. Securities and Exchange (SEC) (September 2022) 'SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures', Press Release 2022-174 https://www.sec.gov/newsroom/press-releases/2022-174; Commodity Future Trading Commission (CFTC) (September 2022) 'CFTC Orders 11 Financial Institutions to Pay Over $710 Million for Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods - Registered Swap Dealers and FCMs Admit Use of Texts, WhatsApp and Other Unapproved Methods to Conduct Business', Press Release 8599-22, available at https://www.lscprom.co.uk/news/cftc-orders-11-financial-institutions-to-pay-for-recordkeeping-and-supervision-failures/; Commodity Future Trading Commission (CFTC) (September 2022) 'CFTC Orders a Los Angeles Futures Commission Merchant to Pay $6 Million for Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods', Press Release 8763-23, available at https://www.cftc.gov/PressRoom/PressReleases/8763-23 (all accessed 4th October, 2024).

(2) *Ibid.*, Press Release 2022-174.

(3) U.S. Securities and Exchange (SEC) (September 2024) 'Eleven Firms to Pay More Than $88 Million Combined to Settle SEC's Charges for Widespread Recordkeeping Failures', Press Release 2024-144,

available at https://www.sec.gov/newsroom/press-releases/2024-144 (accessed 4th October, 2024).

(4) U.S. Securities and Exchange (SEC), ref. 1 above, Press Release 2024-18.

(5) See for example, U.S. Securities and Exchange (SEC), '17 CFR §240.17a-4(b)(4)', (broker-dealer retention requirements for communications and retention period) and 17 CFR § 240.17a-4(f)(2)(i) (storage format requirements for broker-dealers), Gov.US, available at https://www.govinfo.gov/content/pkg/CFR-2011-title17-vol3/pdf/CFR-2011-title17-vol3-sec240-17a-4.pdf; Finance Industry Regulatory Authority (FINRA), 'Rule 4511' (broker-dealer record retention), available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/4511; Commodity Future Trading Commission (CFR), 17 CFR § 275.204-2(e) (Investment Adviser retention period), available at https://www.ecfr.gov/current/title-17/chapter-II/part-275/section-275.204-2; Commodity Future Trading Commission (CFR), '17 CFR § 275.204-2' (Investment Adviser storage format), Gov.US, available at https://www.govinfo.gov/app/details/CFR-2016-title17-vol4/CFR-2016-title17-vol4-sec275-204-2; Commodity Future Trading Commission (CFR), '17 CFR § 1.31(b) & (c)', (CFTC general retention period and storage format), Gov.US, available at https://www.govinfo.gov/content/pkg/CFR-2013-title17-vol1/pdf/CFR-2013-title17-vol1-sec1-31.pdf; Commodity Future Trading Commission (CFR), '17 CFR § 45.2(c)', (swap record retention period), and 17 CFR § 45.2(d) (swap record storage format), available at https://www.ecfr.gov/current/title-17/chapter-I/part-45/section-45.2 (all accessed 4th October, 2024).

(6) See for example, Finance Industry Regulatory Authority (FINRA) 'Rule 3110 Supervision', available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/3110; Finance Industry Regulatory Authority (FINRA) 'Rule 3120 Supervisory Control System', available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/3120; Finance Industry Regulatory Authority (FINRA) (December 2007) 'Regulatory Notice 07-59, FINRA Provides Guidance Regarding the Review and Supervision of Electronic Communications', available at https://www.finra.org/rules-guidance/notices/07-59; Commodity Future Trading Commission (CFR), '17 CFR § 275.206(4)-7', (Investment Advisers required to have policies and procedures designed to prevent violations), available at https://www.ecfr.gov/current/title-17/chapter-II/part-275; Commodity Future Trading Commission (CFR), '17 CFR § 166.3', (CFTC regulated entities supervision), available at https://www.ecfr.gov/current/title-17/chapter-I/part-166/section-166.3; National Futures Association (NFA) 'Compliance Rules 2-9 Supervision,, available at https://www.nfa.futures.org/rulebooksql/rules.aspx?Section=4&RuleID=RULE%202-9 (all accessed 4th October, 2024).

(7) See for example, Commodity Future Trading Commission (CFR), '17 CFR §240.17a-4(b)(4)', (broker-dealer communications relating to the business as such), available at https://www.ecfr.gov/current/title-17/chapter-II/part-240/subpart-A/subject-group-ECFR9a3b1ee5e7a78f3/section-240.17a-4; Finance Industry Regulatory Authority (FINRA) 'Rule 2210(b)', (broker-dealer advertising rule relating to communications with the public),, available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/2210; Finance Industry Regulatory Authority (FINRA) 'Rule 3110.09', (retention of internal communications and correspondence), available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/3110; Commodity Future Trading Commission (CFR), '17 CFR § 275.204-2(a)(7), (11), (c)(2), (g)', (investment adviser records requirements implicating to communications), available at https://www.ecfr.gov/current/title-17/chapter-II/part-275. The CFTC regulations are varied but include specific recordkeeping regulations for different regulated entities and include or implicate communications. See for example, Commodity Future Trading Commission (CFR), '17 CFR § 1.35 (a)(1)-(4)', (general recordkeeping for certain CFTC regulated entities, including pre-trade communications), available at https://www.ecfr.gov/current/title-17/chapter-I/part-1; Commodity Future Trading Commission (CFR), '17 CFR § 23.202 (a)-(b)', (swap dealer and major swap participant records), available at https://www.ecfr.gov/current/title-17/chapter-I/part-23/subpart-F/section-23.202; Commodity Future Trading Commission (CFR), '17 CFR § 4.23', (CPO records), available at https://www.ecfr.gov/current/title-17/chapter-I/part-4/subpart-B/section-4.23; Commodity Future Trading Commission (CFR), '17 CFR § 4.33', (CTA records), available at https://www.ecfr.gov/current/title-17/chapter-I/part-4 (all accessed 4th October, 2024).

(8) See for example, National Futures Association (NFA) (January2020) 'Interpretive Notice 9037, Guidance on the Use and Supervision of Websites, Social Media and Other Electronic Communications', available at https://www.nfa.futures.org/rulebooksql/rules.aspx?Section=9&RuleID=9037; Finance Industry Regulatory Authority (FINRA) (January 2010) 'Regulatory Notice 10-06, Guidance on Blogs and Social Networking Web Sites, available at https://www.finra.org/rules-guidance/notices/10-06#:~:text=Firms%20must%20have%20a%20general,subject%20to%20the%20firm's%20supervision.; Finance Industry Regulatory Authority (FINRA) (August 2011) 'Regulatory Notice 11-39, Guidance on Social Networking Websites and Business Communications', available

at https://www.finra.org/sites/default/files/NoticeDocument/p124186.pdf; Commodity Future Trading Commission (CFTC) (February 2009) 'Staff Advisory, Advisory for Futures Commission Merchants, Introducing Brokers, and Members of a Contract Market over Compliance with Recordkeeping Requirements', available at https://www.cftc.gov/sites/default/files/idc/groups/public/@industryoversight/documents/file/recordkeepingdmoadvisory0209.pdf (all accessed 4th October, 2024).

(9) See European Union (EU), 'Markets in Financial Instruments Directive 2014 (2014/65/EU) Art. 16 Sec. 7', available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065 (accessed 4th October, 2024).

(10) See European Union (EU), 'DelReg (EU) 2017/565 Art. 76 Sec. 1', available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0565 (accessed 4th October, 2024).

(11) *Ibid.*, Art. 76 Sec. 6.

(12) European Securities and Markets Authority (ESMA), 'Questions and Answers, On MiFID II and MiFID investor protection and intermediaries topics', p. 49, available at https://www.esma.europa.eu/sites/default/files/library/esma35-43-349_mifid_ii_qas_on_investor_protection_topics.pdf (accessed 14th October, 2024).

(13) Financial Conduct Authority (FCA) (June 2009) 'Codes of Business Sourcebook', (COBS) 11.8.7.

(14) See U.S. Securities and Exchange (SEC) (January 1998) 'Reporting Requirements for Brokers or Dealers Under the Securities Exchange Act of 1934', Rel. No. 34-38245 (62 Fed. Reg. 6469), available at https://www.sec.gov/files/rules/final/34-38245.txt; Finance Industry Regulatory Authority (FINRA) (February 1998) 'NASD Notice to Member 98-11, SEC Approves Rules Regarding Supervision, Review, And Record Retention Of Correspondence', available at https://www.finra.org/rules-guidance/notices/98-11 (accessed).

(15) See Finance Industry Regulatory Authority (FINRA) (June 2003) 'NASD Notice to Members 03-33, Clarification for Members Regarding Supervisory Obligations and Recordkeeping Requirements for Instant Messaging', available at (accessed 4th October, 2024).

(16) See Finance Industry Regulatory Authority (FINRA) (December 2007) 'Regulatory Notice 07-59, FINRA Provides Guidance Regarding the Review and Supervision of Electronic Communications', available at https://www.finra.org/rules-guidance/notices/07-59 (accessed 4th October, 2024).

(17) See Finance Industry Regulatory Authority (FINRA) (January 2010), ref. 8 above, Regulatory Notice 10-06; Finance Industry Regulatory Authority (FINRA), ref. 8 above, Regulatory Notice 11-39; Finance Industry Regulatory Authority (FINRA) (April 2017) 'Regulatory Notice 17-18, *Guidance on Social Networking Websites and Business Communications*, available at available at https://www.finra.org/rules-guidance/notices/17-18 (all accessed 4th October, 2024.

(18) *Ibid.*, Regulatory Notice 10-06, Regulatory Notice 11-39; Regulatory Notice 17-18.

(19) See 'Frequently Asked Questions About Advertising Regulation', B.4.1.Q, posted 10th May, 2024, available at https://www.finra.org/rules-guidance/guidance/faqs/advertising-regulation.

(20) See European Securities and Markets Authority (ESMA) (May 2024) 'Public Statement on the use of Artificial Intelligence (AI) in the provision of retail investment services', available at https://www.esma.europa.eu/sites/default/files/2024-05/ESMA35-335435667-5924__Public_Statement_on_AI_and_investment_services.pdf (accessed 4th October, 2024).