The Growing Regulatory Risk of Off-Channel and Ephemeral Communications

Recent U.S. enforcement actions and statements made by regulators reveal that issues related to the preservation and retention of messaging on personal devices and third-party applications will remain top-of-mind for regulators and enforcers. A recent series of high-profile fines, adopted and finalized policy changes, probes, and regulator warnings underscore the need for companies to review their compliance programs and policies to ensure they adequately and appropriately monitor and preserve all relevant business communications, and for compliance officers to proactively act to mitigate risk that can stem from employee use of personal devices or ephemeral messaging applications. To address these points, **RANE** spoke to **Matthew Bernstein**, **Founder and Information Governance Strategist at Bernstein Data,** for guidance.

WHAT TO KNOW

On September 27, U.S. regulators fined 15 broker-dealers and one investment advisor a combined $1.8 billion in total civil penalties for failing to maintain and preserve business-related communications on personal devices in violation of federal recordkeeping and supervision requirements. The penalties for these financial firms – including Barclays, Bank of America, Citigroup, Credit Suisse, Goldman Sachs, Morgan Stanley, and UBS – ranged between $16 million and $225 million each and represented a landmark collective resolution for the U.S. Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC).

Employees at these firms, some of whom were senior executives, conducted business-related conversations using "off-channel" (unmonitored or unapproved) messaging applications, such as WhatsApp and Signal, on their personal devices and the firms did not, according to the settlements, "maintain or preserve the substantial majority of these off-channel communications." The SEC alleged that the firms' failures "likely deprived" the SEC of communications in various investigations, and the CFTC also alleged that, in some circumstances, the failure to capture required records resulted in records relevant to investigations not being produced to the government.

While the settlements acknowledge that the firms had policies and procedures in place designed to ostensibly prevent employees from using unmonitored or unapproved messaging apps, the SEC and CFTC found that the firms failed to implement an effective system of review to ascertain that personnel were not using personal devices or prohibited communications channels. SEC Rule 17a-4(b)(4) requires that broker-dealers retain originals of all communications received and copies of all communications sent by the broker-dealer relating to its business for at least three years, specifically in an easily accessible place for the first two years. Meanwhile, CFTC-regulated entities must abide by the CFTC's various recordkeeping and reporting requirements, which are narrower than the SEC rules, but impose a broad duty of supervision.

Significantly, one of the firms that settled is an SEC-registered investment advisor. This is notable because, while SEC rules require less expansive recordkeeping rules for money managers than brokerages, investment firms are still required to monitor business communications in order to avert improper conduct. More actions against investment advisors may be forthcoming, as the SEC's enforcement unit has reportedly sent

inquiries to major funds and advisers asking for information about their protocols for off-channel business communications. The request asked these money managers for details on who at their firms oversees retention of electronic communications and information on policies and key staff whose texts and emails are supposed to be archived.

Securities filings on November 8th and 9th by major US private equity firms KKR & Co, Apollo Global Management, and Carlyle Group revealed that the SEC probe into how financial firms track employees' digital communications has also expanded into private equity. The prominence of these asset managers signals that the SEC is escalating its push to investigate Wall Street's electronic communication methods.

Relatedly, albeit on a smaller scale, on September 23, the U.S. Financial Industry Regulatory Authority (FINRA) brought a similar case against a broker-dealer, its president/head of investment banking, and its director of research. The broker-dealer agreed to a $1.5 million fine to resolve allegations that it had failed to preserve and reasonably supervise business-related text messages, which prevented FINRA from fully investigating two matters.

The SEC, CFTC, and FINRA are not the only enforcement agencies scrutinizing the risks associated with personal and ephemeral messaging. In a September 15 speech, Deputy U.S. Attorney General Lisa Monaco announced significant policy changes to the U.S. Department of Justice (DOJ) corporate enforcement strategy. Among other things, the new guidance, *Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group*, addresses the importance of having policies and controls on the use of personal devices to engage in business communications and emphasizes that in order to receive cooperation credit, corporations must have proper document preservation policies and procedures in place to timely preserve, collect, and disclose relevant documents located in the United States and overseas.

In her speech, DAG Monaco made clear that DOJ expects companies to do more to police themselves through investments in corporate compliance. In its evaluation of compliance programs, the DOJ will consider a corporation's policies and procedures, training to employees, and enforcement regarding the use of personal devices and third-party messaging platforms to ensure that business-related electronic data and communications are preserved — and subsequently collected during an investigation.

For companies being investigated by the DOJ, assisting the DOJ is typically necessary to gain cooperation credit and thereby avoid criminal prosecution or reduce the amount of a fine. Companies hoping to obtain cooperation credit are already required to report all relevant, non-privileged facts about individual misconduct to the DOJ. DAG Monaco announced in her speech that the DOJ is going to "do more and move faster" in these cases, and that companies can maximize cooperation credit by self-disclosing individual misconduct in a thorough, transparent, and — importantly — timely manner. To this end, the aforementioned revised guidance requires companies to produce this material "swiftly and without delay,""— although it is not yet explicit what a "timely" production of facts and evidence means in practice — DOJ prosecutors will now consider the timeliness of the production of information, not just the production of materials alone, when determining whether and how much cooperation credit to allocate at the time of resolution.

WHAT TO THINK ABOUT

Compliance officers looking to anticipate communications retention expectations and possible forthcoming regulation should read these enforcement actions as a signal that the SEC and CFTC are looking to make a statement on recordkeeping obligations. On November 2,

SEC Chairman Gary Gensler gave a speech to the Practising Law Institute's 54th Annual Institute on Securities Regulation in which he highlighted the value of high-impact cases that send a message to market participants. He specifically noted that in 2021, the SEC charged JP Morgan a $125 million penalty because employees, supervisors, and managing directors conducted, and failed to maintain, off-channel communications through WhatsApp, text messages, and personal email accounts. That fine was nearly 10 times what the SEC had imposed in previous similar matters, and Chairman Gensler said the fine was so high because market participants "did not act as if they got the message." That case led to a sweep for similar violations, which resulted in the recent charges against 16 financial firms and a combined $1.1 billion settlement with the SEC (in addition to the $700 million penalty by the CFTC). Chairman Gensler reinforced that these send a message that "books and records matter" and that the SEC will "strive to ensure that penalties are not seen as cost of doing business. [The SEC] will use sweeps, initiative, and undertakings to shape market behavior."

Under the Trump administration, in an attempt to avoid protracted proceedings and strain on the resources of the Enforcement Division, the SEC's stance shifted away from requiring admissions of wrongdoing and away from an aggressive prosecutorial stance altogether. But in the recent cases of JP Morgan and most of the 16 firms, the organizations were required to admit wrongdoing, which is rare compared to the typical "no-admit/no-deny" settlements used by the SEC and CFTC. In October 2021, just two months before JP Morgan was charged, Gurbir Grewal, the SEC's Director of Enforcement appointed under Biden in July 2021, announced in a speech that he intended to recommend "aggressive" use of available remedies in enforcement actions, including requiring admissions of wrongdoing in certain cases.

Bernstein believes the SEC's policy shifts to be in-line with the tenor of the Biden administration. Since the financial crisis in 2008 and resulting bailouts for many banks, there has been a pervasive feeling across many parts of society that major financial institutions have not been held to the same standards as other organizations and individuals. **Bernstein** believes that the current SEC and CFTC leaderships' positions and actions — pressing for larger penalties and forcing admissions of wrongdoing — reflect a more aggressive stance on the part of the Biden administration towards large financial services organizations.

Bernstein does not anticipate the results of the U.S. midterms to materially change this. Even if Republicans gain control of one or both of the congressional chambers, **Bernstein** does not foresee any significant changes in direction or a slowdown of priorities regarding regulation of electronic records, especially as the executive branch continues to control the agencies' leadership composition. The populist character of both political parties means that both are prioritizing appealing to and protecting Main Street rather than Wall Street. **Bernstein** could, however, see a shift in the thresholds of various regulations and enforcement actions should the Republican party gain power in the midterms. For instance, he could see Republicans shifting or pushing back on the scope of the reporting for smaller banks and organizations in an effort to avoid overly burdensome requirements. While it is clear that there have been some aggressive policy shifts from U.S. regulators in the last couple of years, **Bernstein** is not altogether convinced that these enforcement and guidance pushes from the SEC, CFTC, and the DOJ, viewed together, connote an explicit trend of greater recordkeeping enforcement. Instead, he thinks recent enforcement actions, guidance, and speeches show the recognition by regulators that the diversity of "records" and the speed of technological change must be addressed.

This recognition can be seen in recently adopted amendments to the SEC's recordkeeping rules applicable to broker-dealers, security-based swap dealers, and major security-based swap participants. On October 12, the SEC voted to

adopt the amendments in an effort to modernize recordkeeping requirements "given technological changes over the last two decades and to make the rule adaptable to new technologies in electronic recordkeeping." **Bernstein** says that these amendments do not change the recordkeeping obligations of regulated firms, nor do the amendments change what the SEC is looking for. However, **Bernstein** says, the amendments, by using technologically-neutral terminology rather than its outdated descriptions of near-obsolete devices such as optical discs, allow the SEC to future-proof the scope of its supervisory expectations in the hope that these amendments will better withstand the passage of time and accompanying technological advances.

Beyond the amendments, **Bernstein** thinks the SEC may provide more guidance about new technologies and communications platforms so that there is no question that it has enforcement purview and capability. He expects the SEC to get more specific about the kinds of things the Commission is concerned about so that the message will be clear that it is going to enforce its requirements around retention and supervision across whatever platform it finds people using.

Part of that effort may be currently underway, as the SEC has reportedly begun a probe into the use of outside messaging services at major investment firms, asking money managers for recordkeeping policy details, communication channels, and information on key staff whose texts and emails are supposed to be monitored and retained. This inquiry into off-channel communications could be the harbinger of not only more guidance, but potentially more penalties.

Bernstein is not surprised to see increasing interest by the SEC in investment companies and electronic communications, as he says that there has been a general increase in SEC scrutiny of investment funds in the past few years and a recognition that hedge funds and other non-bank market participants play an increasingly large role in financial markets. He thinks the expanding use of communication and collaboration tools is of great concern to regulators, especially in light of the increased use of more secure and thus more secretive communication tools. He says that as individual participants in financial markets read more about people, in all walks of life, using encrypted platforms like Telegram or Signal they start to think about what that could mean for them.

WHAT TO CONSIDER

This type of thinking is not always indicative of nefarious intent, says **Bernstein**, although it can be. Much of the time, he says, workers adopt new methods of communication either due to convenience — because it is more efficient, they can be more productive — or convention — because their peers or clients use it, they must also to remain competitive. The issue, **Bernstein** cautions, is when these platforms and tools are used by teams without compliance departments being involved in their introduction. To resolve this, **Bernstein** recommends expectations reinforcement and control assumptions from compliance teams. Compliance teams need to reinforce that employees engaged in SEC-supervised activities can only conduct those activities on systems the company has access to. There should be a list of acceptable systems, and if a platform or tool is not on that list, the message should be that it should not be used. The "first line of defense", such as the management of sales and trading departments, should be clearly and repeatedly emphasizing expected behavior, so that everyone understands what they should and should not be doing.

The "second line of defense" is that a compliance team needs to work with its company's IT department to implement governance controls that prevent employees from adding unauthorized systems into company devices without proper review. Should an employee propose a new platform or tool, that review, **Bernstein** says, should include questions like: Is this information able to be monitored and retained, are the messages available in timely fashion to surveillance technology solutions, and can messages of interest be retrieved with fidelity

to their original context? (This is in addition to the standard business continuity and information security concerns.) Information governance policies and procedures for messaging platforms should be cross-team conversations that include people from not only compliance, legal, and IT departments, but also a representative from the team that wants the tool who can discuss the ways in which it will be used.

This type of conversation should also be held with executives and board members who may prefer to communicate off-channel because they are discussing highly sensitive information and do not want other people in the company who can look at production systems to have access to it. But they still need to abide by the law, and having conversations with compliance, legal, and IT can facilitate a compromise, such as creating a highly secure platform to which only specific people have access.

When it comes to trying to change behavior, **Bernstein** does not think admission of wrongdoing has as much impact on compliance compared to fines of the magnitude recently seen from the SEC and CFTC. **Bernstein** says shareholders, particularly institutional shareholders, are primarily concerned about the financial impact of wrongdoing rather than the legality of it. Thus, when trying to disincentivize misconduct by employees who are focused on the firm's bottom line, **Bernstein** says it is often more helpful for compliance professionals to present a fine in the context of the profits generated. When the consideration is not "the fine barely makes a ripple in total earnings," but rather "did the fines from misconduct actually make the business in question unprofitable?," the numbers start to take on a shape that discourages bad behavior.

Given that the SEC has repeatedly encouraged corporations to proactively examine their document preservation policies and procedures and self-report any failures before the SEC identifies violations, companies should take steps now to evaluate their situations. To assess current risk with regard to employee use of off-channel or ephemeral messaging applications, companies should review: existing employee use of platforms; the adequacy and modern relevance of existing business policies (do they address current ways technology is used?); relevant legal constraints (are there any data privacy laws that limit monitoring ability?); industry-specific preservation obligations; communications training materials and cadence; and monitoring capabilities (is the company able to identify non-compliance?).

Companies must review their compliance operations and implement policies and controls that are practical and enforceable. Given the global popularity of ephemeral or encrypted messaging apps (**Bernstein** provides the example of how pervasive WeChat is in China, and how Chinese banking regulators use it to communicate), it may be impossible for employers to ban them outright. But companies should adopt approaches that balance the concerns of U.S. regulators with the needs of the business, or they will risk coming to the attention of enforcement authorities for failing to retain required records and properly supervise employees.

Unfortunately, even knowing the SEC, CFTC, and other regulatory agencies have communications retention and supervision in their crosshairs, determined bad actors, says **Bernstein**, will find a way to communicate without their correspondence being captured or surveilled if that is their goal. **Bernstein** says that in light of the focus from regulators, he expects a risk-shifting swing from personal devices being used for work back to corporate-provided devices. There is no way to stop people determined to cheat, but what companies can do, **Bernstein** suggests, is to make clear to both employees and clients, regularly, that business communications should take place on authorized business platforms and devices that have compliance functionality, which will put companies in a stronger compliance position should regulators come calling.

RANE
Risk Assistance Network + Exchange

ABOUT THE EXPERT

Matthew Bernstein led information management practices in various businesses at Deutsche Bank for more than 20 years and now leads his own firm. BernsteinData helps clients implement effective solutions for Information Governance risk and business objectives in Records Management, Information Security, Data Privacy, Legal and Regulatory Responsiveness, and Operational Efficiency. At Deutsche Bank, Matthew was Head of Group Information and Records Management, with global responsibility for Records Management, Archiving, and eDiscovery Operations. Together with the Bank's CISO and CDO, he was responsible for information governance at the bank, which employs more than 100,000 people in over 60 countries.

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is a global risk intelligence company that provides risk and security professionals with access to critical insights, analysis, and support, enabling them to more effectively anticipate, monitor, and respond to emerging risks and threats. RANE clients benefit from improved situational awareness, more efficient access to relevant intelligence and expertise, and better risk management outcomes. Join the millions who are tapping into the collective wisdom of the world's largest community of risk and business professionals. For more information about RANE, visit www.ranenetwork.com.