Why depository institutions, with or without affiliated securities firms, can and should manage employee use of personal devices for work-related communications

Received (in revised form): 9th July, 2024

Richard H. Harvey, Jr
Executive Vice President, General Counsel and Director of Compliance Risk, Beneficial State Bank, USA

Michael J. Leotta
Partner, WilmerHale, USA

Gautam Sachdev
Partner, AlixPartners, USA

Richard H. Harvey, Jr

Michael J. Leotta

Gautam Sachdev

Journal of Financial Compliance
Vol. 8, No. 2 2024, pp. 154–166

2398-8053 (2024)

***Richard H. Harvey, Jr.**, is an experienced executive-level legal and compliance leader and a noted expert in developing and implementing risk-based compliance and anti-money laundering programmes for traditional and non-traditional financial institutions. Richard currently serves as Executive Vice President, General Counsel and Director of Compliance Risk for Beneficial State Bank. Prior to joining Beneficial, Richard served as the General Counsel and Chief Compliance Officer for World Open Network. He has also served as the Chief Compliance Officer for Colonial Savings, FA and General Counsel and Chief Compliance Officer at two start-up financial technology companies. Richard is a graduate of the Catholic University of America Columbus School of Law. He served as an enforcement and litigation attorney with the Office of Thrift Supervision from 1986 to 1993. During his career, Richard has held key roles in many areas of bank compliance. He has had responsibility for managing his institution's legal departments, Bank Secrecy Act (BSA), privacy, consumer compliance, safety and soundness and information technology examinations. Additionally, Richard is a certified regulatory compliance manager and anti-money laundering and fraud professional. He currently serves as a faculty member for the American Bankers Association (ABA) School of Compliance Risk Management. Richard has also taught a course on compliance management at the Stonier School of Banking. In 2017, he was selected to serve on the Consumer Financial Protection Board Community Bank Advisory Council. In 2019, Richard was recognised for his service to the financial services industry with the ABA's Distinguished Service Award. Richard is a frequent speaker at conferences and seminars on the topics of compliance risk management, privacy, BSA and anti-money laundering and fair lending. In 2001, Richard testified on behalf of the ABA before the House of Representatives Banking Committee concerning financial institutions' efforts to combat identity theft.*

***Michael J. Leotta** conducts internal investigations and represents corporations and individuals in white-collar criminal law and regulatory enforcement matters. He regularly represents US consumer banks, global correspondent banks, broker-dealers, investment advisers and FinTech companies in a broad range of matters, including defending financial institutions' compliance with the Bank Secrecy Act and related anti-money laundering rules, securities law and the Foreign Corrupt Practices Act. He represents clients in investigations and examinations by the Department of Justice and state prosecutors; domestic and international financial*

regulators such as the Federal Reserve Board of Governors, the Securities and Exchange Commission, the Financial Industry Regulatory Authority, the Commodity Futures Trading Commission, the Financial Crimes Enforcement Network, the New York Department of Financial Services, and the UK Financial Conduct Authority; state attorneys general; and congressional committees. Before joining WilmerHale in 2011, Michael served for nine years in government, including in the White House Counsel's Office under President Barack Obama, as an assistant US attorney prosecuting fraud and public corruption and as Appellate Chief and Ethics Adviser at the US Attorney's Office for the District of Maryland. Michael recently served as a national chair of the American Bar Association's White Collar Crime Committee and currently serves as a co-chair of its Financial Institution Fraud/Money Laundering and Patriot Act Subcommittee.

***Gautam Sachdev** is a seasoned risk and compliance professional with more than 16 years of in-house experience in various global and regional roles in the areas of compliance, investigations, risk management, operations, governance, technology and risk assessment in the second line of defence. Gautam has experience working at major financial institutions in Australia, Brazil, the UK and the US. Previously, he was with Macquarie Group as Managing Director, Global Head of Risk Surveillance, and Chief Product Owner for Risk Management, overseeing operations, governance, technology and strategy. Prior to joining Macquarie Group, he held similar roles at Citibank and HSBC. Gautam has an MBA from Northwestern University's Kellogg School of Management and a master of science in electrical engineering from New York University. Recently, he attended Oxford University and completed the programme on leading sustainable corporations. Gautam is a published speaker at various industry forums for risk and compliance topics, with a keen focus on markets compliance, corporate investigations and ESG.*

Abstract

This paper shows how the failure to monitor for and prevent off-channel communications poses risk to traditional depository institutions that are not subject to the jurisdiction of securities-law regulators and shows how those institutions can mitigate that risk. US securities regulators have cracked down on broker-dealer, investment-adviser and futures commission merchant employees' use of unapproved personal devices and applications for business communications, imposing over US$2.8bn in penalties between December 2021 and April 2024. However, because there have not, at the time of writing this paper, been similar enforcement actions against traditional depository institutions that do not have securities affiliates, many traditional banks without securities affiliates have continued with business as usual. Nonetheless, the OCC has recognised that electronic communications can constitute records that must be retained pursuant to specific rules and that banks' failure to maintain adequate record retention systems in general can create significant reputation, transaction, credit and compliance risks. This paper aims to illuminate those risks and offers suggestions about how to address them.

Keywords: off-channel communications, business communications, personal devices, text messaging, record keeping, e-communications surveillance

DOI: 10.69554/RDJK5791

INTRODUCTION

The purpose of this paper is to show how the failure to monitor for and prevent off-channel communications poses risk to traditional depository institutions that are not subject to the jurisdiction of securities-law regulators and how those institutions can mitigate that risk.

Starting in late 2021, US securities regulators began a wave of crackdowns on broker-dealer, investment-adviser and futures commission merchant[1] employees' use of unapproved personal devices and applications for business communications. Enforcement

Beneficial State Bank, 1438 Webster Street, Suite 300, Oakland, CA 94612, USA
E-mail: rharvey@beneficialstate.com

WilmerHale, 2100 Pennsylvania Avenue NW, Washington, DC 20037, USA
Tel: +1 202 663 6526;
E-mail: michael.leotta@wilmerhale.com

AlixPartners, 909 3rd Ave, New York, NY 10022, USA
Tel: +1 212 365 8331;
E-mail: gsachdev@alixpartners.com

sweeps by the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) led to charges against scores of firms for failing to reasonably supervise their employees' use of these unapproved communications channels, yielding over US$2.8bn in penalties between December 2021 and July 2024.[2] During this same time period, the Financial Industry Regulation Authority (FINRA) brought over 25 enforcement actions against individual registered representatives and at least one action against a broker-dealer.[3] As a result, only the most risk-seeking — or foolhardy — securities firms are still relying on pre-2021 controls to prevent the use of unapproved electronic communications channels and using similar antiquated tools to preserve business-related communications.

There have not, at the time of writing this paper, been similar enforcement actions against traditional depository institutions that do not have affiliated SEC or CFTC registered broker-dealers, investment advisers or futures commission merchants. Accordingly, many traditional banks without broker-dealer, investment-adviser or CFTC-registered affiliates have continued with business as usual, relying on the fact that the laws and regulations enforced by the SEC and CFTC do not pertain to them.

Traditional banking institutions may not realise the extent of the risk that such complacency poses. The failure to monitor employees' off-channel communications may allow employee policy violations to go undetected, customers to be defrauded and crucial communications to be lost. Should a bank receive a subpoena, the Department of Justice (DOJ) and Federal Trade Commission (FTC) have recently made explicit that they expect a recipient to preserve and produce off-channel messages that the recipient might not otherwise be monitoring or collecting — on the pain of spoliation sanctions if such communications are not preserved.[4] And if a bank finds itself the subject of a DOJ investigation, the prosecutors will evaluate the company's compliance programme in part by how it deals with such messages.[5] Finally, it is not far-fetched to expect prudential banking regulators to deem a failure to preserve such communications to be an unsafe banking practice.[6]

This paper aims to illuminate those risks and offers suggestions about how to address them. In addition, the paper shares insights on how to perform continuous assessments of the corporate communications compliance programme, to help ensure regulatory and reputational risk is appropriately managed.

BACKGROUND OF OFF-CHANNEL COMMUNICATIONS ENFORCEMENT ACTIONS: US$2.8BN IN PENALTIES IN TWO AND A HALF YEARS

When this paper refers to off-channel messages on unapproved platforms, it means business-related communications[7] sent via SMS text message or a similar electronic communication platform (such as iMessage, WhatsApp or Signal) using employees' personal mobile phone or tablet.[8] Prior to December 2021, financial institutions did not routinely monitor or preserve communications sent through employees' personal devices.[9]

The recent off-channel communications settlements reveal that banks and broker-dealers have long had policies prohibiting employees from using unapproved communications channels on their personal devices to communicate about business, but prior to December 2021, these policies went largely unenforced.[10] Indeed, in many cases, senior-level supervisors — 'the very people responsible for supervising employees to prevent this misconduct' — themselves routinely sent business-related communications using their personal devices.[11] Much of this off-channel communication through personal devices may have occurred during the COVID-19 pandemic, when many employees found themselves working from home, but the

settlements reveal that securities personnel were communicating off-channel about business even before the pandemic, and the practice did not necessarily stop when they returned to the office.

It has long been clear that various securities rules and regulations required securities firms to preserve off-channel business-related communications, even if they were sent on personal devices. SEC Rule 17a-4(b)(4), adopted under Section 17(a)(1) of the Securities Exchange Act, requires that broker-dealers preserve in an easily accessible place 'originals of all communications received and copies of all communications sent [. . .] by the member, broker or dealer [. . .] relating to its business as such'.[12] Although originally drafted to apply to paper correspondence, the SEC has applied this rule to e-mail and Internet communications since 1997.[13]

Regulations applicable to investment advisers and CFTC registrants impose similar obligations, although they are narrower than the SEC Rule. Advisers Act Rule 204-2(a)-7 requires investment advisers to make and keep certain books and records relating to their investment advisory business, including, among other things (and subject to certain exceptions):[14]

> [o]riginals of all written communications received and copies of all written communications sent by such investment adviser relating to: (i) Any recommendation made or proposed to be made and any advice given or proposed to be given; (ii) Any receipt, disbursement or delivery of funds or securities; (iii) The placing or execution of any order to purchase or sell any security [. . .]; or (iv) [. . .] the performance or rate of return of any or all managed accounts [. . .] or securities recommendations.

CFTC Regulation 1.35(a)(1) sets forth some of the books and records that are required to be created and maintained by CFTC registrants, including 'all oral and written communications provided or received concerning quotes, solicitations, bids, offers, instructions, trading, and prices that lead to the execution of a transaction in a commodity interest' whether transmitted by telephone, voicemail, facsimile, instant messaging, chat rooms, electronic mail, mobile device or other digital or electronic media.[15]

There are no such rules or regulations pertaining to federally registered banks standing alone — that is, banks that do not have affiliated broker dealers, investment advisers or CFTC registrants — so there is no history of recent enforcement actions in this space. However, there had been more than a dozen SEC and FINRA enforcement actions prior to December 2021, finding that a broker-dealer or its personnel violated applicable rules by communicating about business using unapproved, off-channel platforms that went unpreserved.

What changed in December 2021 was the *size* of the penalties imposed. Just one year prior, in September 2020, the SEC imposed a US$100,000 penalty against JonesTrading Institutional Services for failing to preserve business-related text messages sent or received by several of its registered representatives on their personal devices in violation of the same recordkeeping rules.[16] Prior to December 2021, the largest relevant recordkeeping penalty ever imposed by the SEC had been US$15m.[17]

In the face of this precedent, the combined US$200m fine imposed by the SEC (US$125m) and CFTC (US$75m) on JPMorgan Securities in December 2021, for failing to preserve off-channel communications and failing reasonably to supervise its employees' communications practices, sent a shockwave through Wall Street.

Gurbir Grewal, the SEC's Director of Enforcement, has defended the size of this penalty as necessary for deterrence, claiming that the much smaller prior penalties did not work. But rather than examining firms

to see whether that massive penalty had the desired deterrent effect, the SEC and CFTC went on to impose more than US$2.8bn in fines on at least 55 other firms,[18] largely for actions *preceding* the JP Morgan Securities settlement.[19]

Together, these settlements recognise that virtually all employees at the settling broker-dealers, investment advisers and CFTC-registrants across Wall Street used their personally owned devices to send business-related text messages, despite these firms' policies and procedures prohibiting the same. The settling firms generally admitted the widespread and pervasive use of unapproved messaging platforms like text messages and WhatsApp on personally owned devices for business-related messages. They admitted that in many cases, senior personnel who were responsible for supervising others' compliance with these recordkeeping rules themselves used unapproved messaging platforms. And they each agreed to retain a compliance consultant to review their off-channel communications-related policies and procedures, training, detective controls, technological solutions, preventative controls, incorporation into traditional surveillance, and disciplinary framework.[20]

SEC Commissioner Mark T. Uyeda has criticised the agency's enforcement actions in this space, arguing that 'insufficient clarity' regarding what constitutes a business-related communication may have resulted 'in a lack of understanding, and potentially fair notice, of novel interpretations that the SEC has undertaken' in these enforcement actions.[21] He further described the penalty amounts as 'astonishing, particularly since no investor harm has been identified'.[22]

These settled enforcement actions demanded the attention of in-house lawyers and compliance officers at securities firms. But in-house lawyers and compliance officers at traditional and non-traditional banks should take note as well, so that they too are not surprised if their regulators and law enforcement agencies interpret the banking rules to also require the prevention or preservation of off-channel communications on personal devices and impose similarly eye-popping penalties for activity that has long been (at least implicitly) accepted.

WHY IT IS IMPORTANT FOR BANKS THAT DO NOT HAVE AFFILIATED SECURITIES FIRMS TO PREVENT AND/OR PRESERVE OFF-CHANNEL COMMUNICATIONS

Banks without affiliated broker-dealers, investment advisers or CFTC registrants should also be concerned about off-channel communications. Although federal banking regulators have not issued prescriptive rules regarding the preservation of all business-related communications, along the lines of those rules applicable to securities firms, the Office of the Comptroller of the Currency (OCC) has recognised that electronic communications *can* constitute records that must be retained pursuant to specific rules.[23] And the OCC has recognised that the failure of banks to maintain adequate record retention systems in general 'can create significant reputation, transaction, credit and compliance risks'.[24]

Unpreserved business-related communications present these legal, compliance, credit and reputational risks, which should be mitigated. Similar to the cache of state and federal laws and regulations governing consumer privacy that were promulgated in the wake of the Financial Services Modernization Act of 1999, it should be no surprise if state and federal banking regulators begin to consider whether specific rules should be put in place to evaluate the controls banks have to ensure employees are not engaged in communications that are outside the banks' covered communication channels.

Prudential regulators could interpret the requirements of safety and soundness to require banks to prevent and/or preserve

off-channel internal communications or communications with the public.[25] Even if regulators do not deem the failure to preserve such communications to be a safety or soundness issue, the prevalence of off-channel communications creates risks for a bank:

1. the risk that important decisions will not be documented;
2. the risk that employees may commit misconduct in communications that the bank is not aware of — whether that be policy violations like password sharing or criminal conduct like defrauding the bank or its customers;
3. the risk that documentation necessary for civil litigation or subpoena compliance will not be preserved. To this point, the DOJ and FTC have recently made explicit that they expect a recipient to preserve and upon request to produce off-channel messages that the recipient might not otherwise be monitoring or collecting — on the pain of spoliation sanctions if such communications are not preserved;[26] and
4. if a bank finds itself the subject of a DOJ investigation, the prosecutors will evaluate the company's compliance programme in part by how it deals with such messages.[27]

Banks do maintain communications now, and they need to incorporate off-channel communications into that regime. The idea of maintaining bank records is not foreign to banks. Document retention rules have been in place for many years and regulators routinely review a bank's compliance with records retention requirements. In fact, both federal and state law mandate strict adherence to specific document retention timeframes.

Today, although not specifically required by rule or regulation to preserve all business-related communications, banks without affiliated broker-dealers, investment advisers or CFTC registrants would benefit from including off-channel communications in their scope of compliance and legal risk management. Developing and implementing policies and procedures to cover employees' off-channel communications can help ensure that employees are aware of the boundaries the bank has established for using such communication tools. Establishing such a policy, which will be monitored and audited, will demonstrate the importance the bank attributes to ensuring that customer communications are consistent with the bank's expectations.

Banks currently make efforts to monitor and remain aware of employees' communications. It is just as important to monitor and be aware of off-channel business-related communications. Consistent with regulatory requirements and expectations, banks are familiar with creating policies concerning communications between employees, their customers and prospective customers. These communications include written and verbal disclosures, e-mail and text messages and other communication methods. These communication methods are typically subject to monitoring because they are within the bank's infrastructure. However, with the explosion of communication devices and platforms, coupled with the fact that many employees are working off-site since the advent of COVID-19, the use of non-authorised or non-bank-managed communication channels that are outside the bank's infrastructure has increased exponentially. As a result, it is becoming increasingly more difficult to know whether employees are engaging in conversations that are inconsistent with the bank's requirements.

The fact that the securities regulators have focused and continue to focus on the risks associated with off-channel communications should be a wake-up call for banks without affiliates subject to such regulations. The risks of customers being adversely impacted via off-channel communications are real. And the fines levied against institutions without effective controls to mitigate such risks have been substantial. Thus, it is only a matter of time before the banking

regulators will begin to hold banks without securities affiliates to the same standards.

HOW CAN BANKS ADDRESS THIS RISK?

To develop a comprehensive communications compliance programme, firms should focus on assessing their communications framework — starting with necessary policy updates and review of business channels — to determine what restrictions are appropriate to optimise their retention and monitoring capabilities.

Another important factor for firms to focus on is conduct risk (or lack thereof). Comprehensive assessments frequently reveal the need to adjust for e-communications by enhancing internal policies and procedures, implementing new training and awareness activities and adapting monitoring tools to these new channels.

Given the concerns on hand and the constant catch-up game that the industry is playing with emerging communications technologies, the time to act is . . . yesterday. When Apple launched the first-generation iPhone in June 2007, few anticipated how quickly 'smartphones' would become a necessity. As adoption spread, smartphone users flocked to an ever-increasing array of communications tools, such as SMS, WhatsApp, WeChat, Facebook Messenger, Twitter Direct Messages, SnapChat, GChat, FaceTime, voice messaging, etc., which progressively displaced e-mail and voice calls on traditional phone lines. The enduring increase in remote working triggered by the COVID-19 pandemic further accelerated this transition.

For financial services firms, the flexible working trend has had far-reaching consequences, putting regulatory demands in direct conflict with the needs of tech-savvy clients and employees. On a trading floor, staff are surrounded by posters reminding them to refrain from using their personal phones on the floor. The business risk manager and/or the compliance officer is sitting nearby and will not shy away from slapping a wrist due to non-compliance. However, when operating outside such a controlled environment, an employee is more likely to make a call from their personal phone or to WhatsApp/WeChat message a co-worker. Indeed, with more staff working from home, and in some cases a shared apartment, work and life boundaries blurred, and firms started noticing a dip in communication volumes on approved corporate communication channels.

This transition to off-channel communications is a significant development that suggests that the quality of regulatory compliance is now largely dependent on voluntary employee compliance. Whereas the communication platform integrated into most trading platforms originally managed to preserve a complete record of trading activity, the reality today is that most organisations may have incomplete communications data, and their ability to analyse trades and orders may be significantly diminished.

With this backdrop, recent scrutiny by US, UK and German regulators was to be expected, and these developments should be of equal concern to the financial services industry, even if the solutions are not particularly straightforward.

Although there is not any one single tool, like clear policies or frequent training, that will put an end to the practice of sending messages on unapproved channels, the SEC has telegraphed the seven areas that it thinks firms should assess. They are the same seven areas that each settling firm's consultant is directed to review in the JP Morgan settlement and the subsequent settlements. Every financial institution should itself, or with the assistance of counsel or consultants, evaluate these areas:

Policies and procedures

While most firms have policies and procedures in place, they may not be comprehensive enough. Policies and procedures

must be clear about what is permitted and what is prohibited, and the category of business communications to retain should be as broad as SEC Rule 17a-4(b)(4). Some firms will make exceptions for administrative or logistical communications (eg 'I'm running late for the meeting') but others will not.

In a November 2023 speech, SEC Commissioner Mark T. Uyeda expressed how ambiguous the rule is, asking: 'If co-workers text each other about having lunch — is that a business record? What if they discuss business at lunch, but the text message makes no mention of the business to be discussed?'[28] Uyeda continued: 'Ensuring that the SEC's rule book evolves with technological developments would help management and compliance professionals know what standards they need to meet and will help prevent enforcement actions going forward.'[29]

On the other hand, in a December 2023 *Wall Street Journal* article, Grewal stated:

> we're not looking for communications about people making lunch plans or dinner plans or after-work drink plans. We're looking for communications related to the business, and records that have to be kept. So if there is misconduct, we are able to piece together what happened, and folks are unable to evade those retention requirements and evade us by using ephemeral messaging or off-channel communications.[30]

From a policy point of view, such contexts should be detailed to ensure that employees appreciate where to draw the line between business and non-business communications. It is also important to note that business communications may happen in a non-business setting. To ensure records completion and compliance, the firm should allow for mechanisms to bring such business communications into their books and records.

Training

Firms must also enhance their training and awareness programmes. These initiatives should reinforce messaging from senior executives and managers on the importance of using approved communications platforms. Senior executives and managers should continually demonstrate in their communications and actions the importance of using approved communications platforms and should themselves refrain from engaging in any business-related communications on an unapproved platform.

Training must address not just what is a business communication that must be kept on firm channels, but what to do when (inevitably) an employee gets one or accidentally sends one on their personal device/via an unapproved channel.

Training must be combined with education about how seriously the bank will take any infractions. In the past, general trainings have not worked if violations were common and the bank looked the other way or supervisors condoned the practice.

The SEC has required quarterly attestations; although in the authors' experience, general attestations have not worked in the past.

There is an element of training, and then there is the element of ensuring that employees have developed their understanding of the subject via such training. Post-training assessments often help gauge the knowledge gaps. Assessment records should be maintained and ensure there is a carrot-stick approach incentivising the completion of both training and assessment.

Detective controls

Traditionally, surveillance programmes ensure compliance via mechanisms such as lexicons run across approved communications, searching for references to unapproved communications. Given the evolving world of communications, it is equally important to

ensure additional measures are in place, such as foreign lexicons, random sample searches, machine-learning-based algorithms for targeted searches, artificial-intelligence-based algorithms to assist with gap analysis, and the like.

Where communications surveillance highlights potential concerns, a thorough and well-documented investigation must be conducted to verify and conclude the analysis. Thereafter, preventative measures should be considered in order to avoid such issues in the future.

Keeping a watchful eye out for data privacy concerns is very helpful. With different state laws and business across geographies (both within and outside the US), firms need to be equally mindful to not trip over personal data privacy and protection requirements.

Technological solutions

The SEC-imposed consultants required firms to adopt technological solutions to meet the record retention requirements and to assess the likelihood personnel will use these solutions and track related metrics in some fashion. Some firms have adopted two-device solutions (personal device and business device), whereas others employ software-based bring-your-own-device-solutions (deploying mobile data management software on personal phones). Firms also need solutions for chat functions of videoconferences, social media and web-based electronic communications.

Firms should conduct a thorough analysis of business requirements and thus solutions that are best suited for the business and in line with regulatory compliance requirements. While a non-compliant solution is a non-starter, a solution that is not fulfilling business requirements will trigger the business to conduct communications on a different channel, thus defeating the purpose of a compliant communications programme.[31]

Preventative controls

Firms must consider what restrictions will help prevent the issues to permeate and find those that will prove to be an effective deterrent. Such restrictions should be balanced, though, so as to not to trigger non-compliant behaviour in order for the business to operate. Measures to prevent the use of unauthorised communications methods should be considered. The SEC settlements give as an example a rule of not bringing personal phones to the trading floor. Other possible controls include turning off chat functionality in videoconferences, limiting the use of pre-approved emojis/emoticons, or the like.

Ongoing electronic communications surveillance

Once they adopt compliant solutions, financial institutions should make sure their ongoing electronic communications surveillance incorporates these newly approved e-communications.

Disciplinary framework

Where there is a lack of reaction to a breach of policy, supervision may have broken down. Firms should ensure that a robust disciplinary framework is in place which provides transparency to issues and outcomes. Most people want to be compliant, so behaviour change may be seen even from mild discipline and admonitions if they are swift and certain. On the other hand, more forceful penalties will be warranted where there are aggravating factors, such as intentional efforts to evade controls or other policy violations.

Changes in behaviour over time are worth noting via regular management information reporting. Firms should note that the SEC has required settling firms to report all related discipline for two years. Record retention of outcomes from disciplinary meetings should be maintained.

Aside from these seven categories set forth in the SEC settlements, it is crucial that firms implement a regular and effective means to assess conduct risk. This requires that the tracking of conduct risk on a desk-by-desk basis is held to the same performance standard as revenue and profitability. Such a change to the measurement of performance is one of the most effective means to communicate to employees the weight the firm places on conduct. The assessment of conduct risk by the business (the first line of defence) can include market- and client-related conduct data, periodic conduct risk oversight and evaluation activities, and reviewing employee and client feedback.

It should also be noted that these are typically not the measures that the second line of defence is prepared to work with. Measurement and ownership need to start with the first line of defence. The second line of defence, by definition, should provide oversight and governance, and drive consistency throughout the organisation. Such measurement then needs to be followed by decisive action. There are four milestones to this journey, namely:

1. Set the direction.
2. Build engagement.
3. Execute.
4. Maintain focus.

To operationalise these milestones, firms should not underestimate the importance of developing a strong culture by implementing initiatives that align incentives with good behaviour.

Thereafter, it is necessary to monitor and analyse key risk indicators to identify emerging trends, themes and the underlying causes of misconduct. Conduct cannot be improved unless it can be measured, so this is about ensuring that initiatives are working and that the outcome demonstrates an improvement trend.

When measuring misconduct via pattern anomalies measured against risk indicators, it is important to be mindful that behavioural differences may vary significantly based on the region. This can include market practices as well as the style, mode and frequency of communications. As a result, a one-size-fits-all approach may not produce the desired outcomes. For example, because a customer or employee with overseas personnel and/or business interests may use more than one language to communicate, using single-language detection models may not be most suitable. Similarly, when using pattern detection techniques, frequency of communications and length of communication may vary based on type of platform used. As a result, surveillance routines must search differently to detect those conversations requiring further review in more frequent and shorter-burst communications channels, such as WhatsApp and WeChat (where these are permitted), as opposed to longer e-mails.

And finally, ensure there is a carrot and stick approach. The information gathered is of no use unless it is evaluated and addressed for positive reinforcement, as well as to help resolve negative outcomes.

CONCLUSION

Communication habits and communication technologies have evolved over the last decade. SMS messages, iMessage texts, WhatsApp messages, and other text-message communications are ubiquitous today. As a result, business-related communications are being sent on unapproved and unpreserved channels throughout the financial services industry. Fraudsters and nefarious market players, too, now communicate with victims, clients and other counterparties using these means.

Securities and commodities industry regulators have cracked down on this practice over the past few years. The recent fines (exceeding US$2.8bn) are a sobering reminder of the fact

that securities market institutions can do (and doubtless shall do) better to retain and monitor business communications. While most market participants that are subject to securities regulatory requirements (those regulated by the CFTC, Financial Conduct Authority, SEC and FINRA, for example) have taken steps to retain and monitor such communications, all financial industry participants — including depository institutions without affiliated securities firms — need to thoroughly review their communication compliance programmes for gaps and areas of improvement.

As we discuss above, conduct risk and fraud are not foreign concepts to traditional depository institutions. The OCC and the US DOJ's expectations for record retention apply to traditional banking institutions and beyond. The risk financial institutions face from their personnel sending unretained, unmonitored communications is high: monetary fines; cease and desist orders; reputational damage; and even imposed monitorships. Any one of these could be a significant setback to the bank's bottom-line and, perhaps more importantly, a setback to customers' trust.

The good news, however, is that by taking lessons from the securities enforcement actions, all financial institutions can control these risks. Banking institutions, regardless of whether they have affiliated securities firms, should look to enhance their overall conduct and regulatory compliance programmes by implementing communications retention and monitoring. The risks of failing to do so are too high.

Notes and references

(1) For simplicity, this paper will refer to futures commission merchants, although the relevant rules pertain to futures commission merchants, swaps dealers, and certain introducing brokers.

(2) As of 5th April, 2024, the SEC has charged 57 firms and collected over US$1.7bn in fines. See US Securities and Exchange Commission (3rd April, 2024) 'SEC Charges Advisory Firm Senvest Management with Recordkeeping and Other Failures', available at www.sec.gov/news/press-release/2024-44 (accessed 11th September, 2024); US Securities and Exchange Commission (9th February, 2024) 'Sixteen Firms to Pay More Than $81 Million Combined to Settle Charges for Widespread Recordkeeping Failures', available at www.sec.gov/news/press-release/2024-18 (accessed 11th February, 2024); US Securities and Exchange Commission (29th September, 2023) 'SEC Charges 10 Firms with Widespread Recordkeeping Failures', available at www.sec.gov/news/press-release/2023-212 (accessed 11th September, 2024); US Securities and Exchange Commission (8th August, 2023) 'SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures', available at www.sec.gov/news/press-release/2023-149 (accessed 11th September, 2024); US Securities and Exchange Commission (11th May, 2023) 'SEC Charges HSBC and Scotia Capital with Widespread Recordkeeping Failures', available at www.sec.gov/news/press-release/2023-91 (accessed 11th September, 2024); US Securities and Exchange Commission (27th September, 2022) 'SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures', available at www.sec.gov/news/press-release/2022-174 (accessed 11th September, 2024); US Securities and Exchange Commission (17th December, 2021) 'JPMorgan Admits to Widespread Recordkeeping Failures and Agrees to Pay $125 Million Penalty to Resolve SEC Charges', available at www.sec.gov/news/press-release/2021-262 (accessed 11th September, 2024). Over that same time period, the CFTC has charged more than 20 firms — many of which were also charged by the SEC — and collected an additional over US$1.1bn in fines. See Commodity Future Trading Commission (29th September, 2023) 'CFTC Orders Interactive Brokers to Pay $20 Million for Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods', available at www.cftc.gov/PressRoom/PressReleases/8794-23 (accessed 11th September, 2024); Order Instituting Proceedings at 7, *In re U.S. Bank N.A.*, CFTC Docket No. 24-03 (19th March, 2024) (ordering civil monetary penalty of US$6m); Order Instituting Proceedings at 7, *In re Oppenheimer & Co. Inc.*, CFTC Docket No. 24-04 (19th March, 2024) (ordering civil monetary penalty of US$1m).

(3) See, eg Financial Industry Regulatory Authority (5th April, 2024) 'Letter of Acceptance, Waiver, and Consent, Dawson James Securities, Inc., No. 2020065100701', available at https://www.kurtalawfirm.com/wp-content/uploads/2020065100701-Dawson-James-Securities-Inc.-CRD-130645-and-Robert-Dawson-Keyser-Jr.-CRD-1291503-AWC-gg-2024-1715041194841.pdf (accessed 11th September, 2024).

(4) Federal Trade Commission (26th January, 2024) 'FTC and DOJ Update Guidance That Reinforces Parties' Preservation Obligations for Collaboration Tools and Ephemeral Messaging', available at www.ftc.gov/news-events/news/press-releases/2024/01/ftc-doj-

update-guidance-reinforces-parties-preservation-obligations-collaboration-tools-ephemeral (accessed 11th September, 2024). 'Companies and individuals have a legal responsibility to preserve documents when involved in government investigations or litigation in order to promote efficient and effective enforcement that protects the American public. Today's update reinforces that this preservation responsibility applies to new methods of collaboration and information sharing tools, even including tools that allow for messages to disappear via ephemeral messaging capabilities,' said FTC Bureau of Competition Director Henry Liu.'

(5) US Department of Justice (March 2023) 'Evaluation of Corporate Compliance Programs', available at www.justice.gov/criminal-fraud/page/file/937501/download (accessed 11th September, 2024). 'In evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential misconduct and violations of law, prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications.'

(6) *Cf.* Federal Deposit Insurance Corporation (12th December, 2023) 'Formal and Informal Enforcement Actions Manual 3-1 to 3-2', available at www.fdic.gov/regulations/examinations/enforcement-actions/ch-03.pdf (accessed 11th September, 2024). According to this document the 'Failure to keep accurate books and records' is an 'unsafe or unsound practice; Comptroller of the Currency, Administrator of National Banks (21st June, 2024) 'OCC Advisory Letter AL 2004-9 re: Electronic Record Keeping', available at https://www.occ.gov/news-issuances/advisory-letters/2004/advisory-letter-2004-9.pdf (accessed 11th September, 2024). 'The failure of banks to maintain adequate record retention systems can create significant reputation, transaction, credit, and compliance risks'.

(7) A precise definition of what constitutes a business-related communication is beyond the scope of this paper. There have been numerous enforcement actions setting the bounds of what these regulators deem to be business-related communications, but neither the SEC nor CFTC has definitively addressed what types of communications fall within their recordkeeping rules.

(8) See, eg Securities and Exchance Commission (27th September, 2022) 'SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures', available at www.sec.gov/news/press-release/2022-174 (accessed 11th September, 2024). This press release cites orders regarding multiple firms.

(9) See information in ref 2 above.

(10) See information in ref 2 above.

(11) Order Instituting Administrative Cease-And-Desist Proceedings at 2, *In re J.P. Morgan Securities LLC*, Exchange Act Release No. 93807, Admin. Proceeding No. 3-20681 (17th December, 2021).

(12) 17 C.F.R. § 240.17a-4 (Records to be preserved by certain exchange members, brokers and dealers). The Financial Industry Regulatory Authority (FINRA) Rule 4511 (available at https://www.finra.org/rules-guidance/rulebooks/finra-rules/4511 [accessed 11th September, 2024]) similarly requires FINRA members to 'make and preserve books and records as required under the FINRA rules, the Exchange Act and the applicable Exchange Act rules'.

(13) Securities and Exchange Commission (12th February, 1997) 'Reporting Requirements for Brokers or Dealers Under the Securities Exchange Act of 1934', Exchange Act Release No. 38245, 62 Fed. Reg. 6469, 6472. This document recognises that 'the content of the electronic communication is determinative' for the purposes of Rule 17a-4, so that 'broker-dealers must retain only those e-mail and Internet communications (including inter-office communications) which relate to the broker-dealer's "business as such"'. FINRA has likewise explained that '[w]hether a particular communication is related to the business of the firm depends upon the facts and circumstances. This analysis does not depend upon the type of device or technology used to transmit the communication [. . .] rather, the content of the communication is determinative'. FINRA (18th August, 2011) 'Regulatory Notice 11-39: Guidance on Social Networking Websites and Business Communications', available at www.finra.org/rules-guidance/notices/11-39 (accessed 11th September, 2024); see also 'The obligations of a firm to keep records of communications made through social media depend on whether the content of the communication constitutes a business communication. [. . .] The SEC has stated that the content of an electronic communication determines whether it must be preserved.' *Ibid*.

(14) 17 C.F.R. § 275.204-2 (Books and records to be maintained by investment advisers).

(15) 17 C.F.R. § 1.35(a)(1).

(16) Order Instituting Administrative Cease-And-Desist Proceedings at 2, *In re JonesTrading Institutional Services LLC*, Exchange Act Release No. 89975, Admin. Proceeding No. 3-20050 (23rd September, 2020).

(17) See Alpert, B. (17th December, 2021) JPMorgan Is Fined $200M for Doing Business on Personal Phones, Email', Barron's, available at www.barrons.com/articles/sec-fines-j-p-morgan-record-keeping-jpm-51639748714 (accessed 11th September, 2024): 'That's the largest record-keeping fine in SEC history, said agency officials, and far exceeds a $15 million penalty paid by Morgan Stanley (MS) in 2006.' See also Securities and Exchange Commission (10th May, 2006) 'Morgan Stanley Sued for Repeated E-Mail Production Failures', available at www.sec.gov/news/press/2006/2006-69.htm (accessed 11th September, 2024).

(18) See information in ref 2 above.

(19) *Ibid*.

(20) *Ibid*.

(21) Uyeda, M.T. (6th November, 2023) 'Remarks to the 2023 Conference on SEC Regulation Outside the United States: Fifth Annual Scott Friestad Memorial Lecture', available at www.sec.gov/news/speech/uyeda-remarks-sec-reg-outside-us-5th-annual-scott-friestad-memorial-lecture (accessed 11th September, 2024).
(22) *Ibid*.
(23) See Comptroller of the Currency, ref 6 above, at 7: 'As part of its evaluation of an electronic records retention system, bank management should determine which electronic messages and communications to retain. This determination will depend on whether a particular e-mail or electronic message is a 'record' for purposes of the particular record retention requirement or whether the bank may need it later for business or litigation purposes.'
(24) *Ibid*., at 2,. This advisory letter, drafted while electronic communications were much less prevalent than they are today, observed in footnote 11: 'One challenge facing banks is that new forms of electronic communications are developing beyond the established forms such as e-mail. One example is Instant Messages (IMs); however, this advisory letter will not specifically discuss retention of IMs because their legal status as records is uncertain.'
(25) *Cf.* Federal Deposit Insurance Corporation (12th December, 2023) 'Formal and Informal Enforcement Actions Manual', available at www.fdic.gov/regulations/examinations/enforcement-actions/ch-03.pdf (accessed 11th September, 2024), at 3-1 to 3-2 (finding the 'Failure to keep accurate books and records' to be an 'unsafe or unsound practice'); Comptroller of the Currency, ref 6 above, at 2: 'The failure of banks to maintain adequate record retention systems can create significant reputation, transaction, credit, and compliance risks'.
(26) Federal Trade Commission, ref 4 above: '"Companies and individuals have a legal responsibility to preserve documents when involved in government investigations or litigation in order to promote efficient and effective enforcement that protects the American public. Today's update reinforces that this preservation responsibility applies to new methods of collaboration and information sharing tools, even including tools that allow for messages to disappear via ephemeral messaging capabilities," said FTC Bureau of Competition Director Henry Liu.'
(27) US Department of Justice, ref 5 above, at 17: 'In evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential misconduct and violations of law, prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications.'
(28) Uyeda, ref 21 above.
(29) *Ibid*.
(30) Sun, M. (29th December, 2023). 'SEC Top Enforcer Says Tougher Penalties Are Working', *Wall Street Journal*.
(31) References drawn from Sachdev, G., Battacharyya, A. and Brabant, P. (2023) 'Financial Services and Global Regulatory Requirements: Balancing the Ease of Electronic-communications Usage with Regulatory Expectations, *International In-House Counsel Journal*, Vol. 16, No. 63.