



Risky business: Financial compliance and covid-19

Contents

-
- 2 About this report

 - 3 Key findings

 - 4 Financial compliance in a pandemic: A risk-on environment

 - 5 A need for more extensive communications oversight

 - 7 Balancing priorities: Privacy, productivity and increasing regulation

 - 8 Conclusions and key takeaways
-

About this report

The covid-19 pandemic has kept workers confined to their homes for months on end, significantly increasing the role of digital tools in keeping a firm connected. In heavily regulated sectors like finance, the sheer volume of communications that is now generated over digital channels is raising crucial questions about whether, how and to what extent organisations should exercise oversight of employee communications.

This report explores shifting attitudes towards internal communication oversight in remote working environments, based on findings from a survey of 503 executives in the financial services industry in North America, Europe and Asia. The survey was conducted by The Economist Intelligence Unit and supported by Behavox.

This report was written by Adam Green and edited by Monica Ballesteros.

Key findings

- **Nearly two-thirds of finance executives believe that remote employees are only moderately following company guidelines regarding the security of confidential information**, and just one in five believe that staff are following these guidelines completely. This is particularly troubling given that more than two-thirds of respondents believe that non-compliant behaviour has increased in remote working environments, while 19% believe it has increased significantly.
- **Six out of ten respondents believe that extensive communications oversight has become more important since the covid-19 pandemic began**, as conventional methods for ensuring compliance—such as identifying trades at irregular times, recording telephone calls and restricting the use of private devices—are compromised or made impossible. The increased use of home networks and devices, along with employee-purchased tools, requires new and more extensive approaches to communications oversight.
- **One-third of respondents see advantages in stronger oversight that extend beyond compliance**, especially in terms of increasing employee productivity. This suggests that compliance investments could deliver positive associated benefits. While there are challenges to increasing oversight, such as growing distrust of compliance teams and perceived privacy infringements, the majority of respondents (87%) believe that government regulations around internal communications in the financial services industry will become more stringent in the future.

Financial compliance in a pandemic: A risk-on environment

The financial services industry transitioned rapidly to remote work in early 2020 as a result of the covid-19 pandemic and subsequent stay-at-home directives issued by governments and companies. This shift has brought particular risks to the industry because of the sensitive nature of financial information and the need for compliance monitoring of staff communications to identify suspicious activity or breaches of financial crime rules. Further challenges arise from an abundance of new non-public information on which illegal trading activity could be based, from procurement agreement details related to pandemic logistics, to bankruptcy or supply-chain disruptions, to market-moving data releases from biotechnology companies.

Against this backdrop, our survey reveals two worrying findings. First, nearly two-thirds of executives believe that remote employees are only moderately following company guidelines regarding the security of confidential information, and just one in five believe that staff are following those guidelines completely. Second, more than two-thirds of respondents believe that non-compliant behaviour has increased in remote working environments, and 19% believe it has increased significantly.

The survey also revealed that less than half of the executives (43%) believe that their company has been very successful in shifting to remote work since the start of the pandemic, with 54% reporting that their company has only been “somewhat successful”. European and Japanese respondents were more likely than other respondents to report that the transition had only been partially successful. This finding is noteworthy as the vast majority of respondents (78%) report that half or more of their trade-facing employees are currently working remotely, and nearly half (48%) believe that it will be six months or longer before their workforce can return to working primarily in an office location.

The clear majority of respondents expect an eventual return to normal, in-person work, with only 2% reporting that they do not expect to return to the office environment. This suggests that there is an expectation within financial services that the industry will not shift to a permanent remote working arrangement, unlike some professional services industries. However, it is impossible to predict how long it will take to transition back to office work as vaccine rollouts proceed unevenly and variants of the virus risk undermining vaccine efficacy.

Two-thirds of respondents believe that non-compliant behaviour has increased in remote working environments, and 19% believe it has increased significantly.

A need for more extensive communications oversight

More than seven in ten executives (72%) report that having oversight of their organisation’s internal communications is very important for business success, including for identifying insider threats of leaking or stealing data (29%). Despite this, companies and regulators are struggling to gain full visibility across communications in a remote work setting.

Conventional methods for monitoring communications in on-premise financial trading environments—such as recording telephone calls and restricting access to personal devices—have been critical in the past for proceeding with criminal prosecution for insider trading and market manipulation.¹ However, these methods are not easily implemented in remote work environments. Other methods for spotting suspicious activity, such as identifying trades at irregular times, may also be compromised by atypical work schedules during the pandemic.² In addition, compliance teams

need to attend to risks related to individuals sharing information with family members or cohabitants, or inadvertently providing access to that information. Survey respondents identified this inability to ensure confidentiality in remote work settings as the top challenge (tied with lack of interaction between compliance officers and employees) in conducting communications oversight while employees work remotely.

Employees are also more likely to use personal devices and networks in a remote setting. For instance, finance professionals are reportedly using their mobile devices more frequently, with Refinitiv (a financial data company) reporting a 50% increase in mobile usage of its financial data during the spring 2020 lockdown.³ Personal mobile devices could be used to facilitate unlawful or inappropriate conduct, such as giving insider tips, rigging rates or spoiling evidence. The use of personal devices presents less of a challenge in the office environment,

Refinitiv (a financial company) reported a 50% increase in mobile usage of its financial data during the spring 2020 lockdown.

Figure 1

Challenges faced by organisation in conducting internal communications oversight in remote environments

What are the greatest challenges your organization has faced in conducting internal communications oversight while employees work remotely? (%)



Source: The Economist Intelligence Unit.

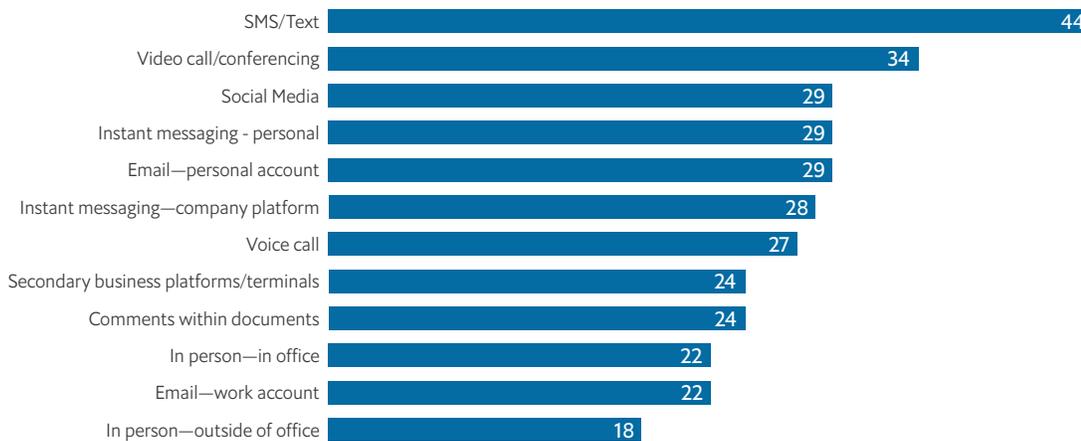
1 *United States v. Afriyie*, No. 16-CR-377 (S.D.N.Y.); *United States v. Siva, et al.*, 17-CR-503 (S.D.N.Y.); *United States v. Smith, et al.*, No. 19-CR-669 (N.D. Ill.).

2 KPMG. 2020. "Key cyber risks for banks during COVID-19." [https://home.kpmg/xx/en/home/insights/2020/05/key-cyber-risks-for-banks-during-covid-19.html]

3 Bunyan, Stuart. 2020. "How is COVID-19 changing operational resilience in trading?" Refinitiv. [https://www.refinitiv.com/perspectives/future-of-investing-trading/how-is-covid-19-changing-operational-resilience-in-trading/]

Figure 2
Channels of communication most likely to be used for non-compliant behaviour

Which communications channels do you think are most utilized for non-compliant behaviour? (%)



Source: The Economist Intelligence Unit.

where they tend to be stored safely during working hours and are less likely to be used in open-plan workspaces.⁴

Greater use of personal devices similarly increases the likelihood and ease of using unsanctioned apps and communications platforms. More than six in ten executives (61%) strongly agree that remote working environments have increased the importance of extensive communications oversight, as the shift to off-premise work encourages greater use of communications channels that are not sanctioned by the company, such as chat apps. Executives believe that the top three channels most used for non-compliant behaviour are SMS/text (44%), video calls/conferencing (34%) and social media (e.g. Facebook, LinkedIn; 29%). Companies regularly monitor some communications channels for non-compliant activities, including email (work accounts;

96%) and company-owned instant messaging platforms (e.g. Slack; 65%). However, only 65% of companies regularly monitor personal instant messaging platforms, which are the most likely channel for non-compliant behaviour; and only 52.5% monitor social media.

The risk of unintentional compliance failures cannot be discounted either. Home internet networks are less cyber-secure than corporate networks, meaning that outside actors are better able to hack into sensitive information. There has already been a significant rise in fraudulent emails during the covid-19 pandemic, when phishing scams may prove more effective due to staff's increased vulnerability or distractedness (as a result of stress or the burden of increased communications). Fraudsters are also taking advantage of issues like staff absences or communications from new names related to covid-19 procedures.⁵

More than six in ten executives (61%) strongly agree that remote working environments have increased the importance of extensive communications oversight

4 K&L Gates LLP. 2020. "COVID-19: Mitigating remote working risks – messaging and chat apps." ICLG. [<https://iclg.com/briefing/13369-covid-19-mitigating-remote-working-risks-messaging-and-chat-apps>]

5 BDO United Kingdom. "Fraud prevention: Maintaining a controlled environment." [<https://www.bdo.co.uk/en-gb/sport-covid-19/fraud>]

Balancing priorities: Privacy, productivity and increasing regulation

Respondents are concerned that increased oversight of communications in remote working environments could be seen as infringing on employees' private lives and may negatively affect corporate culture. Nearly half of respondents are concerned that strong oversight could increase distrust of compliance teams, and 35% worry that it infringes on privacy. However, a third of respondents also see advantages in stronger oversight that extend beyond compliance, including increasing employee productivity.

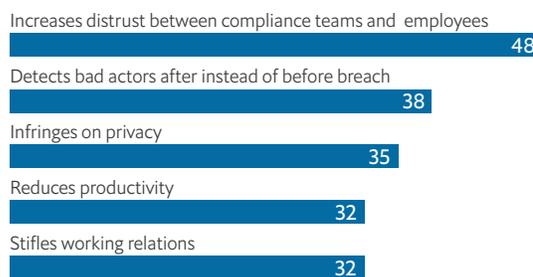
A strong majority of respondents (87%) believe that government regulations around internal communications will become more stringent in the financial services industry, and a quarter believe that they will become much more stringent. Concerns about infringing on privacy need to be balanced against the expectation of tightening regulations and the fact that the right to privacy does not confer freedom to commit illegal acts. (Privacy is overturned via warrants when legal thresholds are met.)

Prior to the covid-19 pandemic, regulators were already increasing their monitoring of emerging communications platforms and tools, including encrypted and private chat apps such as Snapchat, WhatsApp, Telegram and Signal, as well as video-conferencing platforms like Wickr.⁶ The US Securities and Exchange Commission (SEC) requires companies to monitor chat apps and has been requesting access to chats, images and WhatsApp conversations. Recognising

Figure 3

Disadvantages of strong internal communications oversight

What are the main disadvantages to your organisation from strong internal communications oversight? (%)



Source: The Economist Intelligence Unit.

the risks of ephemeral messaging apps, the SEC has also encouraged companies to put in place effective provisions for retaining business communications.^{7,8} The UK Financial Conduct Authority has warned finance players about the risks of WhatsApp and social media during the pandemic,⁹ and in 2019 it brought a prosecution for insider dealing based on the deletion of WhatsApp messages.¹⁰ Texting and chat functions can also increase the risk of litigation due to the use of less careful wording.¹¹

A strong majority of respondents (87%) believe that government regulations around internal communications will become more stringent in the financial services industry

6 Ingoglia, Eugene. 2019. "Instant messaging apps and corporate record retention policies: Revised DOJ guidance for companies." Allen & Overy Investigations Insight. [https://www.aoinvestigationsinsight.com/instant-messaging-apps-and-corporate-record-retention-policies-revised-doj-guidance-for-companies/]

7 Office of Compliance Inspections and Examinations. "Observations from investment advisor examinations relating to electronic messaging." [https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf]

8 Ingoglia, Eugene. 2019. "Instant messaging apps and corporate record retention policies: Revised DOJ guidance for companies." Allen & Overy Investigations Insight. [https://www.aoinvestigationsinsight.com/instant-messaging-apps-and-corporate-record-retention-policies-revised-doj-guidance-for-companies/]

9 Mortimer, Rachel. 2021. "FCA warns advisers on using WhatsApp and social media." [https://www.ftadviser.com/regulation/2021/01/11/fca-warns-advisers-on-using-whatsapp-and-social-media/]

10 FCA. 2019. "Konstantin Vishnyak appears at court for destruction of documents offence." [https://www.fca.org.uk/news/press-releases/konstantin-vishnyak-appears-court-destruction-documents-offence]

11 Cashman, Amanda R., Jacquelyn S. Celender, Katherine M. Gafner and Travis L. Brannon. 2020. "COVID-19: There's no place like home: What GCS need you to remember while working remotely." K&L Gates. [https://www.klgates.com/covid-19-theres-no-place-like-home-best-practices-while-working-remotely-03-23-2020/]

Conclusions and key takeaways

- **Finance executives are dissatisfied with their transition to remote work and believe that non-compliance risks are increasing.** The key risk factors for non-compliance are the increased use of personal devices and insecure networks, and the increased temptation to use communications channels outside of corporate technology infrastructure. The incentives to engage in illegal acts are also stronger in a volatile market environment. Well over half of respondents believe that remote employees are only moderately following guidelines regarding the security of confidential information, and that non-compliant behaviour has increased.
 - **With remote work likely to persist for at least six months, firms must develop more effective communications oversight, covering both technological and behavioural or cultural factors.** Unlike some professional service sectors, which have embraced remote working, survey respondents do not generally expect the finance industry to be permanently transformed. Just 2% of respondents do not expect to return to office work. However, the duration of lockdowns and social-distancing restrictions remains unknown, and nearly half of respondents (48%) believe that the majority of their workforce will not be returning to their office locations in less than six months.
 - **Companies need to augment their communications approaches to handle the risk environment.** Finance companies have technological augmentations at their disposal to adapt their communications oversight, including more effective systems for recording communications and retaining data, along with stronger cyber-secure devices and networks. They should also manage non-technological risks, such as family members or cohabitees having access to sensitive information or sharing non-public information with staff. Companies may look to more elaborate oversight, such as monitoring the presence of other people in a trader's work area at home, although this must be balanced against privacy considerations and must recognise the complications of home parenting. North American and European respondents were much more likely than other respondents to cite distrust of compliance teams as one disadvantage of stronger internal communications oversight.
- The covid-19 crisis may now be at a turning point, as vaccine availability and public health measures transform the pandemic into a controllable endemic and spark hopes of a return to normal life. However, timelines remain subject to considerable uncertainty and variation across markets, and remote work is likely to remain a reality in the near future. Finance executives need to ensure that their communications platforms are adequately recalibrated to identify threats in a high-risk market environment, some of which may be occurring undetected.

While every effort has been taken to verify the accuracy of this information, The Economist Intelligence Unit Ltd. cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report. The findings and views expressed in the report do not necessarily reflect the views of the sponsor.

LONDON

20 Cabot Square
London, E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
Email: london@eiu.com

NEW YORK

750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@eiu.com

HONG KONG

1301 Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@eiu.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@eiu.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@eiu.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@eiu.com