WhatsApp: what's the problem?

A look at the potential issues involved with communicating via WhatsApp and the changes banks are making to avoid additional fines

Risk Universe by RiskBusiness

Some of the world's largest banks are facing a combined US$1bn in fines for allowing employees to converse with other employees and clients using WhatsApp and similar unauthorised messaging apps.

Morgan Stanley, JPMorgan Chase, Citigroup, Goldman Sachs and Bank of America have all either paid, or are preparing to pay, fines of US$200m each to US financial regulators. Barclays has also set aside US$200m in its latest financial report to cover potential fines, and Credit Suisse, Deutsche Bank and UBS face similar charges.

COMPLIANCE HAS LEFT THE CHAT

WhatsApp has two billion global users and handles over 100 billion messages every day. It is a free messaging app which allows users to make voice calls and send messages, with end-to-end encryption. This means the messages cannot be accessed by other parties and can be permanently and irretrievably deleted. It's mostly used for personal correspondence, but many businesses also use WhatsApp to send messages, often informally – despite being in breach of WhatsApp's service agreement.

The problem with bank employees using WhatsApp to discuss work matters is that banks are required to follow rigorous record-keeping regulations in relation to written communication, such as email and other types of messaging. But, when the global Covid-19 pandemic forced millions of people to work from home, it blurred the lines between personal and professional use of mobile devices, and now everyone is trying frantically to get things back in order. "Having an entire workforce switch to remote access at such short notice meant many people were using their own phones and laptops to contact other employees and clients," says Mike Finlay, CEO of RiskBusiness "This wreaked havoc with banks' ability to monitor conversations and, as predicted, we are starting to see the repercussions of that now. The full extent of the problem is just emerging and has already exceeded the US$1bn mark – and that's with just a couple of regulators looking into it."

MAINTAINING AND PRESERVING WRITTEN COMMUNICATIONS

Banks are required to keep a record of any business-related communications including phone calls, emails and messages, to help prevent insider trading, fraud and other forms of misconduct. Despite this, it appears there has been a pretty relaxed attitude towards the use of unmonitored communication methods, such as WhatsApp since the pandemic (and before), even from senior members of staff.

JPMorgan was the first bank to be hit with a US$200m fine for WhatsApp usage by the US Securities and Exchange Commission (SEC) last year. The bank admitted that from at least January 2018 through November 2020, its employees often communicated about securities business matters on their personal devices, using text messages, WhatsApp, and personal email accounts. None of these records were preserved by the firm, as required by federal securities laws.

JPMorgan also admitted that WhatsApp and similar apps were openly used and the practice was not hidden inside of the firm. Even senior members of staff, such as managing directors and supervisors, used personal devices to communicate about the firm's securities business.

JPMorgan was fined in December 2021, but research would suggest banks have been slow to take action since. According to a recent poll reported in *City Am*, only 14% of firms operating in the City of London currently monitor their employees' use of WhatsApp.

JPMorgan admitted that WhatsApp and similar apps were openly used

TOO LITTLE, TOO LATE?

The JPMorgan case, which was the catalyst for the industry-wide probe by US regulators, involved a frantic scramble to try and fill the gaping holes in the bank's communication record keeping. Staff reportedly received a memo instructing them to spend some time going through their messages from the past three years and to save anything that was "related to work." Reports suggest that the memo applied to both personal and professional devices.

In its press release about the JPMorgan charges, the SEC highlighted the lengths the bank had to go to in order to try and make up for this lapse in record keeping: "We encourage registrants to not only scrutinise their document preservation processes and self-report failures such as those outlined in today's action before we identify them," said Gurbir S. Grewal, Director of the SEC's Division of Enforcement, "but to also consider the types of policies and procedures JPMorgan implemented to redress its failures in this case."

"JPMorgan's failures hindered several Commission investigations and required the staff to take additional steps that should not have been necessary," added Sanjay Wadhwa, Deputy Director of Enforcement.

ACCESSING WHATSAPP MESSAGES: WHAT DOES THE LAW SAY?

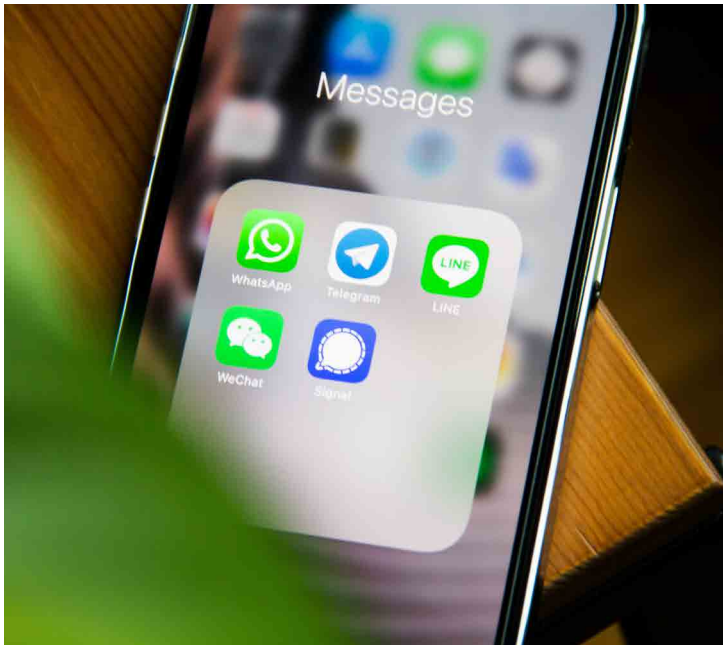
Banks now need to ensure they are adhering to record keeping regulations, but also not falling foul of data privacy laws. The law around accessing WhatsApp messages varies depending on jurisdiction, but firms should make sure this area is at least covered in both employment contracts and IT terms-of-use documents.

Accessing messages on a company-owned device is a much more straightforward process

Accessing messages on a company-owned device is a much more straightforward process than accessing messages held within a personal device, and contracts need to be explicit about this in order to mitigate the regulatory risks in future.

However, telling your employees that they shouldn't use non-authorised communication methods to discuss work isn't always enough to avoid regulatory action. In September 2020, the SEC fined a brokerage firm in the US US$100,000 for failing to provide copies of business-related messages sent via personal mobile devices. The firm in question had specifically prohibited the use of unapproved apps such as WhatsApp in its employee contracts, but was still fined despite this.

In a recent webinar on the topic, law firm Norton Rose Fulbright highlighted the complexities presented by investigations involving access to personal data. "This is the fastest changing area in the world of investigations and white collar," says Christopher Pelham, a partner at the firm's Los Angeles office. "Data privacy laws are becoming more stringent in many jurisdictions and are actually starting to conflict in many cases between those jurisdictions. Individuals are increasingly aware of and asserting their rights with respect to their own data. On top of that, data sources are becoming more varied and complex and authorities' expectations with respect to data preservation, data provision and data review are increasing and changing."



In the UK, the FCA Handbook says firms "must take all reasonable steps to prevent an employee or contractor from making, sending, or receiving relevant telephone conversations and electronic communications on privately-owned equipment which the firm is unable to record or copy." What is meant by "reasonable steps" is likely to become increasingly difficult to determine as the working environment continues to evolve. Andrew Rose, partner at Norton Rose Fulbright's London office, says the issue is only going to get worse as more companies embrace long-term hybrid working models. "The reason there is an issue here is that, mobile phone data in particular, while it's often crucial in an investigation, can be really difficult to collect," he says. "Unless WhatsApp is installed via specialist software by the company, it is unlikely to be able to retrieve that [data] remotely, so you are going to need some degree of custodian cooperation. There's an added complexity

with data privacy as well…You would need to consider what rights you have as a company to review the WhatsApp data, what the data privacy risks are and how they can be best managed…Are the relevant phones company phones, [or] are they personal phones? Does the company have a bring-your-own-device policy, what have the employees been told about how their data will be reviewed? It's very important that you get specialist data-privacy advice on this."

In September 2020, a banker who was charged with destroying evidence for deleting WhatsApp messages from his phone that were linked to an investigation, was found not guilty. Konstantin Vishnyak, who worked at VTB Capital, deleted the messaging app from his phone after it became apparent the data from it would be required for an investigation by the FCA into insider trading. Neil Swift, a partner at law firm Peters & Peters told *Financial News*: "It is for the prosecution [the FCA] to prove their case. They have to have evidence that the defendant knew or suspected that the messages he deleted would be relevant to an investigation into insider dealing. That goes beyond simply proving deletion."

Many banks are now looking into software which can be installed onto employee devices to monitor and preserve messages sent via WhatsApp going forward. The *Financial Times* reported in June that Deutsche Bank would be installing the Movius app on some employees' phones for this purpose. The bank also reportedly sent a memo to employees warning them not to delete any work-related WhatsApp messages as this could potentially be in breach of US laws in relation to the current investigation into WhatsApp usage and recordkeeping.

Software can now be installed onto employee devices to monitor and preserve messages sent via WhatsApp

ACTION AGAINST INDIVIDUALS

It's important to note that it isn't only the banks themselves being hit with fines; individuals are also paying the price for not following policies and procedures around the use of messaging apps. In 2017, Christopher Niehaus, a former investment banker at Jefferies International in the UK, was fined £37,198 for sharing client confidential information over WhatsApp. And this was five years before the latest widespread investigation into the issue, which is likely to unearth other individual cases of misconduct.

Anthony Kontoleon, who had worked at Credit Suisse for 28 years, quit in April 2022 amid reports he was using unapproved messaging applications with clients. In this case, there has been no suggestion that he was sharing inappropriate information, but the simple fact he was using the app to contact clients was enough to lead to his resignation from the bank.

In another, similar case, an FX trader at HSBC was reportedly fired in connection with WhatsApp messages exchanged with a client who is understood to have purchased sporting event tickets for the trader.

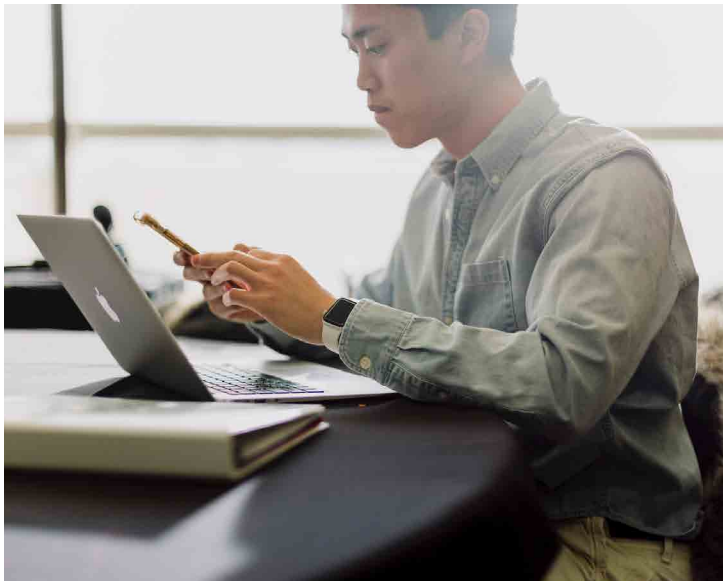
THE TIP OF THE ICEBERG?

The fallout from huge misconduct cases such as the manipulation of LIBOR rates a decade ago, means we will continue to see scrutiny of communication methods and banks' recordkeeping capabilities. While it is the SEC and CFTC in the US who are

> **"It is important for firms to proactively review their recording policies and procedures"**

currently leading the way in these investigations, other regulators around the world have signalled they are likely to follow suit.

The UK's FCA has said the use of messaging apps remains an "area of focus" for the regulator, and in its January newsletter, highlighted firms' obligation to monitor communications: "It is important for firms to proactively review their recording policies and procedures every time the context and environment they operate in changes," it said. "We expect firms to have a rigorous monitoring regime, commensurate to the increased risks, where in-scope activities may be conducted outside the controlled office environment." German financial regulator BaFIN has also asked Deutsche Bank to clarify how its staff uses WhatsApp to communicate for business purposes and will likely be looking into other firms.



Annie Searle, principal of the ASA Institute for Risk and Innovation and a senior lecturer at the University of Washington's School of Information, agrees that the investigation will likely be extensive and far-reaching. "The handwriting is on the wall," she says. "Examiners are going to be sampling both approved and outlier communications platforms, especially those that may have grown up during remote work. The fines look both significant and determined to teach a lesson."

AVOIDING FUTURE FINES

The investigation currently underway is complex because it will require the retrieval of data that may be permanently lost. To prevent these issues from recurring, firms need to regularly review policies in relation to all types of communication – not just specifically WhatsApp, but any form of communication which could fall under regulators' purview. Regular training is also essential to curbing bad habits and senior members of staff should be expected to set an example for others. "It is an issue which will continue to evolve because of the nature of technology," says RiskBusiness' Mike Finlay. "It's not just about getting the policies right though. As is the case whenever we are talking about any type of potential misconduct, it is a culture issue. If we don't create a working environment where there are clear lines between the professional and the personal, we can expect more of this type of thing in the future."

Risk Universe
by RiskBusiness

REFERENCES AND FURTHER READING

Bankers made to install app that tracks messages

Barclays latest global bank ensnared in US 'Whatsapp' probes

Beware the use of WhatsApp at work

Big bank messaging app crackdown exposes policy holes, monitoring struggles

Data issues in an investigation: Navigating a minefield (webinar)

Despite record fine of £160m for JPMorgan, City managers still have WhatsApp 'blind spot'

FCA fines former investment banker for sharing confidential information over WhatsApp

Financial institutions and the hybrid working environment

JPMorgan admits to widespread recordkeeping failures and agrees to pay US$125m penalty to resolve SEC charges

JPMorgan's intrusive WhatsApp message request

About Risk Universe

Risk Universe by RiskBusiness provides in-depth analysis, reviews and research on areas of interest within the broader governance, risk, audit and compliance landscape, designed to provide proactive, 360° intelligence for informed decision making across the enterprise.

About RiskBusiness

RiskBusiness is an international governance, risk, audit and compliance (GRAC) solution provider, delivering risk content, risk intelligence, risk tools and risk advisory services to its clients. It is an association of like-minded industry professionals, who have the aim of furthering the risk management discipline to enable better risk-reward decision making.

Risk management is an evolving discipline, which has developed in close partnership with the industry. RiskBusiness has, both as individuals and collectively, a depth of established relationships with leading players and regulators in the operational risk field. We are also active participants in industry working groups and contribute thought leadership through publications and education.

RiskBusiness was founded in 2003 and today has principal locations in Birmingham, London, Buenos Aries, Amsterdam, Hong Kong, New York, Singapore, Toronto, and Zurich. To learn more, visit **www.riskbusiness.com**

Contacts

Carrie Cook, Editor:
carrie.cook@riskbusiness.com

General enquiries:
info@riskbusiness.com

Risk Universe
by RiskBusiness

www.riskbusiness.com