

INDUSTRY BRIEF

# Why Banks Must Embrace WhatsApp for the Future of Work

SHAUN HURST

 smarsh®



If you had told me a couple years ago that the world's major financial services companies would all be operating almost entirely with a remote workforce, I would have broken out in a cold sweat.

Straight away my mind would have jumped to the severity of the compliance issues that such a move would involve. Then I'd worry about the magnitude of the investment that banks would need to make in innovative collaboration tools — a move they had put off for so long. For nights on end, I would have tossed and turned thinking about the creaking legacy archives so many banks still held onto, already struggling to keep pace with the exponential rise in data flowing in and out of modern businesses every nano-second.

### **What a difference a short time can make.**

Banks are now lightyears ahead of where they were at the turn of the decade. The vast majority have implemented the technology they need to enable their workforce to compliantly use collaboration tools. Most have either moved their archives to the public cloud or have seriously sped up their plans to do so. And “hybrid work” is no longer a buzz phrase. It is now a reality. We will never go back to a situation where employees are only able to work in a physical office.

But there is work still to be done. There is a valuable lesson that banks need to learn from the past two years: embrace technology, do not fear it. Fear of compliance issues was one of the main reasons that so many had put off fully adopting the collaboration tools that are now the lifeblood of their businesses. What they need to do now is expand their newfound wisdom and embrace all communications platforms that enable employees to stay connected and work effectively, wherever they are.

## **WhatsApp and financial services regulations**

This is most evident with WhatsApp. Many people working in the financial services industry already know that the end-to-end encryption messaging tool is ubiquitous and widely used to keep in touch with colleagues, clients, and contacts.

But while company policies largely prohibit the use of WhatsApp, financial regulators have stayed away from an outright ban. Instead, they have issued guidance requiring companies to ensure that the instant messaging tools used by their employees are monitored and in compliance with already existing recordkeeping rules such as MiFID II.

Ensuring that these guidelines are adhered to has been complicated by the fact that many companies have brought in outright or partial bans on unmonitored instant messaging tools, while also adopting bring-your-own-device (BYOD) policies.

Largely implemented to cut costs, these BYOD policies mean businesses are now less able to police which communications apps and platforms their employees are using. This means that they have now lost the oversight they need to ensure that employees are adhering to the bans.

Despite a mountain of anecdotal and judicial evidence that employees in the financial services industry have turned to WhatsApp even more since the outbreak of the pandemic, banks are still failing to adopt the compliance tools they need to ensure their employees are acting legally.

## Importance of capturing WhatsApp

There have been noteworthy legal and disciplinary cases that centred upon the misuse of WhatsApp within banks.

In one case, it was reported that a dozen traders at one investment bank were [punished for using WhatsApp at work](#) – one was fired and the others had their bonuses cut. Later that year, two senior executives working in the commodity sector quit after accusations that they had broken their company's rules on instant messaging platforms.



**While one banker was acquitted over a legal case with the FCA in which he was accused of purposefully obstructing an investigation by deleting WhatsApp messages, the UK regulator stated it would ‘take action whenever evidence we need is tampered with or destroyed.’**

In another case, a bank executive was [charged for insider training](#) with a friend. The executive encouraged his friend to communicate via WhatsApp because messages were encrypted. In one WhatsApp exchange, the executive urged his friend to buy stock, noting that an upcoming tender offer announcement would be released soon. Responding by WhatsApp, the friend agreed to share the profits of his planned trades.

These disciplinary actions are a clear message to banks that they will be expected to provide accurate accounts of any messages sent by their employees over WhatsApp.

# The solution: capturing and supervising WhatsApp communications

The compliance challenges of the increased use of WhatsApp have been widely played out in the financial media in recent years, with multiple firms being handed significant fines due to their communications-monitoring oversights. This doesn't have to be the case.

As I said before: We will never go back to a situation where employees are only able to work in a physical office. Companies working in regulated industries, and especially financial services companies, must embrace the tools that they know are in wide use by their employees.

Very few banks have introduced the monitoring solutions they would need to adequately manage the use of WhatsApp or other encrypted messaging tools by its employees. But encrypted messaging tools like WhatsApp and WeChat can be captured, monitored, and supervised. Firms simply need to invest in the technology in order to do so.

Find out if you can manage your risk profile with the [Hybrid Workforce Risk Assessment Scorecard](#).

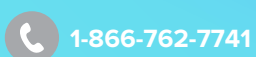


Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals in more than 100 digital communications channels. Regulated organisations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit [www.smarsh.com](http://www.smarsh.com).

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.

Brief - EMEA - 06/22



© 2022 Smarsh, Inc. All rights reserved