January 2021

The need for tighter control on employees' use of chat applications when conducting or discussing company business.

What we learned from the FCA's 2020 Vishnyak prosecution and the FCA's reminder about the need to record telephone calls and electronic communications.

John W Gibson; Tim Harris; Pere Puig Folch

Introduction

- The FCA's failed prosecution of an investment banker for destroying WhatsApp messages taken together with the FCA's 'Market Watch 66' publication highlighting the need to control electronic communications[1] is a reminder to firms to address staff use of personal chat applications to conduct business.

- With the shift to remote working and the convenience of chat applications for conducting business, it is critical for firms to understand that information relevant to their business may be created on personal devices and applications. All commercial entities, but particularly those in the regulated financial sector, need fully to understand where all of their data is held, how to preserve and access it and the consequent risks created by the use of personal chat applications such as WhatsApp.

Vishnyak Case Summary

- On 28 September 2020, the FCA announced that it had lost its first prosecution relating to the destruction of documents. Konstantin Vishnyak was charged with destroying WhatsApp messages which he knew or suspected were relevant to the FCA's investigation of insider dealing (for which Vishnyak was ultimately not charged) contrary to section 177(3)(a) of the Financial Services and Markets Act 2000.

[1] Market Watch 66: Recording telephone conversations and electronic communications published on 11 January 2021. The Market Watch reminded firms, amongst other things: a) of the risks of using unmonitored and/or encrypted communication applications such as WhatsApp for sharing and discussing confidential business matters; and b) that they must ensure that if they allow chat applications to conduct in-scope business activities, the messages must be recorded and auditable (SYSC 10A applies).

- In his defence, Vishnyak claimed that he deleted the application in a panic to hide his chats with prominent Russian politicians and businesspeople (and which included chats with a Russian politician suspected of killing dissident Alexander Litvinenko) from the UK authorities. Consequently, he claimed that he did not delete the application for the purpose of destroying evidence relevant to the FCA's investigation.

- Although Vishnyak was found not guilty by the jury after only 3 hours of deliberation, he may still face regulatory sanction. The case highlights the evidential importance that the FCA attaches to information contained on WhatsApp and other instant messaging applications ("chat applications"). The FCA expects these applications to be preserved and in the words of the FCA's Director of Enforcement, Mark Steward: "[it] will take action whenever evidence we need is tampered with or destroyed." The FCA's Market Watch publication this week is a reassertion of the importance of Mr. Steward's message.

What are the risks presented by communicating via personal chat applications?

- Inherently chat applications encourage users to communicate in a more informal, casual and unguarded manner. Individuals and firms are often required to produce these messages to third parties (as part of an investigation conducted by enforcement authorities or in litigation) in the same way as they can be required to produce emails and hard copy documents. As was apparent from the Bloomberg chat messages identified in the FCA's Libor and Forex investigations, badly chosen words in personal chat messages create significant litigation and reputational risk for firms and individuals. As the famous WWII poster reminds us "loose lips sink ships!"

- We expect that in 2021, investigations into suspicions of regulatory or criminal corporate conduct will put chat applications at the heart of the data strategy. The absence of recorded communications on a deal or transaction may create enhanced suspicion. An inability to recover chat application communication will also count against the corporate suspect, irrespective of the autonomy of the chat application user. In the worst case, the use of chat applications combined with an absence of enhanced restrictions and monitoring of their use in company procedures or training may prevent a corporate suspect from establishing that it put in place the necessary measures to prevent criminal conduct carried out on the company's behalf (further to, for instance, s.7 of the Bribery Act 2010).

- Employees should be prevented from sharing any confidential information over non-work systems. In 2017, the FCA fined an individual, for sharing confidential information, obtained during the course of his employment, with a friend (who was also a client of the firm), in breach of Principle 2 of the FCA's Principles for Businesses. The confidential information related to the identity of clients, details of client mandates and fees payable to the firm, intended acquisitions and views on profit warnings. The information could have provided an undue advantage to the friend.

- Increasingly, the FCA has a focus on non-financial misconduct, for instance, viewing "*sexual harassment as misconduct which falls within the scope of our regulatory framework*"[2]. Individuals risk sanction for misconduct even if the conduct occurs outside the workplace and has no direct relation to their work. Chat applications are more likely to be used to send inappropriate messages than email. In the event that allegations of misconduct arise, these messages may become pertinent to the firm or the FCA's investigation.

- The use of uncontrolled chat applications presents a technical and regulatory challenge to firms and individuals given their regulatory obligations. By design, chat applications such as WhatsApp use on-device encrypted storage for their messages. This means that once a message is delivered to its recipient, it no longer resides in any third party server. The copy of the message is held only on the sender and recipient devices. Therefore, firms have no control on the retention of any information delivered through these platforms.

Does firm policy prohibit employees from using chat applications on non-work devices for business purposes?

- If it does, a firm should clearly communicate the requirements to individuals to ensure they are not using chat applications on non-work devices to conduct business or discuss business matters. Firms should consider methods to enforce this policy, by for instance, requiring staff to certify that they do not use their device to discuss business (and amplify that message through training).

- If the firm has a flexible approach to using personal devices for business purposes (such as a "bring your own device" policy), as part of its approach to mitigate the risks explained above, firms will be unable technically to monitor private communications, which would in any event give rise to data privacy issues. Consideration should be given as to how the firm can record, monitor, and access chat applications on devices which are being used for both business and private purposes (and in line with relevant SYSC obligations). For example, in the event of a regulatory enquiry or investigation is the employee under an obligation to provide the firm with access to a personal device?

- In either case, given the utility of chat applications (and the risk, particularly with home working, that these applications will be used notwithstanding the firm's policy), consideration should be given to allowing employees to download a chat application suitable for and controlled by the firm and by clearly stating what platforms can and cannot be used for business activity by employees. Recognizing this reality, it was reported in November 2020 that Credit Suisse had launched its own collaborative WhatsApp-style chat system for employees. Notwithstanding firm-wide proprietary systems, employees may still want to use chat applications to speak to contacts at other institutions or clients. This has led the largest global banks to partner with platforms, such as Symphony, to enable WhatsApp and WeChat through the firms' own systems.

- If the firm's policy and employment contracts are unclear on: a) allowing employees to use personal devices and non-work chat applications to conduct business; and/or b) the firm's right to record, monitor or obtain any work-related messages on personal devices or non-firm systems,

[2] Megan Butler, Executive Director of Supervision (Investment and Wholesale) wrote a letter to then Chair of the House of Commons Women and Equalities Committee in September 2018 outlining that the FCA views sexual harassment as misconduct which can drive poor culture.

these documents should be updated. Policies should be reappraised in light of current home working arrangements and the FCA's reminder.

Employee communications and training

- The policy requirements and expectations of the content of business communications should be set out clearly in regular firm-wide communications. As with the implementation of all firm processes, the tone is set from the top and senior executives should set the example as to what is and is not acceptable in work communications. Failure to enforce the firm's stated policy on the use of chat applications (or otherwise act without due skill, care and diligence) exposes the firm and individual to the risk of breaching FCA obligations as well as wider issues concerning the provision of material required by law enforcement.

- It is important that employees are adequately trained on the firm's processes and reminded how:

    - Chat messages can create risk for the firm and/or individual.

    - To identify and handle confidential information.

- Individuals should also be reminded about their duty to report breaches of policy to the firm. Once investigated, it may also be necessary to report breaches to the FCA. In the event that enforcement action is taken, cooperation can result in a significant reduction to an individual's financial penalty.

Concluding comments

- Use of chat applications for business purposes is fraught with risk. Firms incur increasing costs in ensuring their data assets, such as email and voice recording systems are archived, searchable and retrievable. Use by staff of WhatsApp and other non-server based chat applications for business purposes, cuts across these processes given the firm has no direct control of communications that would amount to company data. The simplest approach is to prohibit the use of personal chat applications, certainly when communicating with external parties. However, given the ubiquity and practicality of such chat applications a binary prohibition policy may be naïve.

- A blend of policy governance, staff engagement and technical input is required to reach a solution that works for the working methods of the firm taking into account their regulatory obligations in order to control the risks created by chat applications.

The Authors

John W Gibson
Partner

+44 (0) 20 8037 2324
Email John

Tim Harris
Associate

+44 (0) 20 8036 9395
Email Tim

Pere Puig Folch
Consulting Director of Data Strategy

+44 (0) 77 3384 0218
Email Pere

About Cohen & Gresser

Cohen & Gresser is an international law firm with offices in New York, Paris, Washington, DC, and London. We have an outstanding record of success in high-stakes and high-profile litigation, investigations, and transactional work for our clients, including major financial institutions and companies across the world. Our attorneys have superb credentials, and are committed to providing the efficiency and personal service of a boutique law firm along with the quality and attention to detail that are the hallmarks of the best firms in the world. The firm has been recognized in a wide range of publications, including *Chambers* and *The Legal 500*.

New York | Paris | Washington DC | London

www.cohengresser.com
info@cohengresser.com
+44 (0) 20 8037 2330

View C&G's Profile