

Client Alert

Providing Strategic Legal Guidance to the Financial Services Industry



JANUARY 22, 2024

For more information,
contact:

Peter Isajiw
+1 212 556 2235
pisajiw@kslaw.com

Aaron Stephens
+44 20 7551 2179
astephens@kslaw.com

Hannah Thorpe
+44 20 7551 2120
hthorpe@kslaw.com

Alex Tivey
+44 20 7551 7577
ativey@kslaw.com

King & Spalding

New York
1185 Avenue of the Americas
34th Floor
New York, New York 10036
Tel. +1 212 556 2100

London
125 Old Broad Street
London, EC2N 1AR
United Kingdom
Tel. +44 20 7551 7500

Recent Enforcement Trends Regarding the Use of Off-Channel Communications on Personal Devices

What U.K. Firms Need to Know

INTRODUCTION

Over the past decade, the use of messaging applications, such as WhatsApp, for business purposes as an alternative to traditional email has grown exponentially. Ease of use and accessibility for employees on mobile devices has blurred the lines between business and personal communications. Use of these so-called ‘off-channel communications’ – on work or personal devices – complicates a firm’s efforts to comply with regulatory requirements to preserve and monitor business communications. For instance, communications on personal devices are usually not accessible by a firm, and off-channel messaging applications often involve encryption and other features which make it difficult for employers to monitor and preserve communications of this type even when those applications are installed on corporate issued devices. This has led to an increase in related regulatory enforcement actions in both the U.S. and now the U.K.

U.S. REGULATORY ENFORCEMENT

Regulatory enforcement action relating to off-channel communications is a frequent occurrence in the U.S., with the Securities and Exchange Commission (“**SEC**”) and the Commodities Futures Trading Commission (“**CFTC**”) requiring financial institutions to ensure effective record-keeping, retention and monitoring of all relevant business communications.

In September 2022, the SEC and CFTC levied a record-breaking \$1.8 billion in fines against 16 financial services firms after staff discussed business issues on their personal devices and apps.ⁱ The regulators found



these institutions had failed to preserve the majority of those personal chats, violating federal laws which require financial institutions to preserve business communications. The key regulatory concern is that communications from unapproved devices do not flow through a firm's compliance or documentation retention systems and are therefore not available to regulators when conducting oversight and rooting out misconduct.

On 29 September 2023, the SEC announced that it had entered settlements with a further 10 firms.ⁱⁱ The firms in question agreed to pay \$79 million in combined penalties and retain independent compliance consultants to comprehensively review their policies and procedures relating to the retention of electronic communications. Since December 2021, the SEC and CFTC have issued penalties to over thirty firms totaling nearly \$2.8 billion. Additional penalties are expected in 2024.

With each round of regulatory settlements, the SEC has encouraged firms to conduct a self-assessment of their control environment, self-remediate, and potentially self-report violations in an effort to receive reduced penalties. For example, of the firms that settled with the SEC on 29 September, the one that self-reported paid \$2.5 million, significantly less than the \$8 to \$35 million paid by the other firms in that settlement announcement, and the \$9 to \$125 million paid by several firms in prior settlement announcements.

U.K. REGULATORY ENFORCEMENT

The U.K. would now appear to be following in the footsteps of the U.S.; various enforcement agencies are showing an increased focus on the use of off-channel communications.

On 23 August 2023, the U.K.'s Office of Gas and Electricity Markets ("**Ofgem**") fined an energy trading firm £5.41 million for not recording and retaining electronic communications, in breach of the Electricity and Gas (Market Integrity and Transparency) (Enforcement etc.) Regulations 2013, the first fine of its kind in the U.K.ⁱⁱⁱ Traders buying and selling energy had used their private WhatsApp accounts to discuss transactions, meaning that the firm had not preserved, and could not supply, these conversations to Ofgem when asked to do so. The firm had policies in place which prohibited the use of WhatsApp for trading communications but failed to take sufficient reasonable steps to ensure compliance with its own policies and regulatory requirements. The firm did, however, receive a 30% discount (from an original fine of £7.73 million) for settling with Ofgem within the settlement window.

Neither the Financial Conduct Authority ("**FCA**") nor the Prudential Regulation Authority ("**PRA**") prohibit the use of personal devices or encrypted messaging applications for business purposes. However, both have stringent record-keeping requirements that they actively enforce. For example, on 4 April 2023, the PRA censured a bank for "wide-ranging significant regulatory failings", including breaches relating to poor retention of WhatsApp messages.^{iv} Similarly, in October 2022, the FCA fined a broker £531,000 (and three of its directors over £200,000 collectively) for market abuse reporting failures.^v It observed that the broker did not have policies or training in place covering restrictions around the use of personal devices and encrypted messaging applications for business purposes.

In October 2023, it was reported that the FCA had discussed a crackdown on off-channel messaging applications with U.S. regulators,^{vi} suggesting that enforcement action in this space is likely to continue. It is anticipated that financial firm communications on social media and video conferencing platforms will be the next big area of U.K. regulatory focus.^{vii}

PROACTIVE REMEDIATION – U.K. GUIDANCE

Firms operating in the U.K. should be proactive in implementing measures to mitigate the risk of increasing regulatory scrutiny and enforcement. There are several potential issues firms must consider when doing so:



- **Issues with obtaining employees' personal devices** – U.K. firms generally cannot force employees to hand over their personal devices for inspection. In the absence of an express law or regulation providing access to personal devices, or the employee's consent, any requirement to view communications on personal devices may be considered an unjustified interference with the right of privacy.
- **Employment Law Considerations** – U.K. employers generally cannot make an employee's employment conditional on the employer's ability to access an employee's personal device. This concept has not been properly tested under English law but reliance on such a condition to dismiss an employee may give rise to a claim for unfair dismissal.
- **Data Privacy** - firms in the U.K. will need to consider carefully additional complications posed by the U.K. General Data Protection Regulation. Establishing a lawful basis for monitoring and accessing employees' personal devices is likely to be challenging.
- **Evidential Issues** - encrypted messaging applications include a variety of functions, including the ability to edit or delete messages after they have been sent. Firms using messages sent and received on these applications as evidence in investigations should therefore proceed with caution in terms of what evidential value can be placed on these messages.

Given the above considerations, firms operating in the U.K. should consider the following issues:

1. Device Control

To the extent possible, firms should consider prohibiting the use of personal devices and encrypted messaging applications on work devices for business purposes. Where that is not possible, firms should specifically list approved and non-approved messaging applications, and install surveillance software on work devices to allow firms to monitor communications on approved messaging applications.

2. Surveillance Review

Ensure that electronic communications through approved communications methods found on personal devices are incorporated into overall communications surveillance program and enhance surveillance lexicons to detect the potential use of off-channel communications.

3. New Technology

Explore how the emergence of new software and technology (that enables recording and monitoring of approved communication applications) might be deployed on work devices, or approved applications on personal devices, to help ensure on-going compliance with monitoring and recording obligations.

4. Policy Changes and Training

Update policies and procedures to bring them in line with current regulatory requirements and expectations. Clearly communicate any policy changes to all employees and/or reinforce existing procedures via training or otherwise.

5. Employee Attestations

Require employees to provide a specific, periodic written attestation that they are adhering to the firm's off-channel communications policies and procedures.

6. Disciplinary Framework



Review and enhance disciplinary framework to ensure penalties for policy violations related to use of off-channel messages are effective deterrents and consistently applied.

U.K. firms should also ask the following questions to determine whether corrective measures are necessary:

- Do firm policies and procedures related to the use of electronic communications for business, such as “bring your own device” arrangements, adequately address the appropriate use of off-channel messaging apps?
- Have compliance surveillance methodologies been updated to be reasonably designed to catch indications of off-channel business communications?
- Can the firm collect and re-ingest off-channel business-related messages from employee personal devices for surveillance and storage?
- Do firm policies address the human resources and employee relations implications associated with potentially collecting data from employees’ personal devices?
- Have the data privacy implications associated with potential collection of information from employee-owned devices been addressed?
- Does the firm offer technological solutions allowing for compliant text messaging communications? If so, are employees using them?
- Does the firm’s disciplinary framework adequately address the use of off-channel communications in violation of firm policy? If so, is discipline being fairly and consistently applied?
- Is the firm’s training on approved communication channels commensurate with the increased regulatory importance of this issue?

Whilst it is too soon to tell the extent to which U.K. regulators will pursue enforcement action related to the use of off-channel communications, taking these proactive steps now will put firms in a better position to avoid regulatory scrutiny and mitigate against enforcement risk.



ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,300 lawyers in 23 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered “Attorney Advertising.” View our [Privacy Notice](#).

| | | | | | |
|-----------|-----------|-----------|-------------------|----------------|------------------|
| ABU DHABI | CHARLOTTE | FRANKFURT | LOS ANGELES | PARIS | SINGAPORE |
| ATLANTA | CHICAGO | GENEVA | MIAMI | RIYADH | TOKYO |
| AUSTIN | DENVER | HOUSTON | NEW YORK | SAN FRANCISCO | WASHINGTON, D.C. |
| BRUSSELS | DUBAI | LONDON | NORTHERN VIRGINIA | SILICON VALLEY | |

ⁱ <https://www.reuters.com/business/finance/us-fines-16-major-wall-street-firms-11-billion-over-recordkeeping-failures-2022-09-27/>

ⁱⁱ https://www.sec.gov/news/press-release/2023-212?utm_medium=email&utm_source=govdelivery

ⁱⁱⁱ <https://www.ofgem.gov.uk/publications/ofgem-fines-morgan-stanley-co-international-plc-msip-over-ps54m-failure-record-and-retain-electronic-trading-communications>

^{iv} <https://www.bankofengland.co.uk/news/2023/april/pra-censures-wyelands-bank-plc-for-breaching-large-exposure-limits-and-failings>

^v <https://www.fca.org.uk/news/press-releases/fca-fines-sigma-broking-limited-530000-and-bans-and-fines-its-former-directors>

^{vi} <https://www.fnlonon.com/articles/fca-hints-at-future-whatsapp-crackdown-20231004>

^{vii} https://www.law360.com/whitcollar/articles/1773446?nl_pk=250e5db8-945a-4126-8622-1c00559c38f9&utm_source=newsletter&utm_medium=email&utm_campaign=whitcollar&utm_content=2023-12-06&read_main=1&nlsidx=0&nlaidx=0