COMMODITIES | OCTOBER 2022

HEFTY FINES TRIGGER URGENT REVIEWS OF THIRD-PARTY MESSAGING APPS AND PERSONAL DEVICE USE

Commodity traders are urgently recommended to review practices and compliance policies around the use and data retention in respect of personal devices and third-party messaging apps following increased regulatory focus.

The use of personal devices and messaging platforms has exploded and has been the subject of recent enforcement activity. In a coordinated enforcement action, the US Securities and Exchange Commission and the Commodity Futures and Trading Commission recently fined a number of firms a total of US$1.8 billion over their staff's use of personal devices for work related reasons. This is a stark reminder of the potential risks associated with the use of personal devices and third-party messaging apps without appropriate compliance and controls.

While these fines have been levied against financial services firms subject to regulatory oversight from the SEC and CFTC the use of personal devices and third-party messaging apps can, without appropriate compliance steps around their use, create enforcement and/or business exposure for all commodity traders irrespective of where they are based or their regulatory status.

For regulated traders it is likely that regulators may interpret existing rules around retention of books and records as, absent documented compelling reasons, requiring records of work communications documents held on personal devices. Either way it is critical that regulated traders understand and comply with the rules they are subject to in connection with the use of personal devices and third-party messaging and have policies and procedures which take into them into account.

For unregulated businesses and regulated traders, an investigator looking into potential offences (for example market abuse, insider trading, spoofing, bribery etc.) is likely to ask questions about policies and practices concerning personal devices and third-party messaging when assessing a compliance program. Ultimately, if an investigator determines a compliance program is lacking, for example because of a lack of a policy dealing with personal devices/third party messaging and/or books and records as a result of not retaining data, this may increase the likelihood of enforcement action in cases of violations with corresponding significant fines.

The Attorney General of the US, Lisa Monaco, has already telegraphed that this is the US position. In a recently issued memo (which equates to a policy memo) to the Criminal Division of the US Department of Justice the AG records that "*I have asked the Criminal Division to further study best corporate practices regarding use of personal devices and third-party messaging platforms and incorporate the product of that effort into the next edition of its Evaluation of Corporate Compliance Programs, so that the Department can address these issues thoughtfully and consistently.*"

Recently HFW spoke with David Last the Head of the Foreign Corrupt Practices Act Division. He explained that when he is dealing with companies under investigation for suspected Foreign Corrupt Practices Act violations, he is surprised by the number of companies who in the context of their compliance programs have not thought about the issue of personal devices and third-party messaging apps and how they will handle their use including communication, documents and records.

Putting to one side the enforcement perspective, personal devices and third-party messaging apps also create potential significant risk from a business perspective. If compliance and HR programs do not address these risks their businesses are potentially unsighted on what those working for it are doing. Worse, the problem created by the lack of records is compounded if the business is subject to litigation and is unable to properly defend its position because key records generated on personal devices and third-party messaging apps are unavailable because they have not been retained or they are unable to access them. In addition, the use of third-party messaging and

personal devices may increase susceptibility to data breaches arising from hacking with consequent enforcement risks in relation to privacy laws and business reputation among others.

The solution to all this is first to understand what present business practice is within a company for personal devices and third-party messaging apps. Second, to consider personal devices and third-party messaging apps in the context of your business and to comply with the rules which apply to the business if regulated. Third to make an informed decision which is documented about how the business wishes to deal with personal devices and third-party messaging apps and their use for work purposes following an assessment of risk and have corresponding policies and controls.

We are presently advising clients on all these issues against a backdrop of the explosion in the use of personal devices and third-party messaging and consequent increased scrutiny.

If you would like how we can help your business, please contact us.

For more information, please contact the author(s) of this alert

BARRY VITOU
Partner, London
T +44 (0)20 7264 8050
E barry.vitou@hfw.com

CINDY LAING
Associate, London
T +44 (0)20 7264 8263
E cindy.laing@hfw.com

ANNE-MARIE OTTAWAY
Partner, London
T +44 (0)20 7264 8054
E anne-marie.ottaway@hfw.com

hfw.com