HERBERT SMITH FREEHILLS

REGULATORS LEAD BUSINESSES IN MONITORING OF MISCONDUCT

21 July 2020 | Global

As regulators and law enforcement increasingly rely on advanced data analytics for monitoring and surveillance, the risk is growing that they will detect misconduct by employees and customers that has gone undetected by a company's own internal systems.

Business has been slow to adopt big data to monitor misconduct. Just 9% of all businesses recently surveyed by Herbert Smith Freehills said that they 'rely extensively' on data analytics to monitor employee conduct, and only another 25% saying that they were 'in the early stages' of implementing employee supervision through data analytics

This exposes businesses to two significant risks. First, the loss of an opportunity to self-report and secure cooperation credit, and second, that regulators may, with the benefit of hindsight, consider that a firm with adequate internal controls *would* have detected such misconduct – and that a firm's systems and controls themselves may come under scrutiny.

These risks are particularly problematic in an era in which businesses have encountered a significant increase in the volume of data and data sources requested by regulators and law enforcement. Nearly 65% of respondents to our recent survey said that their budgets for collecting data to satisfy regulators or law enforcement had stayed the same despite massive data volume increases.

This raises the key question of what businesses should learn from regulators' increasingly sophisticated use of big data in monitoring – and how best businesses grappling with the use of big data in monitoring can adapt to this new reality.

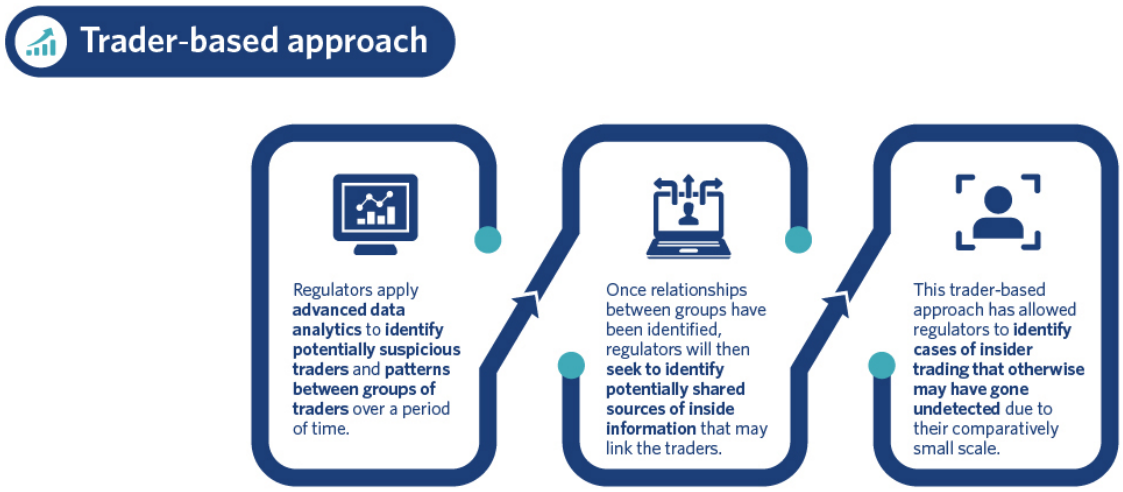
REGULATORS' USE OF BIG DATA TO DETECT AND PROSECUTE MISCONDUCT

Two prominent areas in which regulators have historically had great success in using big data to detect and prosecute misconduct are insider dealing and tax evasion.

Historically, it has been easy to predict the catalysts for insider trading investigations – namely, unusual spikes in the prices of securities shortly prior to the disclosure of material non-public information such as the announcement of a takeover bid or unexpected profit results.

These types of "security-based" investigations have traditionally been reactive, in that they rely on large movements of the market being reported publicly, or matters being reported to regulators (for example, brokers reporting potentially unusual trades by their clients).

However, in recent years, the US Securities and Exchange Commission (SEC)'s Market Abuse Unit has pioneered a "trader-based" approach to insider dealing enforcement which has been quickly emulated by other regulators, including the Hong Kong Securities and Futures Commission and the Australian Securities and Investment Commission.



CASE STUDY
In May 2019, the SEC announced that the Market Abuse Unit's work in detecting patterns of suspicious trades had led to the filing of insider dealing charges against an investment banker and his plumber, who the SEC alleged had made just US$76,000 in illicit profits by trading on tips passed to him by the banker.[1]
Similarly, the SEC has credited the Market Abuse Unit's work as helping identify repeated trades by a Silicon Valley executive prior to his employer's announcements of missed profit forecasts, through which the executive realised profits of US$120,000 and avoided losses of US$76,000.[2]

The use of big data has also allowed tax authorities globally to adopt an increasingly sophisticated approach to the detection of tax evasion, generally through the use of data matching protocols.

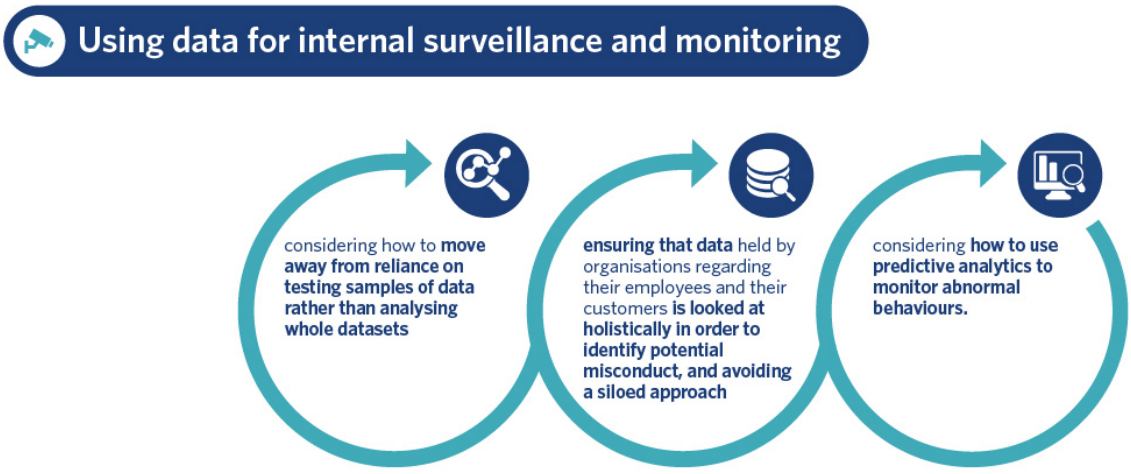
Tax authorities compel the production of data from third parties or request data from other government agencies, and then match that data against records held by tax authorities. In Australia, for example, the Australian Taxation Office (ATO) uses a wide variety of data matching protocols, including:

- Matching of credit and debit card records against income reported to the ATO to identify businesses trading as "cash only", and
- Analysis of insurance records to identify owners of lifestyle assets such as luxury boats and racehorses whose assets are inconsistent with the income they have reported to the ATO.

CASE STUDY
While this sort of data matching – particularly when combined with predicative analytics to identify the types of taxpayers most likely to commit tax evasion – has been used to identify potential cases for investigation, tax authorities have also sought to use big data to build their cases.
Most notably, in December 2018 the US Internal Revenue Service (IRS) released an RFI for a social media scraping tool that would be used to both advance their ongoing investigations as well as identify potential areas for audit.[3]

KEY NEXT STEPS FOR BUSINESSES AS THEY INCORPORATE BIG DATA INTO MONITORING PROCESSES

As businesses start to grapple with the challenges of incorporating big data and data analytics into their monitoring and surveillance processes, we recommend that businesses consider how they can use the data sources already available to them, alongside data analytics, in their own internal surveillance and monitoring capabilities. This approach is outlined below:



For example, it may not be possible for a bank to detect an employee trading on inside information if the trades are executed through accounts held with other institutions that have not been reported by the employee. However, the use of predictive analytics should increasingly make it possible for organisations to predict how frequently employees in particular parts of their business need to access confidential information – and identify employees who may be accessing such information more frequently than would be expected.

Despite the need to develop the use of big data for internal monitoring in order to protect against regulatory criticism and/or sanctions for weak controls, businesses need to ensure that their use of big data complies with all data regulation laws, as well as balancing the ethical considerations raised by enhanced surveillance.

ENDNOTES

1. https://www.sec.gov/news/pressrelease/2016-96.html
2. https://www.sec.gov/litigation/admin/2018/33-10525.pdf
3. https://www.fbo.gov/utils/view?id=db3ead17aa1c8d834e37f9ba4d6b3bc4

EXPLORE OUR CAMPAIGN

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

JOHN O'DONNELL
PARTNER, NEW YORK

+1 917 542 7809
John.ODonnell@hsf.com

CAMERON DUNSTAN-SMITH
PARTNER, JOHANNESBURG
+27 10 500 2692
Cameron.Dunstan-Smith@hsf.com

JEREMY BIRCH
PARTNER, PERTH

+61 8 9211 7214
Jeremy.Birch@hsf.com

CAMERON HANSON
PARTNER, SYDNEY

+61 2 9225 5224
cameron.hanson@hsf.com

LEGAL NOTICE