REPRINT FINANCIER WORLDWIDE

AUGUST 2013

FINANCIER WORLDWIDE corporatefinanceintelligence

WHITE-COLLAR CRIME

How to use company data efficiently to detect fraud and corruption

F. JOSEPH WARIN, MICHAEL DIAMANT AND OLEH VRETSONA

GIBSON, DUNN & CRUTCHER LLP

Organisations generate millions of pieces of data in the ordinary course of their business. This information "comes from many sources—internal and external, and in quantitative and qualitative forms – and facilitates responses to changing conditions", according to a report by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) entitled 'Enterprise Risk Management – Integrated Framework'. The creation and storage of such data is essential to the daily functioning of the organisation, not only in terms of achieving operational objectives and enhancing financial results, but also because it may help prevent or root out organisational misconduct, including fraud and corruption. But the presence of this data alone is not necessarily enough to prevent and detect wrongdoing. To leverage business information effectively, organisations need to "process and refine large volumes of data into actionable information", says COSO. Below, we describe how appropriately using company data can help prevent and detect organisational misconduct, including fraud and corruption, and we also provide general tips on creating

⏩

GIBSON DUNN

F. Joseph Warin and Michael Diamant are partners, and Oleh Vretsona is a senior associate, at Gibson, Dunn & Crutcher LLP. Mr Warin can be contacted on +1 (202) 887 3609 or by email: fwarin@gibsondunn.com. Mr Diamant can be contacted on +1 (202) 887 3604 or by email: mdiamant@gibsondunn.com. Mr Vretsona can be contacted on +1 (202) 887 3779 or by email: ovretsona@gibsondunn.com.

The authors wish to thank their colleague Asad Kudiya for his assistance.

effective information analysis controls. These tips are not exhaustive, and we recommend that any organisation confronting these issues consult with an information systems specialist – and any other necessary experts or consultants – to implement an effective information analysis protocol.

As one of the most prevalent types of organisational misconduct – fraud – poses a substantial risk to all organisations. The typical organisation loses 5 percent of its revenues to fraud each year. Applied to the 2011 Gross World Product, this figure translates to a potential projected annual fraud loss of more than $3.5 trillion, according to the Association of Certified Fraud Examiners 'Report to the Nations on Occupational Fraud and Abuse 2012 Global Fraud Study' (2012). In many cases, fraud is very difficult to detect. For example, the Association of Certified Fraud Examiners found fraud schemes lasted for a median of 18 months before being detected. The study also concluded that there are primary categories of fraud found in organisations: (i) asset misappropriation where "an employee steals or misuses the organisation's resources"; (ii) corruption schemes where "an employee misuses his or her influence in a business transaction in way that violates his or her duty to the employer in order to gain a direct or indirect benefit"; and (iii) fraud with respect to financial statements where an employee "intentionally causes a misstatement or omission of material information in the organization's financial report".

The type of organisation-generated information that may be relevant to detecting organisational fraud and identifying the key fraud risk areas is largely idiosyncratic to the attributes of the particular organisation. Information about misconduct frequently comes from tips, customer complaints, risk assessments, internal and external audit reports, investigation results, and remediation data, which generally results in organisations adopting reactive measures to address the identified misconduct. To seek out patterns of potential fraudulent behaviour more proactively and identify control gaps that permit fraud to go undetected, organisations increasingly focus on analyses of financial and operations data that they create in the ordinary course of business. Examples of such relevant data include basic balance sheet data, such as revenues and liabilities, procurement data, inventory write offs, payment data, costs, etc. The wide variety of data that may be used for this purpose – from employee complaints about low wages to unusual payment data to divergence between contract costs and deliverables – places an emphasis on creating a central repository of data analyses that allows the organisation to take advantage of the synergies in combining information from numerous sources and provides management and control functions with much needed access to a holistic view of the organisation's activities and behavioural trends.

Appropriately leveraging organisational data can help detect and address misconduct, including fraud, in a number of ways. At its most basic level, proper information analysis control allows for sensitive information, such as tips and negative risk assessments, to flow to appropriate executives and officers within the organisations. At a more indirect, and potentially more effective, level, the collective analysis of data showing, for example, a correlation between division revenue and a higher number of donations to third parties or employment of third-party agents by division could trigger a further review to determine if any corruption is present. This range of potential utility in leveraging organisational data only

▸▸

further emphasises the importance of implementing effective data gathering and analysis controls.

Irrespective of the possible complex information analysis controls that can be put into place, the objective for an organisation is simple: it should "establish□ an information systems infrastructure to source, capture, process, analyze, and report relevant information", notes the COSO report. Within this construct, we provide the following non-exhaustive tips in implementing an information analysis protocol. These tips are merely a starting point from which an organisation can begin constructing its own protocol.

Source and capture data

The first step is to locate relevant data. That includes, among other things, collecting all data created in the ordinary course of business and data that flow to the organisation from third parties. It also includes data in all divisions of the organisation and data from related legal entities. Without appropriately accumulating raw data, any examination of the collected data could lead to inaccurate findings and incomplete analysis about potential indications of fraud and corruption.

Process and analysis

For large or complex organisations, a technological platform is necessary to ensure data are properly collected, reviewed, and reported. Many entities have chosen internet-based platforms, allowing for "real-time information capture, maintenance, and distribution across units and functions", according to the COSO report. These platforms greatly improve data gathering and analysis by, among other things, diminishing the prospects of human error and also greatly improving the speed with which organisation-wide analyses can be conducted. An organisation should consult with an appropriate specialist to choose the best platform for its needs.

Once a technological platform is implemented, an organisation must apply appropriate tools, statistical or otherwise, to analyse the data. For example, one important tool in rooting out fraud is developing statistical models that can be applied to collected historical and current data to glean relevant patterns of potentially suspect behaviour and unusual activities, and flag outlier data.

Reporting the results

All completed data analysis, if relevant, should flow to the appropriate individuals or groups within the organisation, and should be stored in a central repository accessible to the organisation's management and control functions. Organisations should consider creating classification systems whereby various types of analyses are immediately forwarded onto those responsible for choosing to act on such analysis. A comprehensive reporting and data repository system is an important component of an effective information analysis protocol and equips management and control functions with comprehensive insight into the potentially suspect or unfavourable trends within the organisation. The easy access to critical information that such a system enables creates opportunities for management, internal audit, compliance, and other control functions to develop proactive and targeted measures that help detect and address organisational misconduct more effectively and efficiently.

Information analysis controls will necessarily vary based on the type of organisation at issue, its business, and its specific risk profile. But any management team should consider how to leverage the data its organisation creates or possesses to detect and prevent fraud and corruption. ■