Fraud Intelligence
Business intelligence | informa
www.counter-fraud.com

FEATURE › FRAUD (RISK) MANAGEMENT

Sound check

A clear view of the fraud risks in a business can often be obscured by disconnected data, as well as inadequate focus, technology and expertise. That's why an organisational risk check-up – followed by a deeper investigation if potential fraud or corruption are detected – is a relatively low-cost way of realising great benefits, explains Darren Matthews of K2 Intelligence.

In the United Kingdom alone, an estimated seven per cent of annual turnover is lost to schemes that might involve, variously, kickbacks, insider trading, financial statement and invoice fraud, bribery, as well as simple skimming and misappropriation of assets. [1] It is estimated that fraud costs business in the UK around UK£110 billion per year. [2]

Fraud, like any serious disease, spreads if not treated early. It saps corporate reputations and finances – and, in the worst cases, can prove fatal to an organisation. Though most companies can survive the financial impact of fraud, the reputational damage can be devastating. A loss of confidence by shareholders, customers, suppliers and regulators, along with the potential for litigation in the wake of a fraud, can lead to a drop in share price from which a company may never recover. In addition, if it can be shown that a company's directors and management have neglected their fiduciary responsibilities, criminal and civil charges could be brought against them.

Too many symptoms: all the data, none of the resources

For internal counsel and other corporate fiduciaries, it is a nightmare scenario to discover they have not put the necessary controls in place to combat fraud and corruption. However, determining where and how to deploy the proper preventive and early detection mechanisms can prove challenging and implementing such measures internally both inefficient and costly.

Technology has given companies an overwhelming supply of internal data to analyse, but the information is usually held in multiple locations and in systems that do not interact. Supplier and customer master files rarely cross paths with accounts receivable and payable files, while few companies have the internal staff resources and expertise

to analyse the data adequately to identify the ever-growing array of frauds that plague organisations.

Many companies rely, to some extent, on their audit process to find fraud. But an audit only examines part of the picture, namely the accuracy of a company's financial statements, and may not connect enough data points to allow a company to uncover a long-running or well-hidden fraud.

Finding the right doctor: independent assessments

Just like an annual physical, a regular, independent fraud risk assessment provides a focused check-up of a company around fraud issues – one that marries data with investigative skills to help flag potential problem areas unique to that organisation or industry. Experts in fraud risk know which data sets to look at, tests to run and the outside intelligence needed to identify red flags and ferret out the corrupt actors. With a better understanding of where and how fraud can occur, organisations can implement

targeted internal controls and greatly improve their ability to spot future frauds before they cause significant damage.

Having the right anti-fraud programme in place to help detect corruption as early as possible can protect assets, minimise risk, as well as improve the chances of recovering stolen assets. Finding a fraud as it is happening dramatically increases the likelihood of a significant recovery. Even if the programme does not detect a specific fraudulent transaction, a company can demonstrate to regulators and the public that it did everything reasonably possible to put policies and procedures in place to detect and deter fraud.

Developing a treatment: data and expertise

With companies now drawing a huge amount of data from a number of different sources, many find that performing a proper risk assessment – one that combines vast data sets and uses data analytics alongside data mining tools to identify patterns that indicate fraud and corruption – is beyond their resources and abilities.

Such a risk assessment will leverage bespoke technology to gather, link and test the data, as well as utilise industry experts to determine which tests to run and what types of results point toward fraud. These assessments involve experienced teams composed of fraud examiners and forensic accountants, former law enforcement professionals, prosecutors, and compliance professionals. Each risk assessment is unique to the company being analysed and is designed to identify red flags within the organisation, enabling the company to investigate and shore up its anti-fraud programmes and procedures accordingly.

The good news is that no matter how much a party tries to hide fraud, patterns tend to emerge. People have to authorise payments, invoices must go into systems, companies and accounts are created, and cash has to move. Each step leaves a trail that can help identify if a transaction was corrupt.

As an added benefit, because the examination is aimed at detecting patterns of behaviour and anomalies in corporate processes, companies can also weed out accounting irregularities that may have nothing directly to do with fraud. A large organisation, for example, may be recording double payments for goods or services because of a bad entry in the billing system.

Reviewing the symptoms: red flags

Just because a transaction exhibits multiple red flags does not mean it is part of a fraud. But the issues identified during a risk check-up do provide companies with strong clues about areas to investigate. Here are just a few of the most common red flags identified during a check:

- Invoices that use vague keywords (like 'consulting services', 'marketing' or 'entertainment') or that lack essential details like contact information or details about the supplier;
- Unusual invoice numbers and sequential invoicing. Fraudulent invoices can have invoice numbers invented by the fraudster. And a series of sequential invoices from a supplier may suggest over-reliance between the company and the supplier, increasing risk of fraud or business stoppage;
- Invoices that share a bank account, a next of kin, a phone number, or other data with a company employee. These can be flagged by cross-referencing Human Resources, payroll and other company information;
- Invoices that include offshore account information, as well as invoices with false tax and VAT numbers;
- Invoices that are just below authorised spending limits or that are divided to avoid limits. For instance, a manager is authorised to spend UK£5,000, and his or her invoices consistently come in just below that amount. Tests may also catch efforts to divide a large, single payment into two payments to get around control limits;
- Invoices paid more quickly than usual. In a fraud, the parties often try to move fast. For instance, a company may have 30-day payment terms but analysis shows that invoices for a particular supplier are paid in one or two days.

Diagnosis and prevention

Using subject-matter experts to follow up on red flags can yield substantial results. A dedicated team of fraud hunters, located across the world and with expertise in a broad range of industries, brings a unique perspective to examining transactions, people and companies. They leverage customised data analytics tools to handle more information, more efficiently. Not only does this provide insight into current wrongdoing but it also gives a company direction on where to improve their controls.

For instance, K2 Intelligence investigated a fraud involving a maintenance supplier for a large hotel chain. During the initial check, investigators flagged a certain maintenance supplier with a name that struck the investigators as odd for a company in its industry. Further research revealed that the company had invoiced the hotel chain in round numbers and that the invoices were sequential, which suggested that the company only had a single client. In addition, the price of the units it was supplying – towels – was very high compared to other suppliers. Those red flags led to a deeper investigation and investigators identified that a shareholder of the company was the wife of one of the hotel's procurement managers. They had scammed the hotel out of approximately UK£350,000 during a six-month period.

In another investigation, we helped a state-owned company based in the Middle East recover US$450 million after a check of its data flagged discrepancies in the price of raw materials. It was later discovered that a bogus procurement system had been developed to defraud the company.

This combination of technology and experience can be a game-changer for companies looking to root out corruption. In isolation, a single transaction may not raise an eyebrow. Yet when examined in context with other data, the transaction may prove to be a single strand in a web of corruption. And performing a regular check-up can ensure that fraud is identified before it can do significant damage. It's preventive medicine that will help ensure the company's reputation and finances remain healthy.

It is important to understand that a company's risk areas will evolve alongside an ever-expanding landscape of fraud schemes. Semi-annual or annual examinations ensure peace of mind for a company's board and management – and also take a bite out of losses that affect revenues and profits. An organisational risk check-up – followed by a deeper investigation if potential corruption is detected – is a relatively low-cost way of achieving a substantial increase in profitability.

Notes

1. Page 14 www.crowe.com/uk/croweuk/-/media/Crowe/Firms/Europe/uk/CroweUK/PDF-publications/Financial-Cost-of-Fraud-2018.ashx. The chart 'Increasing losses since 2007' indicates that losses from 2016 to 2017 are nearly seven per cent.
2. Note 5.8 page 15, ibid.

Darren Matthews (dmatthews@k2intelligence.com) is an executive managing director and regional head of Europe, Middle East, and Africa (EMEA) for K2 Intelligence.

Fraud Intelligence is published by Informa Law, Third Floor, Blue Fin Building, 110 Southwark Street, London SE1 0TA. *Fraud Intelligence* gives you practical insight, analysis and tools to combat fraud, whether you're in the corporate or non-commercial sector. Our financial crime content is available online via single-user subscriptions or multi-user licences at https://www.i-law.com/ilaw/financial.htm including *Lloyd's Law Reports: Financial Crime* (ISSN 1756 7637) and *Compliance Monitor* (ISSN 0953 9239).

Client Services: Please contact Client Services on tel: +44 (0)20 7017 7701; +65 65082430 (APAC Singapore), or email clientservices@i-law.com

Editorial queries: Please contact Timon Molloy on tel: +44 (0)20 7017 4214, or email timon.molloy@informa.com

Informa Law is an Informa business, one of the world's leading providers of specialist information and services for the academic, scientific, professional and commercial business communities.

Registered Office: 5 Howick Place, London SW1P 1WG. Registered in England and Wales No 1072954.

Print managed by: Paragon Customer Communications.