Our Code of Conduct

Know it. Use it. Live it.

Fraud

Our reputation for financial integrity and honesty is essential. Fraud is the opposite of honesty. Even when unproven, it can destroy our reputation. So we leave no room for doubt by applying due diligence and ensuring our books, records and financial reporting accurately reflect the true state of our business, our costs and our transactions.

In the simplest terms, fraud is a deception deliberately practiced in order to secure unfair or unlawful gain. **It is deceit for financial profit and it does not discriminate by geography or industry.** Although direct financial losses from fraud can vary significantly from one industry to another or in different parts of the world, the annual cost of fraud is substantial**. It has been estimated that a typical organisation can lose up to 5% of its annual revenue to fraud related activities.** Organisations are facing increasing threat on three fronts:

(1) Organised crime – as cross-border criminal activities are becoming more sophisticated;
(2) Cyber fraud – theft of business identity and confidential [digital] information; and
(3) Its own employees – from petty theft to infringement of intellectual property.

Today's fraud schemes are more advanced than ever, and governments across the world are increasingly investing skills and resources to track down the perpetrators and stop scams before they start.

Defrauding companies of money, goods and trade secrets is the most common aim of fraud. A single scam can destroy a company, deprive employees of their pensions, or cost investors billions. In addition, fraud has adverse economic effects on public services and less financially stable companies; it can affect job security and diminish levels of disposable income for society at large. For multinational and larger companies, big data and intelligence are invaluable assets for combating fraud across different sectors and in different countries. The problem is not that there is too little information, but too much – and most of it is not interlinked. Next generation technologies, in addition to their monitoring capabilities, are increasingly allowing companies to move from post-incident damage control to a more predictive approach, where weak-links can be identified in the system before fraudulent activity takes place.

The majority of corporate fraud cases involve accounting schemes designed to deceive investors, auditors, and analysts about the true financial condition of a company. This is usually done through the manipulation of financial data and the share price of a corporation. Artificially inflated value of the company is usually based on 'creative' accounting and fictitious performance indicators. Beside significant losses to investors, corporate fraud has the potential to cause serious damage to national economies and country reputation. It has been estimated that fraud committed by company owners and executives was more than nine times as costly as employee fraud. That is why 'white-collar' crime has become synonymous with the large-scale fraud schemes committed by high-ranking professionals and government officials.

Fraud

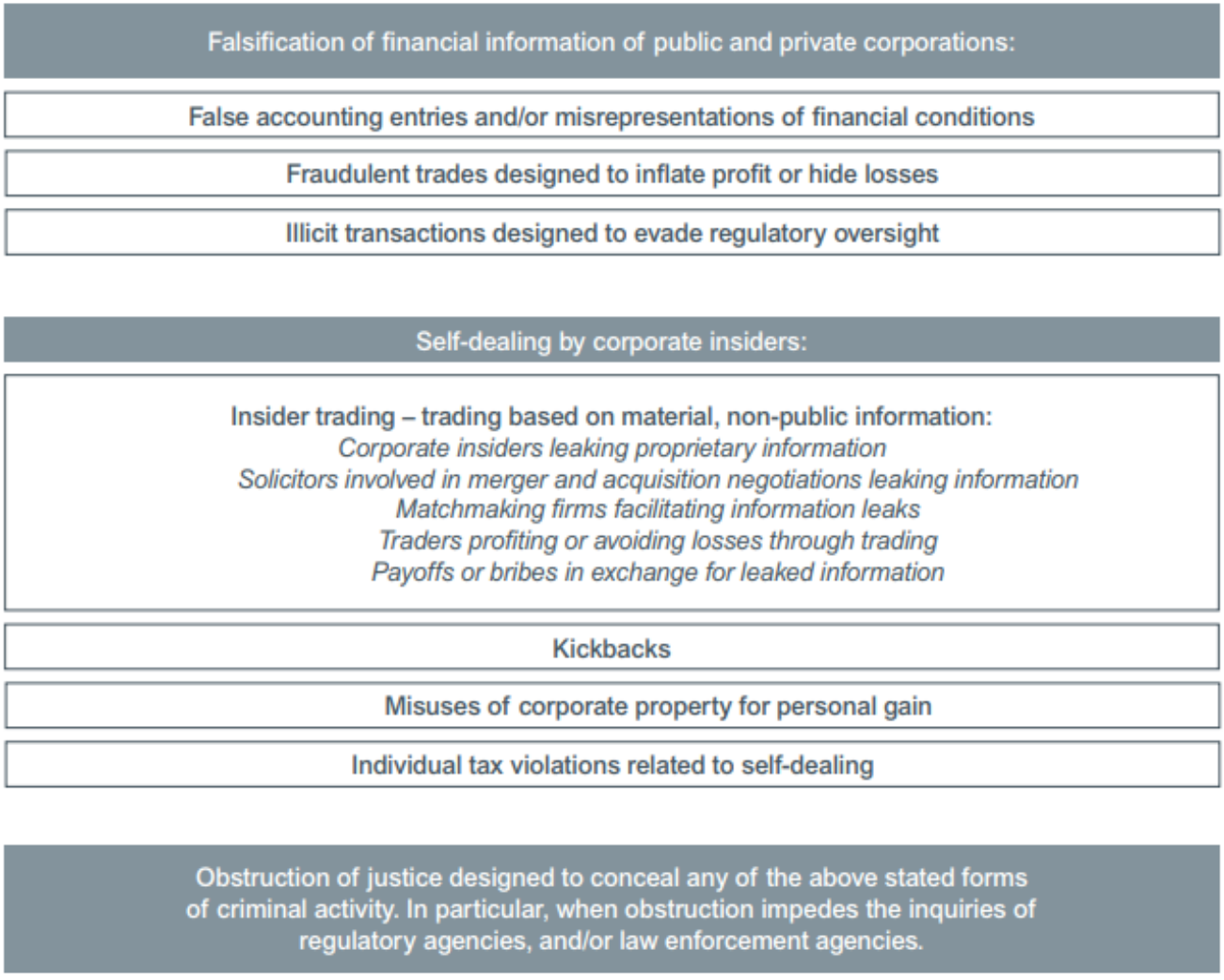
The four basic types of financial fraud in business include:

- **Embezzlement**: the illegal use of funds by a person who controls those assets.
- **Internal theft:** the theft of company assets by employees.
- **Payoffs and kickbacks:** situations where employees accept cash or other benefits in exchange for access to the company's business.
- **Skimming:** this occurs when employees take money from receipts and don't record the revenue on the books

Even with technology and monitoring systems in place, there is still no crime that has a 100% detection rate. On the one hand, if identified losses increase due to fraud, does that mean we are getting better at detecting fraud; or does it mean that the scope and scale of fraud is expanding in every direction?

Detection and reporting of fraud doesn't automatically mean that it will be prosecuted. This is because many companies are not willing to publicise fraudulent activity for fear of damaging their reputation and exposing their weaknesses. Such a selective form of transparency can only increase the problem if a company is not able or willing to sort out its internal checks and balances.

Once fraud is reported, some cases fail to be prosecuted due to legal loopholes, especially if the case involves several countries. Because of this,



Source: based on Federal Bureau of Investigations methodology (www.fbi.gov)

fraud is now one of the great unreduced business costs.

Experience shows that fraud can flourish in times of economic boom or bust. This level of continuity and consistency is particularly visible within the procurement cycle and can be extremely damaging for the company – from the magnitude of financial losses, to serious disruptions in supply chains, and loss of trust among investors, customers and regulators. If the practice remains unchallenged at the detection stage, the perpetrator will be encouraged to continue until the scheme is terminated or exposed by a third party. However, in cases where losses are avoidable, it becomes the duty of every enterprise to identify those weak-spots in the system before practices become institutionalised opportunities for unlawful gains.

Even when a company feels confident that they can spot the profile of a fraudster, and even if they know what to look out for, they must remain vigilant at all times. It is one thing to know when to raise the 'red flags', but knowing how to deal with fraud and retroactively address the problem is a different matter. Even though the overall process is not easy, by being aware of the dangers and potential weak spots in the system is half the battle. The second half is about detecting and addressing the issue in a timely manner and making sure that lessons-learned protocol have been consigned to institutional and operational memory. According to KPMG's analysis, the majority of scams are directed towards organisations where the relationship between buyer and supplier is in the public domain. In the age of open information, fraudsters appear to be abusing this trend with a high level of success. Paradoxically, as the private sector is trying to demonstrate greater commitment to transparency in their business dealings, that very action is simultaneously making them more vulnerable to fraud.

A cost due to fraudulent activity can only be reduced if it can be measured. A methodology to do this accurately has only been around for the past ten to fifteen years. Now that we can quantity fraud, companies may be also in the position to measure the financial benefits from investing in prevention and detection protocols. In the current macro-economic climate, reducing fraud may be one of the least challenging ways of reducing operating costs, while becoming more efficient at the same time. In the general scheme of things, fraud is an 'unnecessary' cost because much of it can be pre-empted.

The foundation of any fraud prevention program rests within the leadership of the company. Tone from the top is the essential ingredient in the fight against fraudulent activities. If staff are witnessing the abuse of authority or promotion of unethical activities, those practices will be interpreted as the company's norms and in no time bad governance will be institutionalised. In order to streamline behaviour expectations, a clear guidance on how to report and confront suspected fraudulent activity needs to be developed and communicated. Although it is an important step, formalising documentation will not be enough. As words are ingrained onto paper, good practices must be ingrained into business activity through active enforcement of its principles across operations. In addition, properly structured and interactive fraud awareness training can be an effective way of building staff capacity to monitor and detect inappropriate behaviour. Finally, time and resources need to be invested in conducting due diligence and fraud risk assessments at every stage of the business's operations and also across its supply chain.

Additional resources Further Reading

Step 1

Please refer back to Our Code of Conduct.

Step 2

If you would like to know more about Human Rights & Business, the following external links have been selected for your reference:

Serious Fraud Office (UK)

The SFO investigate, and where appropriate, prosecutes cases of serious of complex fraud which, call for the multidisciplinary approach and legislative powers of the SFO.

https://www.sfo.gov.uk/

KPMG Fraud Website

KPMG brings together information and thought leadership on fraud and related topics, creating a regularly updated source for analysis and comment on current issues in this area.

https://www.sfo.gov.uk/

UK Government Guidance on Crime and Fraud Prevention for Businesses in International Trade

Crime and fraud issues in international trade - theft of goods, money laundering, cybercrime, employee fraud, infringement of intellectual property.

https://www.gov.uk/guidance/crime-and-fraud-prevention-for-businesses-in-international-trade

PWC Fraud Academy

It is a forum through which members can share knowledge and participate in research to help prevent, detect and investigate fraud and economic crime in all their many forms.

http://www.pwc.co.uk/fraud-academy/

Federal Bureau of Investigation (FBI): White Collar Crime

It contains the most common scams that the FBI investigates and tips to help prevent individuals and organisations from being victimized. White-Collar crime is now synonymous with the full range of frauds committed by business and government professionals.

http://www.fbi.gov/about-us/investigate/white_collar

International Fraud Awareness Week

The weeklong campaign encourages business leaders and employees to proactively take steps to minimize the impact of fraud by promoting anti-fraud awareness and education. It takes place yearly during the third week of November.

http://www.fraudweek.com/

Step 3

Do your own research on the Internet