

Forensic Focus on COVID-19 Fortifying the front line of defence against fraud

This is the third part in a Deloitte Forensic series around COVID-19 business impacts and steps you can proactively take to help respond to and recover from the outbreak and mitigate potential fraud and financial crime risks.

Fraud and employee misconduct thrive during a crisis. The last downturn taught us that fraudsters are quick to find loopholes when the chips are down. The COVID-19 outbreak poses new challenges at a time when global growth is already slowing, and now organisations must fortify their defences against such opportunists more than ever.

Businesses may have let their guard down as they focus to stay afloat, by relaxing control procedures, delaying internal audits, reducing headcounts, or implementing long-term arrangements to work from home. The change from “business as usual” creates vulnerabilities for companies and new pressures for workers as they worry about their futures and job security.

When the tide is out, we have historically seen an increase in long-running schemes or frauds getting uncovered as there is a shock to their existing modus operandi – as was evident in the Madoff investment scandal that unravelled off the back of the 2008 Global Financial Crisis.

The fraud triangle

Fraud typically occurs where opportunity, motive, and rationalisation converge. This is known as the fraud triangle, and the COVID-19 crisis creates a perfect storm for fraudsters to exploit:

1. Opportunity

- **Lack of supervision and oversight:** With social distancing measures in place, offices are now empty but nonetheless

accessible. The usual lines of defence, such as management oversight, are also no longer present onsite, and fraudsters can now get away with misconduct without detection.

- **Controls and processes overridden:** As organisations quickly adapt to new ways of working, including virtual and remote work arrangements, many existing controls and procedures may be compromised, or even entirely disregarded.
- **Management distraction:** Reactive decisions made at short notice in response to the evolving COVID-19 situation may not have been adequately considered from a fraud risk perspective.

2. Motivation

- **Distressed employees:** For employees, the thought of potential job losses and pay cuts in the gloomy economic landscape may be a source of mental distress.
- **Projected prolonged economic downturn:** In certain situations, people may commit fraud to safeguard themselves to weather a perceived impending storm.
- **Pressure on financial results:** As businesses fail to meet key targets defined prior to the COVID-19 outbreak, individuals may feel the pressure to safeguard bonuses, or avoid presenting unfavourable results that will drive down share prices.

3. Rationalisation

- **Feeling unfairly penalised:** Employees may feel that they are entitled to better treatment as they had contributed to business success prior to the sudden disruption caused by the COVID-19 slowdown.
- **Prioritisation of self-interest:** During a crisis, the 'every man for himself' mindset may become more salient.

Red flags to look out for during the COVID-19 crisis

Businesses have to remain vigilant and actively seek out red flags¹ that may surface in this crisis, including:

- **Theft of confidential data:** Temporary or relaxed workarounds, including the sharing of remote log-ins, may create opportunities for fraudsters to steal confidential data.
- **Payroll fraud:** New and complex government COVID-19 support schemes that offer rebates and conditional payout may encourage fraud and manipulation.
- **Bribery and corruption:** With global supply chain disruptions, essential suppliers are demanding kickbacks or grease payments to facilitate cross-border shipments.
- **False reporting:** As the crisis wreaks havoc in the financial markets, some may see the opportunity to their camouflage non COVID-19 related losses.



Protect your people and your organisation

Against these headwinds, employees are an organisation's first line of defence. A recent survey by the Association of Certified Fraud Examiners showed that 43%² of fraud cases came to light through tip-offs, with half of them from employees.

Establishing safe channels – such as whistleblower or "speak-up" hotlines – for employees to step forward and 'blow-the-whistle' to expose sensitive issues in a confidential manner is therefore critical, and can be a simple, cost-effective way to enable companies to remain resilient throughout the COVID-19 crisis.

Designing an effective whistleblowing mechanism

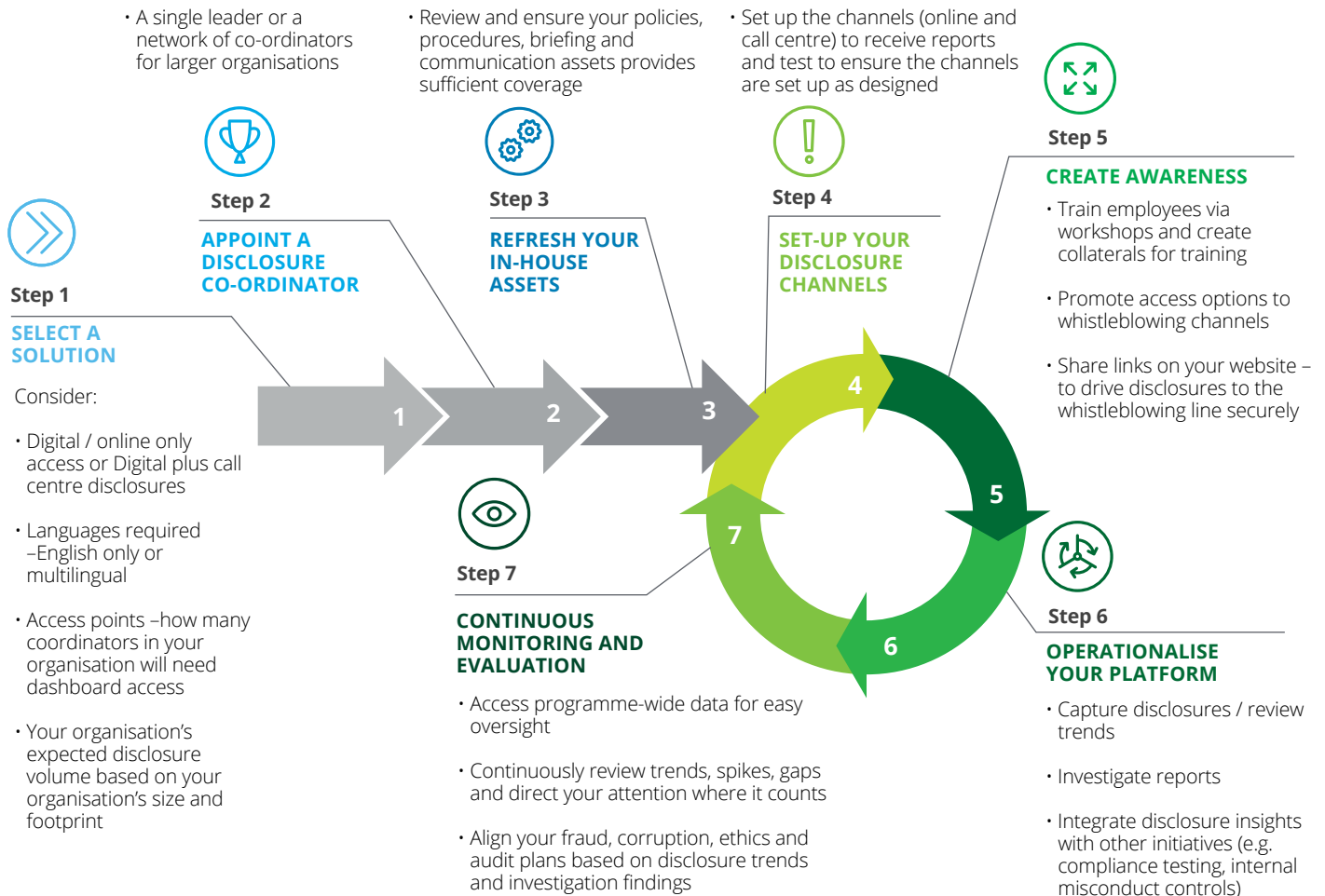
For the last two decades, Deloitte has been designing clear, practical and implementable whistleblowing programs to support organisations in monitoring their policies and assessing the effectiveness of their controls to minimise workplace misconduct and strengthen governance.

Broadly, this process entails five key steps (see Figure 1 below):

1. Select a solution
2. Appoint a disclosure coordinator
3. Refresh in-house assets
4. Set up disclosure channels
5. Create awareness

Deloitte Halo, our digital whistleblowing solution equips organisations with secure and confidential reporting channels layered with advanced security features. It also facilitates case management and provides insight using analytics across an organisation's whistleblowing disclosures. Incidents are reviewed by trained analysts, and high-risk matters are promptly escalated for immediate action.

Figure 1: Steps to design an effective whistleblowing mechanism



Should allegations surface regarding accounting/financial reporting misconduct and/or regulatory inquiries, it is important to seek assistance from an experienced team of forensic professionals dedicated to and well-versed in conducting extensive fact-finding financial statement fraud and corruption investigations using advanced analytics, digital forensics, and control remediation.

Marc Anley
Forensic Leader
Deloitte Southeast Asia
maranley@deloitte.com
+65 6800 1974

Jarrod Baker
Forensic Investigations Leader
Deloitte Southeast Asia
jarbaker@deloitte.com
+65 6800 3858

Oo Yang Ping
Forensic Digital Solutions
Deloitte Southeast Asia
yoo@deloitte.com
+603 7610 8537

Endnotes

- 1 Examples and descriptions provided are not exhaustive and may vary with the circumstances.
- 2 "Report to the Nations: 2020 Global Study on Occupational Fraud and Abuse". Association of Certified Fraud Examiners.2020.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax & legal and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organisation") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 312,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Ho Chi Minh City, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Shanghai, Singapore, Sydney, Taipei, Tokyo and Yangon.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organisation") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.