COVID-19 implications: internal fraud

Minds made for protecting financial services

Building a better working world

Introduction

The COVID-19 pandemic is a major event that is continuing to impact global businesses and economies in many ways. The risk of internal fraud has heightened due to an abrupt change in working practices, as well as increasing pressure on organizations and employees.

This paper focuses on the heightened internal fraud risks associated with the COVID-19 crisis.

- Enterprise-wide controls to prevent and detect fraud and network breaches may not be designed to operate in near-100% virtual environments.
- Anti-fraud, compliance and cybersecurity concerns may also have been de-prioritized in favor of maintaining business-as-usual (BAU) services.
- The reliance on staff to comply with policies and operate those controls is also under strain: as many people are working remotely, they may become disengaged and their actions may be subject to less scrutiny and oversight; similarly, financial and other concerns caused by COVID-19 may cause those in important oversight roles to be less vigilant.
- There may be pressure on organizations and staff to report positive results – i.e., demonstrating organizations are operating as usual without a negative impact on earnings and profitability, or staff compensation and incentive plans.

Red flags: what to look out for right now

The new challenges posed by the COVID-19 pandemic present heightened risks across all elements of The Cressey fraud triangle (1953):

1. Incentive or pressure

- Employees may feel worried that their jobs are at risk.
- There may be pressure to report positive results.

2. Opportunity

Employee risks

- If employees are not under pressure to report positive results, the current situation may provide them with opportunities to delay recognizing revenues or create provisions to cover up the effects of fraud temporarily.
- Employees may have more freedom to steal or distribute sensitive data if they are working remotely.

Control function/technology risks

- Employee surveillance, whistle-blowing lines and internal investigation mechanisms may not be operating at full capacity or optimized for remote working.
- Cyber controls (for example, firewalls) may be reduced to facilitate working remotely.
- Rapidly setting up laptops for remote working to maintain BAU may result in users being given inappropriate system access or insufficient cybersecurity.

Ask us for other EY Financial Crime and Forensics COVID-19 implication papers:

- Bribery and corruption risks
- External fraud
- Market abuse
- Navigating the impacts of the pandemic on financial crime compliance
- The internal investigation process
- The whistle-blowing function

*based on EY Financial Crime Compliance webinar 30 March 2020.

3. Rationalization

- Employees may find it easier to rationalize defrauding their company if they think they won't be getting a raise or bonus this year. This is more likely where incentive compensation is a large proportion of total compensation, or the method of incentive compensation is narrowly focused on short-term performance, or affected by earn-out provisions at acquired operations.
- Employees may be more inclined to commit fraud if long periods of remote working make them feel disengaged or undervalued.

We have identified several situations and potential trends where internal fraud risk should be considered in connection with the current COVID-19 crisis:

Financial reporting fraud

- Employees may have the ability to digitally manipulate supporting documents used to prepare financial statements.
- Market volatility may put pressure on employees to manipulate investment values to show a positive return/asset position.
- Revenue and expense recognition may not follow usual policies and accounting rules.
- Employees may be tempted to use the crisis to create unnecessarily large financial provisions, either to recognize a lot of unrelated issues all at once, or to use as a "cookie jar" that can be released to flatter financial results in the future.

Internal controls

- Key approvers may be off sick or unavailable, leading to issues with segregation of duties.
- Middle management's attention may be diverted to focus on maintaining sales and cash flow rather than oversight and control. Second and third lines of defense, such as internal audit, compliance and risk management, are unlikely to be able to fully compensate, and may have been asked to scale back their activity while the business implements new ways of working.
- Key approvers working from home may not show the same level of diligence in reviewing documents as they would if they were in the office.

Cyber risks and data access

- Employees may have, or adopt, irresponsible social media use habits.
- Employees may maintain access to sensitive data after notice of termination is served.
- Working remotely may increase the opportunity for employees to exfiltrate sensitive data.
- Employees may be working in shared accommodation where others can access and view sensitive data.

What does this mean for you?

Fraud risk assessment

Organizations should consider the changes the COVID-19 pandemic has created in their operations and re-perform fraud risk assessments in light of these changes. For example, what measures exist to deal with the concerns regarding falling incentives or contingent compensation? This will help organizations identify whether existing controls are still operating effectively, as well as identifying areas where new controls need to be introduced.

Internal controls

- Robust segregation of duties should remain in place, despite the logistical issues of teams working remotely. Flexibility should be incorporated into existing review processes to provide alternative reviewers and authorizers in case key employees are off sick or unable to connect.
- Fraud investigations and whistle-blowing teams should be active and appropriately staffed to respond swiftly to any reported issues. If employees know that these teams are still working effectively, it will be a strong disincentive for those considering to commit fraud.
- Plans to remediate internal control deficiencies identified before the lockdown, and that are still relevant, should be reassessed so that they are adequate and on schedule.

Surveillance and monitoring

- Provide the necessary infrastructure to work securely from home, including secure connections to the organization's network. Activity levels on organization-issued phones and laptops should be monitored to check that employees are not working on personal devices.
- Adequate monitoring of the content of calls, messaging and emails should also be in place. This should include monitoring sensitive data being sent outside the organization: for example, employees sending data to their personal email accounts or printing sensitive documents unnecessarily.
- Consider what additional monitoring and oversight is required for employees who historically did not have the option of working remotely: for example, trading employees or operational employees (both of which also pose regulatory risks through market abuse – see our separate paper "COVID-19 implications: market abuse" for more details).
- Keep track of working outside of office hours. While employees may be encouraged to work flexibly, organizations should still monitor this for potential abuse.

Training, oversight and morale

- Ensure adequate training and oversight is provided to employees who are moved to work in different parts of the business from their usual role.
- Where employees are working in a different part of the business, organizations should consider whether existing system access is appropriate, or whether previous access rights should be removed.
- Measure and maintain employee engagement to prevent employees becoming disengaged. This could include regular short surveys, leadership recognition of the difficult trading and working environment, and communications and tips on maintaining discipline and focus.

Key contacts

For further information, please contact the Financial Crime and Forensics team.

Rachel Sexton
Partner, Ernst & Young LLP
+44 20 7951 1179
rsexton1@uk.ey.com

David Higginson
Partner, Ernst & Young LLP
+44 779 877 4840
dhigginson@uk.ey.com

Glenn Perachio
Partner, Ernst & Young LLP
+44 20 7951 4628
gperachio@uk.ey.com

Julie Fenton
Partner, EY Business Advisory Services
+353 86 383 5556
julie.fenton@ie.ey.com

John Clinton
Associate Partner, EY Business Advisory Services
+353 87 231 5205
john.clinton@ie.ey.com