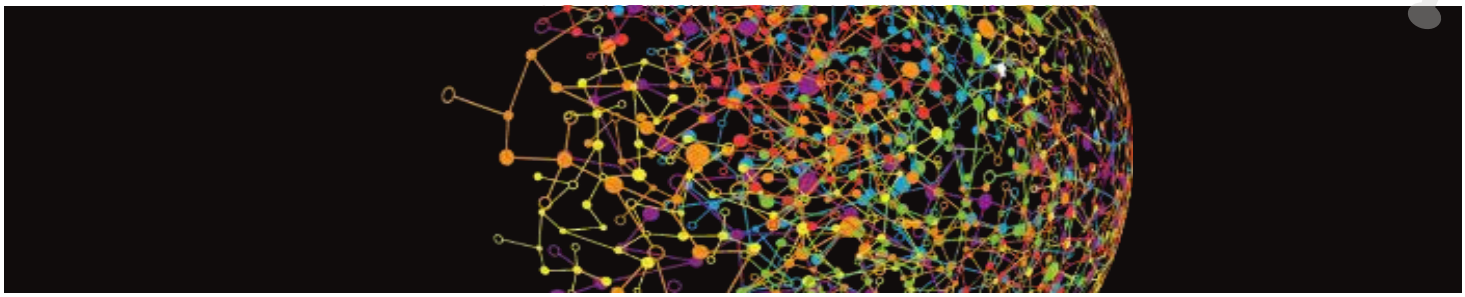
Deloitte.



COVID-19 Operating in the “new normal” – A backdoor to increased fraud risk?

Chief Compliance Officer support | Investigations team

The COVID-19 outbreak continues to have a devastating impact across the globe. The numbers of infected people increase every hour, and in many countries, movement restrictions are becoming tighter, health systems are struggling, and the stock markets have experienced their worst weeks since the 2008 financial crisis. It is not hard to see why the crisis might provide fertile ground for fraud. The combination of financial and health threats makes people more vulnerable and creates opportunities for fraudsters. In some countries it has already been reported that criminal gangs have started to target deserted commercial premises to steal goods and stock.
How long will it be before some employees are guilty of misconduct?

> “Companies need to assess how their employees might respond to the intense commercial pressure brought on by this unique economic situation.”

Key pressure points we observe in the new environment that increase the risk of fraud

Fast tracking new suppliers and other business partners (customers, suppliers, agents, intermediaries or other advisors)

- The risk of onboarding third parties which are not fully vetted and screened may result in working with disreputable or even restricted parties;
- Working with new agents/intermediaries, due either to closure of existing agents or inability to deliver the volume needed;
- The pressure of bringing products very quickly to market.

Increased dealings with government officials

- Regulatory approvals, key IP issues, supply chain, financial aid: all of these are increasing the dealings employees have with government officials in higher risk jurisdictions, many of whom may not be trained for such interactions.

Shift of resources

- Business models are challenged and executives are more focused on operational measures than compliance and fighting fraud;
- The temporary transfer of staff into operations may leave prevention functions understaffed;
- Illness among the workforce and absences from work become an issue in terms of capacity and finding replacements to do the work;
- Ongoing investigations are halted due to lack of resources and focus;
- Budgets are reduced for any activity considered ‘non-essential’.

Significant job cuts

- In the current situation, every company is looking for savings, and one of the immediate measures is to cut jobs or reduce payments to employees. As experience has shown, for some employees this may create an incentive to commit fraud.

Illustrative fraud schemes in the context of COVID-19

Using third parties which were not fully vetted and screened:

- Collusion with disreputable third parties by some employees, for their personal benefit;
- Submitting duplicate invoices for work performed, which are not properly checked and verified by the company;
- Invoicing for work not done may not be discovered due to temporarily weakened controls;
- Paying bribes or being engaged in illegal activities on behalf of the company.

Asset Misappropriation

- Theft of cash;
- Larceny, e.g. warehouse theft;
- Misuse/theft of data: temptation for employees, in particular leavers, to copy sensitive data (customer lists, pricing calculations, IP theft);
- Payment of invoices without usual approvals.

What questions should businesses be asking

New ways of working

- Are your employees able to perform their daily tasks remotely? Are digital signatures used? Can they approve processes without encountering physical constraints?
- Is there still enough oversight and control over foreign operations?
- Are there any controls in place to prevent theft of data by employees working remotely?
- Do you carry out a reprioritization of the risks? In our experience, risks such as lavish gifts and entertainment will be lower, but third party risks related to the supply chain will be greater. Are key controls in place to mitigate them?

Internal and external risks

- Did you assess your reliance on third parties? Are there any that will not have capacity or bandwidth to deliver? If yes, would you have time for the normal vetting process before onboarding new third parties?
- Does the shift or reduction in resources increase the risk of physical misappropriation of assets?
- Did you include anyone from the compliance/legal/investigation team in the crisis response taskforce?
- Do you send risk reminder communications to staff, that even in a time of crisis zero tolerance to fraud still applies and that employees should report any suspicious behaviour or fraud?
- Are the people dealing with government officials trained in respect of what they are allowed to do and what they cannot do?

Financial risks

- Is the company eligible for any of the government aid? Is there a risk that conditions for eligibility are partially fabricated?
- Is the company applying for the Swiss government backed loans? Is there a risk that cash pooling and intercompany loan set up are changed?
- Is there still enough oversight over bank transfers and defined authorization procedures?

Your local Contacts

Sven Probst
Lead Partner | Forensic
+41 58 279 64 01
sprobst@deloitte.ch

Nic Carrington
Partner | Forensic
+ 41 58 279 71 46
nicarrington@deloitte.ch

Andra-Aurora Horwat
Senior Manager | Forensic
+41 79 528 55 38
ahorwat@deloitte.ch