Deloitte.

Covid 19 and Fraud Risk:
Managing and responding in times of crisis

Companies across various industries are experiencing increased operational and financial pressure due to the COVID-19 pandemic. These pressures create a heightened level of economic risks such as:

- Significant reduction in trading
- Loss in revenue
- Loss in profits
- Loss in market demand
- Going concern
- Liquidation and total collapse.

These economic risks may lead to increased motivation or justification to commit fraud, through manipulation of financial results, misrepresentation of facts, misappropriation of assets and other fraud schemes.

Auditors should assess the ease of perpetrating fraud by being cognisant of the following basic indicators:

- Weak internal controls
- High tolerance for poor financial disciplines and errors in financial information
- Weak or non-existent processes by management for identifying fraud
- Non-compliance with Laws and Regulations and failure to report legislative contraventions
- Management override of controls
- Levels of actual or allegations of fraud or corruption (both internal and external) and the number of cases finalised
- Allegations against management and those charged with governance
- History of fraudulent financial reporting.

The fraud triangle is a model for explaining the factors that cause someone to commit fraud. It consists of three components which, together, lead to fraudulent behaviour:

- **Pressure –** Perceived un-shareable financial need
- **Opportunity –** Employees have access to assets and information that allows them to both commit and conceal fraud
- **Rationalisation –** "I was trying to support my family".

Financial statement fraud

For some, as these financial pressures mount, the line separating acceptable from unacceptable behavior can become blurred. At the same time, controls such as segregation of duties may be weakened due to work force displacement or distraction. Organisations have to be sensitive to the pressures that could result in financial statement manipulations at the corporate or operating subsidiary level.

Further, management should recognise that the environment created by adverse events such as COVID-19 could lead to increased fraud by employees (e.g., asset misappropriation or bonus maximisation schemes).

In particular, organisations should consider the following potential financial statement fraud risks:

- **Overstatement of revenue –** To make up for decreased trading, companies may endeavour to deliberately fabricate revenue to boost bottom lines and show how management was able to persevere in a challenging customer/ business environment.
- **Understatement of allowances and reserves –** Companies have numerous valuation accounts, allowances, and reserves including, but not limited to, those for inventory, accounts receivable, insurance claims incurred but not recorded, income taxes, and contingent liabilities. Management may be motivated to intentionally manage these reserves to avoid additional charges to the bottom line.
- **Manipulation of valuations and impairments –** Organisations use forecasts as a key element in the valuation of assets such as inventory, goodwill, financial instruments, investments (such as portfolio companies and debt/equity securities issued by entities), and certain long-term contracts. Disruptions to supply chains and the volatility in financial markets may result in organisational challenges to record such assets at their net realisable or fair values. Given the inherent uncertainty in valuing such assets in turbulent times, some companies may take advantage and consider intentionally delaying the recording of such losses or may attempt to overvalue certain assets in order to generate insurance recoveries.
- **Restructurings and "big bath" charges –** Given the strong probability of outbreak-related financial losses, affected companies may seek to write-off underperforming assets and/or record charges as part of larger organisational restructurings, sale, or closure of parts of their business that are either marginally associated with the impact from COVID-19 or not associated at all.
- **Capitalisation of expenses –** It may be tempting for companies to capitalise expenses and deduct them over several accounting periods rather than expense them immediately. Outbreak-related costs may be substantial, and executives may be inclined to spread the costs out over a few years, rather than expensing them when incurred.
- **Disclosure fraud –** Companies may be motivated to avoid fully disclosing the impact of COVID-19 on its overall business results, particularly with respect to risks, uncertainties, contingencies, and representations contained in their public statements, and regulatory filings. For example, particular concerns may arise regarding companies' or their counterparties' ability to satisfy contractual obligations. The disclosure should also include an assessment of whether reliance on force majeure provisions or common law principles of non-performance may apply. The adequacy and sufficiency of such disclosures may lead to claims of securities fraud by regulators and investors.
- **Margin manipulation –** Many companies are already experiencing significant decline in revenues, closures of plants, facilities, and storefronts, reduced transaction fees, and declines in assets under management, all while paying their employees and supporting current-state cost structures. Each of these actions increases the risk that an organisation's profit margins could be manipulated. There are many ways in which this can be done, but organisations should consider these risks and be aware of how it could potentially happen within their company.
- **Internal Controls over Financial Reporting (ICFR) –** The current economic environment may result in increased fraud risks related to internal controls. As many organisations move to a virtual work environment, there is a significant risk that fraudsters may find new ways to override existing internal controls, especially those critical to ICFR. Such controls may include, but are not limited to segregation of duties, delegation of authority, and information systems access. With a potential decrease in workforce, the rapidly changing nature of working environments, and the possibility of changes in individual responsibilities, modifications to existing controls may not happen with the same speed, or new controls may be implemented without sufficient testing of their design and/or effectiveness. Accordingly, the nature, timing, and extent of diligence performed in a changing control environment creates an increased opportunity for fraud.

Insider trading in the wake of COVID-19: An alert to boards and audit committees

Recent accusations of "stock dumping" raise questions about whether those made privy to nonpublic material information during times of crisis have placed their personal financial interests ahead of those of the investing public or their companies, potentially violating insider trading laws. "Stock dumping" is the selling of large amounts of a stock or stocks in general (shares as we know it in South Africa) at whatever market prices are in effect. For example, investors might dump stocks/ shares upon hearing of an outbreak of fighting in some part of the world or the impact of the Covid-19 pandemic we are currently experiencing.

In the United States of America (USA), the Securities and Exchange Commission (SEC) requires that any director, officer, or beneficial owner of a registered company file a Form 4 (Statement of Changes in Beneficial Ownership) with the SEC at any time a transaction resulting in a change in beneficial ownership has been executed. The filings documenting execution of these transactions are easily accessible by the general public via the SEC's online Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system.

The Wall Street Journal recently examined more than 4,000 public company SEC filings and reported that top executives of SEC registered companies sold approximately:

- $9.2 billion worth of shares in their own companies from February 1, 2020, through March 19, 2020, resulting in approximately
- $1.9 billion in savings. This activity apparently drew the SEC's attention, where in early March 2020, it issued a press release stating that "where a company has become aware of a risk related to the coronavirus that would be material to its investors, it should refrain from engaging in securities transactions with the public and to take steps to prevent directors and officers (and other corporate insiders who are aware of these matters) from initiating such transactions until investors have been appropriately informed about the risk."

The SEC's Division of Enforcement weighed in as well in a March 23, 2020, release in which it emphasized that corporate insiders privy to new material nonpublic information on the outbreak "should be mindful of their obligations to keep this information confidential and comply with the prohibitions on illegal securities trading." The release further referenced the Division of Enforcement's commitment to "ensuring that our Main Street Investors are not victims of fraud or illegal practices in these unprecedented market and economic conditions."

While the legal analysis as to whether specific trading violated securities laws is often complex, factual questions regarding the timing of trades, whether and to what extent nonpublic material information was available and disseminated prior to trading and to whom, the potential impact of such information to a company's financial condition and share price, and consistencies or inconsistencies between internal and public communications prior to and after trading activity—as well as other issues— will need to be resolved prior to legal determinations on the propriety of the trades.

In light of publicly disclosed trading activity and the recent SEC releases, boards of directors and audit committees, as well as legal and compliance departments of companies impacted by COVID-19, should assess whether trades made by insiders require additional scrutiny and/or investigation. Potential "red-flag" transactions will require prompt attention to determine the propriety of the trades, as such transaction may well give rise to regulatory inquiries and potential shareholder litigation.

We could face similar insider trading fraud schemes in a South African environment, given the potential pressures and opportunities created in our current economic crisis.

Cyber fraud schemes

As fraud and cybercrime experts we see situations that require extra attention in these unprecedented times. To name a few:

Averted awareness for cyber or financial crime
As many organisations encourage staff to work from home and in "crisis mode", existing internal controls could more easily be circumvented. The "let's do this first and worry about the documentation and procedures afterwards" attitude increases the risk of asset misappropriation and CEO fraud type of scams. The same applies for the "in order for your laptop to continue working you must install this software to continue working from home" rationale.

What to do?

- Do not accept instructions via phone from a person you do not know
- Do not allow for circumvention of internal control measures
- Do not click on links or open documents you do not 100% trust.

Reduced capability to prevent cyber or financial crime
With the closing of schools, universities and day care facilities, part of the working force is distracted, not in the usual location and may not have the same facilities as in the office. Documents are physically in a different location, internet connections and security from home is organised differently in comparison to office locations. This could lead to doing things slightly differently from the business as usual scenario.

What to do?

- If you cannot follow the normal procedures: wait, think and consult.
- Provide clear instructions to your employees and keep them updated on developments.

Rationalisation could increase pressure for downturn, insurance or bankruptcy fraud schemes
Classic fraud. As many organisations face financially uncertain times, classic fraud schemes might rise as well. People feel unfairly affected ("it is not my fault") and could take to fraud, ranging from simple larceny/theft to fake invoices and inventory manipulation.

Insurance fraud. The ACFE warns for increased insurance fraud related to disasters. The original warning is related to natural disasters like hurricane Katrina. At this moment it is uncertain what kind of claims will come.

Bankruptcy fraud. If the financial crisis is as significant as many are predicting it will be, this could mean a huge number of corporate bankruptcies. In fear of losing their business some will attempt to hide assets, divert funds or goods, favour certain debtors/creditors or try to increase credit lines.

What to do?

- Monitor transactions to identify possible red flags, unusual transactions or events.
- Manage third party risks including credit risks.

New arising schemes

Financial crime is ever evolving. Individuals are constantly seeking new opportunities for new scams. Some examples already witnessed by the Financial Crime Enforcement Network (FinCen) include:

Imposter Scams – Bad actors attempt to solicit donations, steal personal information, or distribute malware by impersonating government agencies (e.g. Centre for Disease Control and Prevention), international organisations (e.g. World Health Organization/WHO or healthcare organizations).

Investment Scams – The U.S. Securities and Exchange Commission (SEC) urged investors to be wary of COVID-19-related investment scams, such as promotions that falsely claim that the products or services of publicly traded companies can prevent, detect, or cure coronavirus.

Product Scams – The U.S. Federal Trade Commission (FTC) and U.S. Food and Drug Administration (FDA) have issued public statements and warning letters to companies selling unapproved or misbranded products that make false health claims pertaining to COVID-19.

FinCEN has received reports regarding fraudulent marketing of COVID-19-related supplies, such as certain facemasks. Insider Trading – FinCEN has received reports regarding suspected COVID-19-related insider trading.

Additionally, with social media and the public's need for information and updates on COVID-19, scammers attempt to create urgency or anxiety with emails purporting to be from an official source with information and or links relating to updates or news relating to COVID-19.

What to do?

- If it sounds too good to be true, it often is.
- Please verify the legitimacy of all organizations you're doing business with that is related to COVID-19 or for the purpose of managing the COVID-19 situation.
- Re-emphasise the awareness of Cybercrime and what employees should do when handling potentially malicious or phishing type correspondence.

Information security during COVID 19 (and generally for that matter) is of paramount importance in being one of many mechanisms to effectively prevent fraud. Some basic measures should be considered and these include amongst others:

- Preventing the use of external storage media and in instances where this is unavoidable these should be encrypted through the use of stringent passwords and kept under lock and key (ideally external storage media should be avoided)
- Prohibiting the use of personal email accounts to receive or distribute official company correspondence and data;
- Ensuring guidelines and protocols are in place for employee participation in video and audio conference calls in order to ensure privacy and confidentiality during lockdown periods
- With the increased use of home Wi-Fi networks there should be focused communications regarding the use of password protected services and that specific security measures should be in place to prevent unauthorised access to home Wi-Fi networks;
- Should printing of official company documentation take place at home there should be protocols in place regarding storage and subsequent secure and confidential destruction in line with each organisation's specific policies and guidelines.

These unprecedented times will be hard on people, organisations and governments. It is extremely difficult for organisations to navigate these unclear situations. However, it is important to keep an open eye for cybercrime and financial crime which can make the situation worse. Existing controls and procedures should at least remain intact, and when in doubt: take a step back, think and consult.

What should management do during these times?

Entity management should should conduct fraud risk assessment and update their fraud risk register and documentation to specifically consider whether there is a heightened risk of fraud as a result of the impact from the spread of COVID-19. This assessment should include any changes that have been made to the internal control environment to allow the continuing operation of the business and how these have been designed to mitigate the risk of fraud. Such an expectation equally applies to those charged with governance in terms of a reconsideration of the risk of management fraud. It is important that management include, not only their response to the current situation, but continue their assessment through the recovery process as different risks and motivations will arise. The fraud risk assessment outcome should be reviewed by those in a third line of defence, to ensure there's proper governance and systems of controls to prevent and detect fraud. This process should be updated regularly and be properly documented for evidentiary proof.

Wherever possible it is important to maintain segregation of duties. However, if for a short time this is not possible, say due to illness, those charged with governance must have early warning and monitoring mechanisms in place to ensure the lack of segregation of duties is not abused.

Below we provide insight into some of the fraud risk factors and potential fraud schemes that might be prevalent during this Covid-19 pandemic as well as controls and mitigations to consider:

Enhanced fraud risk factors	Potential frauds	Controls and mitigation
Pressure Management should be vigilant of the pressure to perpetrate fraud created by the distress of Covid-19 including: • Pressure to keep the company a going concern • Pressure to pay dividends and thus maintain distributable reserves • Pressure to continue to pay employees and suppliers • Pressure to meet bank and other covenants • Financial pressures on individual employees due to lost jobs, pay-freezes/cuts, unpaid leave, no bonuses or promotions • Pressure to report all bad news now and make unnecessary write-offs that can be wrongly attributed to Covid-19. Industries (travel, hospitality, retail) that have been impacted more severely by the economic impact of Covid-19 will see increased pressure to commit fraud. **Rationalisation** There will be those that see this as an opportunity to commit fraud, believing they are less likely to get caught as the current disruption draws management's attention to other areas. In addition, those that would not normally commit fraud may see it as acceptable in these circumstances 'for the greater good' of protecting their company, employees or themselves.	**Manipulation** Altering accounting records and supporting documentation is potentially easier when much of the workforce is working remotely. For example: • Models and forecasts may be edited to produce favourable answers and avoid impairments or covenant breaches • Transactions may be changed to avoid their impact on the balance sheet or income statement. E.g. changing the useful economic life of assets • Digital copies of supporting evidence may be changed as people have more time and space to do this at home • Changing cash flow forecasts to continue as a going concern • Failing to provide for loss making contracts • Failure to impair goodwill or other intangible assets that are no longer supportable • Missing provisions or write-offs of bad debts • Inappropriate capitalisation of expenses as tangible or intangible assets • Manipulating ratios to avoid breaches of covenants • Manipulation of alternative performance measures and other key performance indicators • Manipulating forecasts and ratios to attract new capital finance or short term loans • Manipulating results to qualify for state funding.	**Override of controls** In the normal course of business, management should have a robust control environment to prevent and detect fraud. However, the disruption caused by Covid-19 may require changes to that control environment for operational reasons. The disruption caused by Covid19 may result in a weakened control environment. There may be more opportunity for entity staff to override the controls that would normally be in place. Care should be taken that such changes do not expose the Company to increased risk of fraud: • Maintain segregation of duties so that no one individual has too much authority to post inappropriate journals, make payments and misappropriate cash or other assets • Ensure proper accounting records are still maintained. Consider requesting third parties send data to more than one employee so it can be subsequently cross checked for changes if required • Think about ways to secure the Company's assets using technology where physical controls cannot be implemented. Consider more digital security such as CCTV and electronic tagging of assets.
Opportunity Disruption and changing working patterns may lead to companies needing to change their usual internal controls to allow operations to continue. For example: approvers of journals or other financial decisions may change if key people are off work; system access rights for employees may be increased to allow remote working; and documentation requirements may be reduced. However, disruption may cause existing fraud schemes to surface as the perpetrators are unable to keep them hidden. Management should be alert to pre-existing frauds, not just new ones.	**Misrepresentation** Financial statements must be a true and fair reflection of the company. In the current environment entities may look to misrepresent the true position of the company. Examples may include: • Omitting information that could change the reader's view of the performance of the company. For example, failure to disclose the breach of a loan covenant, or the loss of material contracts • Missing or limited scenario analysis. Scenarios that were previously considered remote may now be relevant to readers of the financial information. Intentionally excluding such information from reporting could impact a readers view of the company • Concealing related party transactions • Giving undue prominence to alternate performance measures designed to hide the true reality of the Company's position • Intentional failure to disclose post balance sheet events. Scenarios that were previously considered too remote to be worth reporting may now be required to give a full picture of possible future events, for example the impact of an 80% drop in customer numbers or prolonged supply chain disruption. The fraudulent reporting of financial information may range from bias when preparing the reports, to ignoring negative events and information, to outright falsifications.	IT controls are important too. With increased home working and remote access to company systems, controls need to make sure only the right people are accessing the right systems. Home networks may not have the same security and firewall defences as office environments. Regular activity log reviews and increased cyber awareness are recommended to identify unexpected behaviour. Similarly, administrative functions which may normally be restricted to a few privileged individuals may have been provided to additional staff to provide some resilience; it is important this is managed in a risk-aware manner, for example through monitoring of activity and time-limited access. The tone from the top is important. Whilst current times increase the demands on management and flexibility is needed to ensure continued operations, this must not be at the cost of good internal control. Leadership must make sure segregation of duties remains intact and that staff continue to act ethically at all times.
	Misappropriation Risk of theft of valuable, marketable inventory or fixed assets will be increased. Where sites are not staffed to their usual levels, physical security may be reduced creating an opportunity for theft. Examples may include: • A spike in the disposal of assets with no proceeds • Unusual write-offs of stock; • New suppliers that have not gone through appropriate vetting processes • Purchasing staff collusion with suppliers leading to inflated pricing to the company (to cover bribes to purchasing staff) • Payments to suppliers that are not on the approved supplier lists or intervention to divert payments (e.g. change in payment details) • Payments to related parties, or members of staff outside of payroll. There is also an increased risk of misappropriation of funds where the disruption requires changes to authorisation controls. Management should be vigilant for unrecognised payments or new suppliers. We expect the disruption to lead to increased activity from perpetrators.	

Management and those charged with governance should clearly report any material changes to the fraud profile of their business, and any changes that have been made to the internal controls they have in place to mitigate the risk of fraud in their annual report. The recent reviews into the audit profession show there is a clear demand from stakeholders for greater detail about the fraud risks and the actions directors have taken to fulfil their obligations to prevent and detect material fraud against the background of their fraud risk assessment. Companies should carefully consider whether it is helpful to include specific comments in the annual report about the company's response to fraud risk associated with Covid-19.

The audit report must also reflect, where material, the procedures teams have performed and the findings and observations made in relation to the increased risk of fraud from Covid-19.

Deloitte's dedicated team of forensic professionals can assist companies in navigating through these uncertain times, helping organisations to manage/ mitigate fraud risks and potential resulting damages

Deloitte can assist you with any fraud risk and forensic related matter, in particular, Deloitte have experience assisting in the following areas:

Remote Forensic Investigations

Assist companies throughout the investigative lifecycle to modify their "traditional" approach to effectively conduct investigations remotely while maintaining confidentiality and information security.

Digital Forensic

Apply forensic practices to collect preserve and process structured and unstructured data in a legally, defensible manner.

eDiscovery services

Deliver solutions to complex document review challenges using a wide range of advanced technologies to process, host, search and produce relevant and reliable evidence. Depending on the matter type, data volumes, case theory, and number of concurrent users, we match the right technology, people and processes to meet our clients' unique needs.

Fraud Risk Analytics

Assist companies with the earlier detection of fraud and the continuous monitoring of fraud risks. This includes fraud risk assessment services.

Managed document review

Deliver efficient and defensible managed document review services to clients and their legal counsel in complex business disputes and investigations in a controlled operations environment. Combining multidisciplinary teams of expert document reviewers, such as lawyers, chartered accountants and certified fraud examiners, with tested methodologies for conducting defensible technology-assisted document reviews.

For more information or assistance please contact:

Gregory Rammego – grammego@deloitte.co.za
Kgomotso Ngakane – kngakane@deloitte.co.za