Understanding Fraud, Corruption & Financial Crime in South Africa

Fraud, corruption and financial crime are often discussed when a major scandal makes the news. We hear about government tenders being manipulated, public money being misused, companies being investigated and individuals being accused of taking bribes. It can sometimes feel like these are problems that only affect large organisations or the public sector, but that is not the case. Fraud and corruption can happen in businesses of any size and can involve employees, suppliers, clients, business partners or even people outside the organisation.

For a business, the consequences can go much further than simply losing money. A fraudulent transaction can damage relationships with clients and suppliers, while corruption can result in investigations, legal costs, loss of contracts and serious reputational damage. Businesses also have responsibilities when it comes to understanding who they are dealing with, where money comes from and how certain transactions are handled. This is where concepts such as due diligence, ethical business practices and FICA compliance become important.

What is fraud?

In simple terms, fraud involves deliberately deceiving another person or organisation in order to obtain an advantage or cause someone else a loss. While people often associate fraud with someone stealing money directly, it can take many different forms and is not always immediately obvious.

In a workplace, fraud could involve an employee submitting false expense claims, creating or approving fake invoices, using a company credit card for personal purchases or manipulating financial records. It could also involve someone providing false information to obtain funding, creating fictitious suppliers or employees, misrepresenting their qualifications or using confidential company information for personal gain.

Fraud can be committed by almost anyone who has access to a business, including employees, management, suppliers, contractors and clients. It can also happen internally or externally. For example, a business could be targeted by someone pretending to be a legitimate supplier, while an employee could abuse their position to make unauthorised payments.

One of the reasons fraud can be difficult to detect is that the person responsible may not fit the stereotype of a fraudster. It could be a long-serving employee who is trusted by management or a supplier that the business has worked with for years. This does not mean businesses should treat everyone with suspicion, but it does mean that proper controls and checks should not be replaced by trust alone.

What is corruption?

Corruption is generally associated with the abuse of power or a position of authority for an improper benefit. Bribery is one of the most familiar examples. This could involve offering or accepting money, gifts, favours or another benefit in exchange for influencing a decision.

However, corruption is not always as obvious as someone handing over an envelope of cash. It can involve a company being given preferential treatment because of a personal relationship, a supplier paying a kickback to secure a contract, an employee failing to disclose a conflict of interest or someone manipulating a procurement process so that a particular business wins a contract.

For example, imagine an employee is responsible for choosing a supplier and recommends a company owned by a close family member without disclosing the relationship. The supplier may still be capable of doing the work, but the undisclosed relationship creates a conflict of interest and raises questions about whether the process was fair.

This is why businesses need clear rules around conflicts of interest, gifts, procurement and business relationships. Not every gift or business relationship is automatically corrupt, but businesses should be able to identify situations where personal interests could influence professional decisions.

Fraud in the workplace

Workplace fraud can be particularly damaging because it often involves people who already have access to the organisation's money, information or systems. A person who understands the company's processes may also understand how to work around them.

Some warning signs may include unusual or unexplained payments, repeated expense claims without proper documentation, sudden changes to supplier banking details, payments to third parties, missing records or pressure from someone to bypass the normal approval process. None of these things automatically means that fraud has taken place, but they can justify asking further questions.

This is where internal controls become important. Businesses should have clear procedures for approving payments, appointing suppliers, recording expenses and managing access to financial systems. Where possible, responsibilities should also be separated so that one person does not have complete control over a transaction from beginning to end.

The aim is not to create an environment where employees feel that they are constantly being watched. Good controls are there to protect the business and its employees. If something does go wrong, proper records and approval processes can also help establish what happened and who was responsible.

Why corruption affects businesses and the economy

Corruption has an impact beyond the people directly involved in a corrupt transaction. When contracts are awarded because of personal relationships or improper payments rather than through a fair process, businesses that follow the rules can lose opportunities. When public money is misused, the wider public ultimately carries the cost.

There is also a significant impact on confidence. Businesses are less likely to invest or compete in an environment where they believe contracts can only be secured through connections or improper payments. Over time, corruption can affect competition, economic growth and trust in institutions.

For individual businesses, the consequences can be just as serious. A company linked to corruption may face investigations, legal proceedings, financial losses, loss of clients or contracts and reputational damage. Even where a business was not directly involved in the wrongdoing, being associated with a problematic transaction or business partner can create significant difficulties.

South Africa's ongoing investigations into fraud, corruption and the misuse of public funds provide numerous examples of how these problems can develop. The Special Investigating Unit (SIU), for instance, has continued to investigate matters involving public procurement, UIF-TERS claims, National Lotteries Commission funding, Eskom-related contracts and other transactions. Each investigation has its own facts and circumstances, but they demonstrate the importance of proper oversight and accountability.

For businesses, the lesson is fairly straightforward: a transaction that looks beneficial in the short term can become a much bigger problem if the people involved, the source of the money or the process used to approve the transaction were not properly considered.

Building an ethical business

Most businesses have policies covering issues such as fraud, conflicts of interest and workplace conduct. The bigger challenge is making sure that these policies actually influence the way people behave.

Ethical business practices need to be part of the company's culture rather than something that only gets discussed when there is a problem. Employees should know what is expected of them when dealing with clients, suppliers and business partners, and they should understand what to do if they are offered a gift, become aware of a conflict of interest or notice something that does not seem right.

Leadership plays an important role here. If senior employees are seen ignoring policies or making exceptions for themselves, it becomes difficult to convince everyone else that the rules matter. On the other hand, when management follows the same standards expected from everyone else, it helps create an environment where ethical behaviour becomes part of normal business practice.

An ethical culture also means making it possible for employees to raise concerns. People are far more likely to speak up when they know there is a clear process for reporting misconduct and that they will not automatically be treated as the problem for raising an issue.

Understanding FICA and why compliance matters

The Financial Intelligence Centre Act 38 of 2001, commonly referred to as the FIC Act or FICA, forms part of South Africa's framework for combating money laundering, terrorist financing and related financial crime.

The Act places specific obligations on businesses and professionals that fall within the definition of an "accountable institution". These institutions are listed in Schedule 1 of the Act and include certain legal practitioners, estate agents, trust and company service providers, financial services businesses and other specified entities.

Depending on the type of business, compliance obligations can include identifying and verifying clients, understanding beneficial ownership, assessing risk, monitoring transactions, keeping appropriate records and reporting certain suspicious transactions and activities to the Financial Intelligence Centre.

For businesses that fall within the scope of the FIC Act, these are legal obligations rather than optional good practices. It is therefore important for a business to understand whether it is an accountable institution and, if it is, what requirements apply to its particular activities.

It is also worth remembering that compliance is not simply about collecting an identity document and putting it in a file. Businesses need to understand who they are dealing with, why the relationship exists and whether the transactions taking place are consistent with what they know about the client and the relationship.

Due diligence: know who you are doing business with

Before entering into a relationship with a new client, supplier, investor or business partner, one of the most basic questions a business should ask is: **Who are we actually dealing with?**

Due diligence is about obtaining and verifying information so that a business can make an informed decision about who it is working with. The level of due diligence required will depend on the nature of the relationship and the risks involved, but it may include information such as identification documents, proof of address, company registration documents, details of directors and information about the individuals who ultimately own or control a company.

Businesses may also need to understand the purpose of the relationship, the nature of the transaction and, where appropriate, the source of funds or source of wealth. Supporting documents such as contracts, invoices or other records may help confirm that the transaction is genuine.

The point of due diligence is not to make business unnecessarily difficult. It is about identifying problems before the business becomes involved in them. If a potential client cannot clearly explain who owns their company, where significant funds have come from or why a transaction is being structured in an unusual way, those issues should not simply be ignored.

Due diligence should also not necessarily end once a client has been accepted. Relationships can change, businesses can change ownership and transactions can become more complicated over time. Businesses should therefore remain alert to information that may change the level of risk associated with a client.

What should businesses check before accepting funding or working with a client?

There is no single set of documents that will apply to every client or transaction. The information required will depend on the circumstances, the nature of the business and any applicable legal or regulatory requirements.

However, businesses should generally be able to establish who their client is and, where relevant, who owns or controls the entity. They should understand why the client is approaching them, what services are being requested and what the transaction is intended to achieve.

Where money is involved, businesses should also consider whether the source of the funds makes sense in the context of the client and the transaction. If a client suddenly provides a large amount of money that does not appear to match their known circumstances, it may be appropriate to ask for further information.

The same applies to inconsistencies in documents. Different company names, unexplained third-party payments, conflicting addresses or changes to banking details should be checked rather than simply accepted because the transaction appears legitimate on the surface.

Good due diligence is ultimately about being able to answer a few basic questions: **Who is this person or business? Why are we dealing with them? What is the purpose of the transaction? Where is the money coming from? And does everything we have been told make sense?**

Handling clients' money

Businesses that handle money on behalf of clients have an additional responsibility to make sure those funds are properly managed. Client money should not simply be treated as ordinary business income, and there should be clear procedures for receiving, recording, holding and paying out funds.

Businesses should know who is authorised to receive money, who can approve payments and who can make changes to banking information. Where possible, responsibilities should be separated so that one person does not have unrestricted control over the entire process.

Accurate records and regular reconciliations are also important. If a payment is questioned several months later, the business should be able to explain what the payment was for, who authorised it, where the money came from and where it went.

This is particularly important for professional firms that handle client funds. In these circumstances, the money may belong to the client or another party rather than the business itself, making proper controls and record-keeping essential.

Why verifying the source of funds matters

Knowing who transferred money is not necessarily the same as knowing where the money came from.

Source of funds refers to the origin of the particular money being used in a transaction. Depending on the circumstances, the funds could have come from a legitimate business transaction, the sale of an asset, a loan, an investment or an inheritance.

The important question is whether the explanation makes sense when compared with what the business knows about the client and the transaction.

For example, a client may transfer a substantial amount of money into an account and explain that it came from the sale of a property. That explanation may be supported by a sale agreement and other documentation. If, however, the client cannot explain the origin of the money, the funds come from an unrelated third party or the transaction is structured in an unusual way, further questions may be necessary.

Under the FIC Act, accountable institutions may be required to monitor transactions and consider whether the source of funds is consistent with their knowledge of the client and the client's risk profile. Businesses do not necessarily need to prove that money comes from criminal activity before concerns can be raised. Suspicion can arise from the circumstances surrounding a transaction.

Reporting suspicious transactions

When something does not look right, ignoring it does not make the problem disappear.

Businesses that are subject to the FIC Act have specific reporting obligations in relation to suspicious and unusual transactions or activities. This can include transactions where there are reasonable grounds to suspect that the money may be connected to unlawful activity, transactions that have no apparent lawful or business purpose, or transactions structured in a way that appears intended to avoid reporting requirements.

Suspicious Transaction Reports generally need to be submitted to the Financial Intelligence Centre as soon as possible and no later than 15 days, excluding Saturdays, Sundays and public holidays, after the person becomes aware of the facts giving rise to the reporting obligation.

Businesses should also be careful about discussing the report with the client. The FIC Act contains provisions dealing with the disclosure of information relating to suspicious transaction reports, commonly referred to as the prohibition against "tipping off". For this reason, businesses should have a clear internal process for escalating concerns to the appropriate compliance officer or responsible person rather than confronting a client without understanding the legal implications.

The important point is that reporting a suspicious transaction does not mean a business has personally determined that a crime has been committed. The purpose of the reporting system is to provide relevant financial intelligence to the appropriate authorities.

Whistleblowing and the duty to report

Employees are often the people who notice problems first. They may see unusual payments, hear conversations about a bribe, notice that procurement procedures are being bypassed or become aware that someone is receiving an undisclosed benefit from a supplier.

However, employees are unlikely to report wrongdoing if they believe doing so will put their jobs or careers at risk.

South Africa's Protected Disclosures Act 26 of 2000 provides a framework for certain disclosures of unlawful or irregular conduct by employees and provides protection where the requirements for a protected disclosure are met. Businesses should therefore consider whether they have appropriate mechanisms in place for employees to raise concerns.

This could involve an internal ethics process, a compliance officer, a confidential reporting line or another appropriate mechanism. What matters is that employees know where to go and that concerns are dealt with seriously.

A whistleblowing system is only useful if people trust it. If employees believe that reports will be ignored, or that they will face consequences for speaking up, they are much less likely to use the system.

The issue of whistleblower protection has also received significant attention in South Africa following the State Capture Commission and subsequent discussions around how whistleblowers can be better protected. This is another reminder that businesses need to think about not only how they prevent misconduct, but also how they respond when someone brings a problem to their attention.

Lessons businesses can learn from current events in South Africa

South Africa continues to deal with investigations and legal proceedings involving allegations of fraud, corruption and the misuse of public funds. Recent SIU investigations have included matters involving UIF-TERS claims, National Lotteries Commission funding, Eskom-related contracts and other public-sector transactions.

One example reported by the SIU in 2026 involved a court judgment setting aside a R9 million National Lotteries Commission grant relating to a sports complex that was never built. Other investigations have involved allegations of irregular contracts, fraudulent claims and the misuse of funds.

The facts of these cases are different, and allegations should always be distinguished from findings that have been established through the appropriate legal process. However, there are still useful lessons that businesses can take from what is happening around them.

Firstly, businesses should not skip their normal checks simply because a deal looks attractive. A large contract or profitable opportunity can still carry significant risk. Secondly, procurement processes need to be transparent, particularly where large amounts of money are involved. Thirdly, businesses need to understand where their money is going and, where required, where incoming money has come from.

Perhaps most importantly, businesses should not wait until there is a major problem before looking at their internal controls. By the time fraud or corruption has been discovered, the money may already be gone, records may have been altered and relationships may have been damaged.

Final thoughts

Fraud, corruption and financial crime cannot be prevented by one policy or one person within a business. It requires a combination of good systems, responsible management, proper due diligence and a workplace culture where people understand that ethical behaviour matters.

For businesses that fall within the scope of the FIC Act, understanding and meeting their compliance obligations is part of operating responsibly. For businesses more generally, the principles behind these requirements are still useful: know who you are dealing with, understand the purpose of a transaction, verify information, keep proper records and ask questions when something does not make sense.

Businesses should also remember that compliance is not about making it impossible to do business. It is about making informed decisions and reducing the chances of becoming involved in something that could cause serious problems later.

Fraud can start with one false invoice. Corruption can start with one undisclosed favour. Financial crime can start with one unexplained payment. The earlier a business identifies the warning signs, the more options it has to deal with the problem.

Ultimately, protecting a business from financial crime is about more than protecting its money. It is about protecting its reputation, its employees, its clients and the trust that allows the business to operate in the first place.