The Financial Intelligence Centre Act, 38 of 2001

Introduction by the EAAB as the Supervisory Body of the estate agency sector

The EAAB, as the Supervisory Body of the estate agency sector, plays a key role in overseeing the implementation of the FIC Act, as amended, within the sector. The implementation, compliance and enforcement of the FIC Act, including customer due diligence and the application of the risk-based approach, requires continuous engagement between the EAAB and estate agency enterprises.

It is self-evident that a transitional period was required before full compliance with the new requirements of the FIC Act could be achieved by the sector. The necessary transitional period will, however, cease as from 1 April 2019 - after which date all estate agency enterprises will be required fully to ensure compliance with the provisions of the FIC Act.

The EAAB will, in the interim, continue to oversee the implementation of the FIC Act by the sector especially as estate agency enterprises undergo the period of transition enabling them to meet the new customer due diligence and risk-based requirements. The EAAB will, during the changeover period, liaise with the FIC while also applying a risk-based supervisory approach so as to ensure knowledge of, and compliance with, the FIC Act by estate agency enterprises both large and small. The EAAB has, thus far, primarily engaged with the sector in this respect through its Continuing Professional Development programme which has been used as a vehicle to advise estate agency enterprises on how to implement any remedial actions that might be necessary in respect of possible non-compliance with the requirements of the FIC Act. This interaction will need to be comprehensively broadened to ensure compliance with the FIC Act after 1 April 2019 and the EAAB intends implementing positive steps in this regard.

Estate agency enterprises are expected, in the interim, to start demonstrating progress towards full compliance with the new requirements of the FIC Act. The EAAB, together with the FIC, will utilise such measures as inspections and other available oversight activities to monitor, guide and advise estate agency enterprises on the correct implementation of the amended FIC Act. In so doing both the EAAB and the FIC will always remain mindful of the fact that the larger enterprises may well be better resourced and equipped to satisfy compliance expectations more quickly than might be the case with smaller enterprises.

The FIC has indicated that the sanctioning of non-compliance with the new requirements of the FIC Act is likely to be delayed so as to allow sufficient time for estate agency enterprises to make the required implementation adjustments. The process of implementing the new FIC Act requirements will take account of any imbalances and inconsistencies that may be found to exist within the estate agency sector. It cannot be overlooked, however, that the sector plays a critical role within the South African economy as a whole. The result is that there is a definite sense of urgency in ensuring and expediting full compliance with the risk-based and customer due diligence approaches now embodied in the FIC Act.

It is hoped that this revised study material will play a significant role in enabling full compliance by the estate agency sector with the FIC Act sooner rather than later.

The Financial Intelligence Centre (FIC)

The Financial Intelligence Centre (the FIC), established by the Financial Intelligence Centre Act, 38 of 2001 (the FIC Act), is the national point for the gathering, analysis and dissemination of financial intelligence. The FIC identifies the proceeds of crime and combats both money laundering and the financing of terrorism with its primary role being to protect the integrity of the South African financial system.

Discharging the important anti-money laundering and terrorist financing legislative mandate

The FIC discharges this important legislative mandate by:

- developing and providing financial intelligence to a range of agencies; and
- supporting the investigation and prosecution of criminal activity; by
- identifying the proceeds of crime and combating money laundering and the financing of terrorism.

The FIC Act is a key component in the regulatory architecture and legal framework designed both to protect the integrity of the South African financial system and enhance the administration of the criminal justice system.

Other noteworthy legislation relevant to achieving this objective includes:

- the Prevention of Organised Crime Act, 121 of 1998; and
- the Prevention of Constitutional Democracy against Terrorism and Related Activities Act, 32 of 2004.

Ensuring that the South African financial system is as transparent as possible

It is self-evident that, to achieve efficacy in the combating of money laundering and terrorist financing, the South African financial system must be as transparent as possible. The financial system should, ideally, be based on the introduction and implementation of robust client due diligence measures that ensure the timeous capture of adequate information in the records of financial, and other, enterprises and make possible the real-time sharing of information which is essential to the further investigation of money laundering and terrorist financing.

Creating the required level of transparency

The provisions of the FIC Act are, therefore, designed to create the required level of transparency within the South African financial system.

In so doing the FIC Act:

- renders it extremely difficult for criminals to hide the illicit proceeds of their activities in the formal financial sector;
- prevents criminals from profiting from their criminal activities; and
- cuts off the resources that might otherwise be available for terrorist financing.

Implementing the risk-based approach

The FIC Act presently incorporates a **risk-based approach** to such necessary compliance elements as, for instance, client due diligence (CDD), into the regulatory framework. Estate agency enterprises, as accountable institutions in terms of the FIC Act, must not only fully understand but also appreciate their potential exposure to money laundering and terrorist financing risks in the sector within which they operate. Through understanding, and effectively managing, such identified money laundering and terrorist financing risks, estate agency enterprises will be placed in a better position not only to protect and maintain the integrity of their enterprise activities but also materially to contribute to the integrity of the South African financial system as a whole.

Glossary of acronyms and common terms

It is desirable, at the outset, to be aware of some of the more common acronyms and terms found in the FIC Act and which are also generally used by the Financial Intelligence Centre.

'Accountable institution' means a person referred to in Schedule 1 of the FIC Act which schedule includes, inter alia, an estate agent as defined in the Estate Agents Act, 112 of 1976.

'Controlling ownership interest' refers to the ability, by virtue of voting rights attached to share holdings, to take relevant decisions within a legal person and to pass resolutions by the legal person.

"CTR" refers to a cash threshold report submitted in terms of section 28 of the FIC Act.

"CTRA" refers to a cash threshold report submitted in terms of section 28 of the FIC Act where the transaction values have been aggregated and add up to total of the prescribed threshold value.

'Effective control' means the ability to materially to influence key decisions relating to a legal person or the ability to take advantage of capital or assets of a legal person.

"FATF" refers to the Financial Action Task Force, to which South Africa belongs, an international standard-setting body that is headquartered in France and which seeks effectively to combat money laundering and terrorism financing worldwide.

"The FIC" means the Financial Intelligence Centre established in terms of section 2 of the FIC Act.

"FIC Act" refers to the Financial Intelligence Centre Act, 38 of 2001.

"IFTR" means the International Funds Transfer, referred to in section 31 of the FIC Act, which must be reported to the FIC.

"MLTFC Regulations" refer to the Money Laundering and Terrorist Financing Control Regulations made in terms of section 77 of the FIC Act.

"POCDATARA" means the Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 33 of 2004.

"Prospective Client" means a person who has indicated a wish to enlist the estate agency services of an estate agency enterprise but who is unlikely either to transfer any value to the enterprise or has not firmly indicated a readiness to transfer value to the enterprise.

'Risk' means the impact and likelihood of money laundering and terrorist financing taking place. Risk refers to the **inherent risk**, or the level of risk that exists before mitigation, and not the **residual risk**, or the level of risk that still remains after mitigation.

'Risk-based approach' means the approach pursuant to which an accountable institution identifies, assesses and understands the money laundering and terrorist financing risks to which enterprises are exposed and implements appropriate anti-money laundering and counter-terrorist financing measures proportionate to those risks.

'**Risk factors'** means variables that, either on their own or together, may increase or decrease the money laundering and terrorist financing risk posed by a enterprise relationship or a single transaction.

'**RMCP'** refers to the Risk Management and Compliance Programme of an accountable institution in terms of section 42 of the FIC Act.

'Senior management' in an accountable institution is determined by the size, structure, and nature of the enterprise. The senior manager whose approval is required for purposes of the FIC Act must have sufficient seniority and oversight to take informed decisions concerning the enterprise's compliance with the FIC Act that will actually bind the enterprise to those decisions.

'Source of funds' means the origin of the funds involved in an enterprise relationship or a single transaction and includes the activities that generated the funds used in the enterprise relationship.

'Source of wealth' means the activities that have generated the total net worth of the client such as, for instance, the activities that produced the client's funds and property. These may, for instance, be derived from an inheritance or savings.

'**Supervisory body**' means a functionary or enterprise referred to in Schedule 2 of the FIC Act, which schedule includes, inter alia, the Estate Agency Affairs Board, established in terms of the Estate Agency Affairs Act, 112 of 1976.

"The POC Act" refers to the Prevention of Organised Crime Act, 121 of 1998.

"Reporter" means the person or entity that makes a report to the FIC.

"SAR" refers to a Suspicious or Unusual Activity Report submitted to the FIC in terms of section 29(1) or 29(2) of the FIC Act.

"STR" refers to a Suspicious or Unusual Transaction Report submitted to the FIC in terms of section 29(1) of the FIC Act.

"TFAR" refers to a Terrorist Financing Activity Report submitted to the FIC in terms of section 29(1) or 29(2) of the FIC Act.

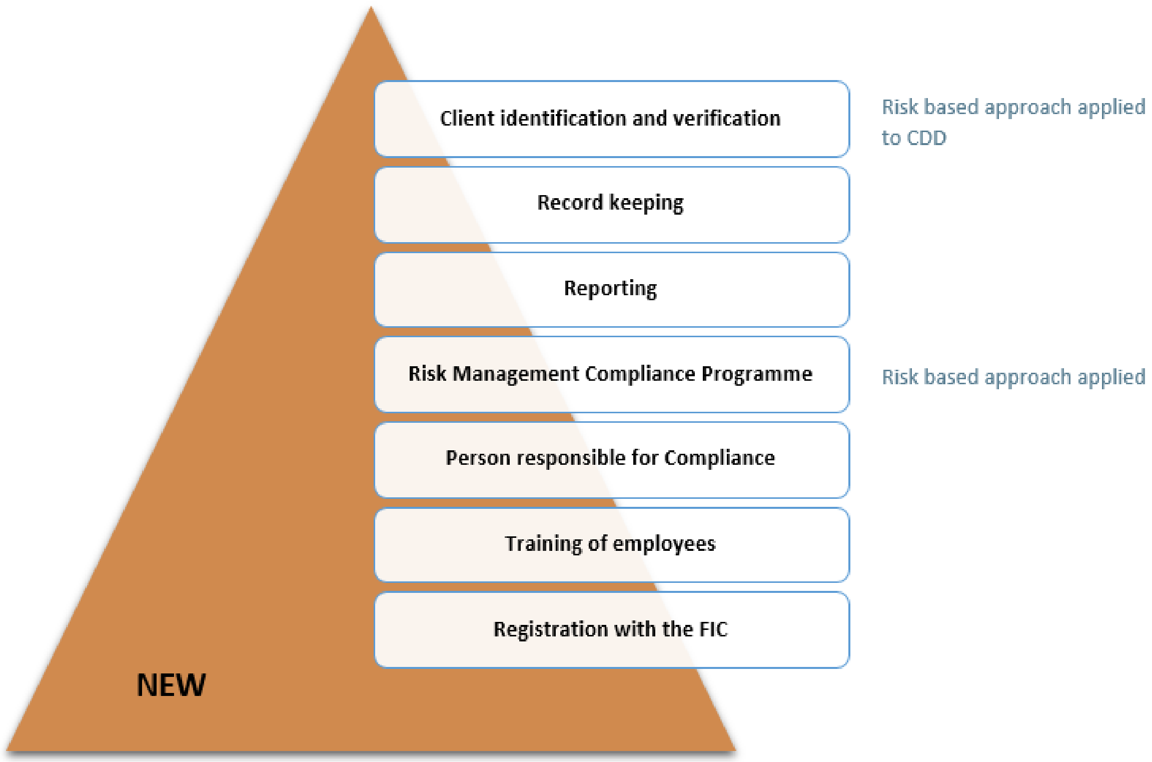
"TFTR" refers to a Terrorist Financing Transaction Report which must be submitted to the FIC in terms of section 29(1) of the FIC Act.

"TPR" refers to the Terrorist Property Report which must be submitted to the FIC in terms of section 28A of the FIC Act.

The seven pillars of compliance

It is important, at the outset, for estate agency practitioners and enterprises both to understand and appreciate that the amended FIC Act relies, for its efficacy in eradicating the twin scourges of money laundering and terrorist financing, on the application of **the seven pillars of compliance**, as reflected in the diagram hereunder.

Each separate pillar forms an integral component in the successful application of the risk-based approach that has now been adopted by the FIC Act. Each of the seven pillars of compliance is more comprehensively dealt with in the course of the study material. It is suggested, moreover, that the diagram be continuously referred to as a guide to the implementation of the risk-based approach contained in the FIC Act and also used as a valuable aid in assimilating the study material in context.



The concept of money laundering

The FIC defines money laundering as "… the manipulation of money or property in order to disguise its true source."

The FIC, furthermore, notes that criminal activities, such as, inter alia, drug trafficking, human trafficking, racketeering and corruption, generate significant profits for the individuals or groups who engage in these unlawful activities. When seeking to utilise the illegal funds, however, criminals risk drawing the attention of the authorities to their criminal activities. This has the further effect of exposing them to prosecution and the possible forfeiture of the unlawful proceeds of crime. If, thus, criminals are to benefit from their ill-gotten gains they must strive to conceal the origins of those funds. They attempt to do precisely this by engaging in money laundering activities.

The financing of terrorism

The FIC describes the financing of terrorism as involving "… the solicitation, collection and the providing of funds and other assets with the intention that it may be used to support terrorist acts, terrorist organisations or individual terrorists. The funds and assets may stem from both legal and illicit sources. The primary goal of persons involved in the financing of terrorism is not to conceal the sources of the funds and assets, as with money laundering, but to conceal both the financing and the nature of the activity being financed."

Risk

It must, at the outset, be noted that the FIC Act requires estate agency enterprises, as accountable institutions referred to in Schedule 1 of the FIC Act, to apply a risk-based approach when performing mandatory client due diligence measures. Risk, in this respect, refers to the likelihood, and the consequent impact, of uncertain events on set objectives. Risk, thus, derives mainly from threat, vulnerability and consequence.

- **Threat** can, potentially, cause harm and, in the context of money laundering and terrorist financing, includes criminals, terrorist groups and their facilitators, their funds, as well as the past, present and future money laundering or terrorist financing activities.

- **Vulnerability** comprises those things which can be exploited by the threat or which may support or facilitate that threat. When identifying vulnerabilities the focus will necessarily be on, for example, the factors representing weaknesses or the features that can be exploited in a given system, enterprise, product or service.

- **Consequences** are the impacts of a threat, or the exploitation of vulnerability, if this impact were actually to materialise.

In the context of money laundering or terrorist financing, therefore, risk may be thought of as the likelihood and impact of money laundering or terrorist financing activities that could materialise due to a combination of threats and vulnerabilities manifesting themselves in an estate agency enterprise.

Inherent and residual risks

For the purpose of money laundering it is important to distinguish between **inherent** and **residual** risks. The inherent risk is the risk that an event or circumstance will exist before the application of the necessary controls or mitigation measures designed to address that risk. A residual risk refers to level of remaining risk once the necessary controls and mitigation measures have been implemented.

In this context money laundering and terrorist financing risks refer to:

- the threats and vulnerabilities that promote the laundering of the proceeds of unlawful activities or the financing of terrorism; or
- risks that may jeopardise the detection, investigation or prosecution of money laundering and terrorist financing activities; or
- the possibility of the forfeiture of the proceeds of such unlawful activities.

Estate agency enterprises are vulnerable to being abused for money laundering and terrorist financing activities

It is these very threats and vulnerabilities which, on the one hand, place the integrity of South Africa's financial system at risk and, on the other, negatively impact the administration of criminal justice. It has been empirically shown that estate agency enterprises are at a particularly high risk of being abused for money laundering and terrorist financing activities in that estate agency services, by their very nature, lend themselves to being used to facilitate such nefarious activities. Criminals have frequently sought, and will no doubt continue to seek, to use estate agency products and services to exploit estate agency enterprises in promoting money laundering and/or terrorist financing activities.

Bearing this in mind estate agency enterprises must ensure that they have robust money laundering and terrorist financing risk management systems in place. Enterprises must be able convincingly to show that they have internally contextualised the concepts of money laundering and terrorist financing where their operational, line management and strategic objectives are concerned. It is essential, furthermore, that estate agency enterprises ensure that controls have been purposefully built and/or adapted to address all identified money laundering and terrorist financing risks which they are likely to face.

Money laundering and terrorist financing risk management

Money laundering and terrorist financing risk management is a process which includes:

- identifying risks;
- assessing those risks; and
- developing appropriate methods to manage and mitigate the identified risks.

International Organization for Standardization - ISO 31000:2009

The International Organization for Standardization has, in ISO 31000:2009, provided an indication of how risks may be dealt with, or managed, as follows:

- avoid the risk by deciding not to start or to continue with the activity giving rise to the risk;
- accept or even increase the risk to pursue an opportunity;
- remove the source of the risk;
- change the likelihood of the risk;
- change the consequences of the risk;
- share the risk with another party or parties (including contracts and risk financing);
- retain the risk by informed decision.

ISO 31000:2009 applies equally to money laundering and terrorist financing risks. The risk appetite of an estate agency enterprise is a key determining factor in its risk management decisions and, also, the extent to which the enterprise will:

- apply resources to avoid or mitigate risks;
- tolerate certain risks; and
- avoid or terminate risks.

The management and mitigation of money laundering and terrorist financing risks also entails the treatment of those risks that have been identified within the estate agency enterprise itself. The enterprise must, accordingly, develop appropriate systems and controls to manage, or mitigate, such identified risks and which will comprise all relevant risk mitigation measures that may be the disposal of the enterprise in dealing with particular risks.

Possible risk mitigation measures

Risk mitigation measures could, for instance, include:

- the application of client due diligence measures;
- the monitoring of business relationships with clients;
- managing delivery channels for particular products and services; and
- structuring the features of particular products and services.

The process of managing money laundering and terrorist financing risk is a continuous one

The FIC emphasises that the process of managing money laundering and terrorist financing risk must be a continuous one. Estate agency enterprises must constantly seek to satisfy themselves that their money laundering and terrorist financing risk management systems and controls are adequate, especially having regard to possibly changing circumstances in a continuously developing and volatile real estate environment and the emergence of new threats and vulnerabilities, product innovations, target markets and changes in circumstances of individual clients or classes of clients.

Estate agency enterprises must, consequently, ensure that their money laundering and terrorist financing risk management systems and controls are also well known and strictly adhered to within the enterprise itself. Estate agency enterprises are, to this end, required to consistently reassess their money laundering and terrorist financing risks at regular intervals.

Reassessing money laundering and terrorist financing risks

In the process of reassessing money laundering and terrorist financing risks enterprises should, in particular:

- reconsider the residual risks after the implementation of the money laundering and terrorist financing risk management systems and controls; and
- review the continued adequacy of money laundering and terrorist financing management systems and controls on the basis of the performance of such regular re-assessments.

Applying the risk-based approach

By applying a risk-based approach estate agency enterprises can ensure that appropriate measures to prevent, or at the very least mitigate, money laundering and terrorist financing are commensurate with the identified risks and also that available organisational resources are utilised in accordance with established priorities so that the highest risks receive the most attention.

The risk-based approach gives estate agency enterprises the flexibility to:

- use a wider range of mechanisms to establish and verify the identities of clients;
- create opportunities to explore innovative ways of offering estate agency services to a broader range of clients; and
- bring previously excluded sectors of society fully into the formal economy.

If applied correctly, the risk-based approach improves the efficacy of measures for the combatting of money laundering and terrorist financing while simultaneously promoting financial inclusion without in any way undermining the primary anti-money laundering and terrorist financing objectives.

The risk-based approach allows estate agency enterprises to simplify due diligence measures where the risk of money laundering and terrorist financing seems to be lower. Instead of relying on rigidly imposed requirements estate agency enterprises have been afforded a greater discretion in determining appropriate compliance steps for themselves.

Creating processes to identify and assess money laundering and terrorist financing risks

Estate agency enterprises must, in any event, ensure that adequate processes, proportionate to the size and complexity of the enterprise, are in place to identify and assess money laundering and terrorist financing risks.

The range of the risk assessment process

Depending on the size and structure of the enterprise, as well as the nature and variety of products and services that it offers, the risk assessment process could range from the very simple at one end of the spectrum to the highly sophisticated at the other.

The risk assessment processes, however, must take account of a whole gamut of factors that could indicate greater or lesser threats and vulnerabilities to money laundering and terrorist financing. Identified factors indicating an increased threat or vulnerability will tend more readily to lend themselves to criminal abuse.

Estate agency enterprises must, in their own risk assessment processes, also decide on the weight that they will give to the risks that have been identified at the national level.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully identify and describe the sources of information on risk indicators and the processes by which the enterprise will consider those information sources.

Factors that may indicate money laundering and terrorist financing risks

The FIC has identified various factors which may be indicative of money laundering and terrorist financing risks. Such factors should, however, not be regarded as being either exhaustive or prescriptive.

Estate agency enterprises must, in addition to the factors provided by the FIC, take account of any other factors that may be particularly relevant to their own organisations or sector. Estate agency enterprises must be able conclusively to show how the various indicators were brought to bear on given scenarios thereby enabling them to reach valid and appropriate risk classification levels.

Products and services

- To what extent does the product provide anonymity to the client?
- Does the product enable third parties who are not known to the enterprise to make use of it?
- Does the product allow for third party payments?
- Is another estate agency enterprise involved in the usage of the product?
- Can the product be funded with cash or must it be funded only by way of a transfer to or from another financial enterprise?
- How easily and quickly can the funds be converted to cash?
- Does the product facilitate the cross-border transfer of funds?
- Is the offering of the product subject to regulatory approval and/or reporting?
- What does the product enablement processes entail and to what extent does it include additional checks such as credit approvals, disclosure of information, legal agreements, licensing, regulatory approvals, registration, involvement of legal professionals, etc.?
- To what extent is the usage of the product subject to parameters set by the enterprise such as, for instance, value limits, duration limits, transaction limits, etc., or to what extent is the usage of the product subject to penalties when certain conditions are not adhered to?
- Is the usage of the product subject to reporting to regulators and/or to "the market"?
- Does historic transaction monitoring information indicate a lower or higher prevalence of abuse of the product for money laundering or terrorist financing purposes?
- What is the intended target market segment for the product, for example:
  - "entry-level", "retail" or "high net worth individuals";
  - larger corporates, SMEs, etc;
  - specific industries, sectors or professions;
  - salaried versus self-employed individuals;
  - minors?
- Is the usage of the product subject to additional scrutiny from a market abuse or consumer protection perspective?
- What is the time duration for the conversion of funds, property, etc., through the usage of the product?
- Is the product an industry regulated product?
- Does the product allow for the flow of physical cash?
- Are there specific conditions that must be met or events that must happen for clients to have access to funds, property. etc.?
- Does the usage of the product entail structured transactions such as periodic payments at fixed intervals or does it facilitate an unstructured flow of funds?
- What is the transaction volume facilitated by the product?
- Does the product have a "cooling off" period which allows for a contract to be cancelled without much formality and a refund of moneys paid?
- Are the products offered short term or longer-term contractual relationships?
- Do products require a payment from a same name account/facility to facilitate the opening of a product

Delivery channels (or the means by which enterprises and clients interact with each other in the offering of products and services, on-boarding of clients and the usage of the products and services)

- Is the product offered to prospective clients directly or through intermediaries?
- Are prospective clients on-boarded through direct interaction or through intermediaries?
- Do clients transact by engaging with the enterprise directly or through intermediaries?
- Where clients interact through intermediaries, are the intermediaries subject to licencing and/or other regulatory requirements?
- Are products and services acquired or transactions performed through an exchange?
- Are products and services traded in secondary markets?
- To what extent does the usage of the product require the participation of the enterprise or the application of the enterprises' systems and transaction platforms?
- What are the payment systems or other technological platforms that support the functioning of the product?
- Are prospective clients on-boarded through non-face-to-face processes and/or do they use the enterprises products and services through non-face-to-face transactions?

Geographic locations

- Is the client domiciled in South Africa or in another country or does the client operate in another country?
- Do clients who are domiciled outside of South Africa or operate outside South Africa engage with the enterprise in South Africa or through branches, subsidiaries or intermediaries outside South Africa?
- Have credible sources identified geographic locations from where clients engage with an enterprise as high-risk jurisdictions?
- Are the geographic locations from where clients engage with an enterprise subject to sanctions regimes?
- If the client is a corporate vehicle, has it been incorporated in a country which has been identified by credible sources as a high-risk jurisdictions or in a country which is the subject of a sanctions regime, or does it operate in such a country?
- Has an international body, a domestic regulator or supervisory body or other credible source expressed concern with weak regulatory measures against money laundering and terrorist financing, weak transparency requirements for beneficial ownership of corporate structures or weak enterprise frameworks such as supervisory, law enforcement and prosecuting agencies in relation to a geographic location from where clients engage with an enterprise?
- Are the geographic locations from where clients engage with an enterprise known to applying excessive client confidentiality?

Not all clients pose the same money laundering or terrorist financing risk

It is self-evident that not all clients of an estate agency enterprise will necessarily pose exactly the same money laundering or terrorist financing risk. Enterprises must, accordingly, adopt a holistic view of the information gathered concerning clients across all the points of engagement between the enterprises and their clients.

Enterprises should, thus, consider the different engagements with particular clients in relation to the different estate agency products and services that they offer. It may, for instance, sometimes be necessary for the enterprise to conduct a separate risk assessment for each individual client while, on other occasions, whole groups of clients could all fit the same risk profile. If an enterprise is evaluating the characteristics of a group of clients as part of its risk assessment it should take great care to ensure that any individual client to whom the characteristics of the group are ascribed actually does meet the profile of that group.

Some of the factors to be taken into account when engaging with clients

- Is the client a natural person or a corporate vehicle?
- If the client is a corporate vehicle is it part of a complex or multi-layered structure of ownership or control?
- What information does the client provide concerning their source(s) of income?
- What is the nature of the client's enterprise activity, e.g., does the activity involve transacting in large amounts of cash, cross-border movements of funds, trading in sensitive, controlled or sanctioned commodities, etc.?
- What is the nature of the type of the products and services offered by the client?
- Does the client operate solely within the country or have cross-border operations?
- Is the client's product selection rational with a view to support their enterprise or personal needs?
- Does the client occupy a prominent public position or perform a public function at a senior level or does it have such individuals within its ownership and control structure?
- Is there any adverse information about the client available from public or commercial sources?
- Is the client known to be subject to financial sanctions?
- Does the client operate in a sector or industry that is subject to specific standards, market entry or market conduct requirements, other regulatory requirements?
- Is the client supervised for compliance with anti-money laundering and terrorist financing measures?
- Has the client been penalised or subjected to adverse findings relating to failures to implement money laundering and terrorist financing measures?
- Has the client been in an enterprise relationship with the enterprise for a period of time?
- What have been the patterns of transaction behaviour (e.g., speed, frequency, size, volume, etc.) of a client who has a history of an enterprise relationship with an enterprise?
- Has the enterprise previously observed suspicious or unusual activities or transactions on the part of the client?

Various other contextual factors need also to be taken into account regarding particular business relationships or categories of relationships or to assist in determining the risk appetite of an enterprise in relation to particular business relationships or categories of relationships.

Relevant contextual factors

- The demographics of a society, its social and economic circumstances, trade dependencies and Gross Domestic Product.
- Financial inclusion objectives and how particular products and services contribute to this.
- The impact of the enterprise's business strategy on its money laundering and terrorist financing risk profile.
- The money laundering and terrorist financing impact on the enterprise as a result of having operations in particular jurisdictions (i.e., jurisdictional risk associated with the estate agency enterprise itself and not its clients).
- The communication of risk factors by authorities based on their understanding of money laundering and terrorist financing risks at a national or sectoral level.
- Trends and typologies identified by the Financial Action Task Force and other international bodies which indicate jurisdictions, structures, products and services, etc., favoured by money launderers and terrorist financiers.
- Anti-fraud measures that may be in place in an estate agency enterprise.
- The consideration of previous regulatory fines.
- The frequency of internal audit findings and the outcomes thereof.

Undertaking a risk-rating assessment of the money laundering and terrorist financing risk

When undertaking a risk-rating assessment different categories will be assigned to different levels of money laundering and terrorist financing risk according to the risk scale that is used. The risk scale must be tailored to the size and circumstances of the estate agency enterprise. Consideration should also be given in the risk scale to the criteria established by international best practice. The complexity of the risk scale will ultimately reflect the size and complexity of the enterprise as well as its nature and the range of products and services that it offers.

Thus, estate agency enterprises that:

- offer a relatively homogeneous range of products and services;
- use only a limited range of delivery channels;
- operate in one or only a few geographic location(s); or
- engage with a relatively homogeneous range of clients;

will generally require only relatively simplistic risk scales that enable it to distinguish between two or three risk categories.

Enterprises that:

- offer a more diverse and complicated range of products and services;
- use a wider range of delivery channels;
- operate in a larger number of geographic locations; or
- engage with a highly diverse range of clients;

will, however, need to use more finely calibrated risk scales which are able to distinguish between a larger number of identified risk categories.

It is likely, in addition, that the factors underlying any given risk-rating will undergo change over time. Estate agency enterprises must, accordingly, ensure that they continually assess and re-evaluate the relevance of particular risk factors and also investigate the appropriateness of previous risk-ratings.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully document the money laundering and terrorism financing risk-rating methodology and procedures that it will apply, the criteria and the intervals for the re-evaluation of such risk-ratings and the conclusions reached through the implementation of these processes.

The assessment of the money laundering and terrorist financing risk should, ultimately, draw together all factors deemed to be relevant to an engagement with particular clients. A risk matrix, which provides an objective basis for assessing the different risk indicators, might need to comprise different components in evaluating clients, transactions, products or services in their entirety.

Developing a risk management framework

In developing a meaningful risk management framework estate agency enterprises must be mindful of:

- events, products and services, clients and so forth that lead to inherent money laundering and terrorist financing risks;
- internal control activities necessary to mitigate money laundering and terrorist financing risks; and
- residual risks to indicate levels of comfort as to whether or not the enterprise is sufficiently managing the probability and impact of the risk occurring.

Risk mitigation

Risk mitigation, in the context of money laundering and terrorist financing, refers to the activities and methods used by estate agency enterprises to control and minimise identified money laundering and terrorist financing risks. The risk assessment process also assists estate agency enterprises to determine the nature and extent of the resources that will be required to mitigate these risks.

Managing risks

It may be said that a particular risk will have been adequately addressed once the level of residual risk is acceptable to, and within the risk appetite of, the estate agency enterprise. Notwithstanding the implementation of the risk-based approach, estate agency enterprises are still required always to apply effective money laundering and terrorist financing controls.

Enterprises remain fully responsible to ensure that all money laundering and terrorist financing risks are properly and effectively managed. The controls that are implemented by enterprises should, therefore, be sufficient to detect any money laundering and terrorist financing and to respond appropriately thereto, as and when the identified risks materialise.

Identifying higher and lower money laundering and terrorist financing risks

Higher money laundering and terrorist financing risks will necessarily imply the implementation of enhanced measures to mitigate those risks. In such a scenario the range, degree, frequency or intensity of preventive measures and controls will have to be stronger. Where, on the other hand, money laundering and terrorist financing risks are assessed as being lower, more simplified measures may be applied in the sense that the degree, frequency and/or intensity of the controls conducted will be relatively lighter.

Pursuant to enhanced due diligence requirements estate agency enterprises must ensure that implemented systems and controls provide for:

- the obtaining of necessary additional information about clients;
- applying secure confirmation of clients' information; and
- conducting closer scrutiny regarding clients' transaction activities;

in cases where the risk of money laundering and terrorist financing abuse is assessed to be higher.

A simplified due diligence requirement implying systems and controls allowing for less:

- information to be obtained;
- secure confirmation of information to be applied; and
- frequent scrutiny to be conducted;

may well be sufficient in cases where the risk of money laundering and terrorist financing abuse has been assessed to be lower.

Estate agency enterprises must, in any event, always be able to provide valid and acceptable grounds to justify decisions taken in striking the appropriate risk assessment balance in the given circumstances.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully document both the systems and controls it will adopt in managing money laundering and terrorist financing risks and identifying higher or lower money laundering and terrorist financing risks as well as the levels of due diligence that it will apply in respect of the various identified risk levels.

Detection and reporting measures

It may happen that, despite having adopted and implemented all reasonable measures to identify and mitigate money laundering and terrorist financing risks, an estate agency enterprise is still exploited for money laundering or terrorist financing purposes. It is essential, therefore, that each enterprise have sufficient detection and reporting measures in place to address any and all money laundering and terrorist financing risks that may theoretically arise.

Possible detection and reporting measures

- Systems, policies and procedures which are included in the Risk Management and Compliance Programme.
- Awareness training for staff members.
- Reporting channels.
- Client analytics.
- Processes to exit from high risk relationships.
- Approval procedures for higher risk transactions and relationships.
- Adequate supervision for higher risk activities.
- Appropriate screening tools.

Customer due diligence (CDD)

As one of the available measures, the client due diligence process serves a valuable purpose in mitigating the money laundering and terrorist financing risk often associated with either a proposed business relationship or single transactions.

The client due diligence process provides estate agency enterprises with the necessary information so as to ensure that they:

- know who they are doing business with;
- know who benefits from the business done with clients;
- understand the nature of the business done with clients; and
- can determine when the business with clients seems to be suspicious or unusual.

CDD where a higher money laundering and terrorist financing risk has been identified

In cases where a higher money laundering and terrorist financing risk has been identified the following measures could be usefully applied by estate agency enterprises:

- increased automated transaction monitoring;
- increased intensity of client due diligence measures;
- increased review periods of client information;
- utilising more, or higher quality, sources for the vetting of information;
- increased senior management involvement in decisions made to take on clients;
- dedicated specialist staff to manage enhanced due diligence for specifically identified clients;
- limiting reliance on the control measures of other estate agency enterprises.

It is to be emphasised that defining clients and products or services as being high-risk for money laundering and terrorist financing purposes does not in any way reflect negatively on the estate agency enterprise or the clients, products and services of that particular enterprise.

When client relationships must be terminated

The risk assessment process does not envisage or encourage the practice of estate agency enterprises, in an endeavour entirely to avoid money laundering and terrorist financing risks, terminating all client relationships falling within certain sectors. Doing so, in fact, may pose a greater threat to the financial integrity of the enterprise in general as well as to the implementation of the risk-based approach in particular. If, as a result of being overly risk averse, all client relationships were to be terminated there would be a total lack of information regarding the affairs or financial conduct of the affected persons and/or entities. This would actually reduce the possibility of effectively treating money laundering and terrorist financing risks. The blanket refusal of services, or the termination of services, to any class of clients, is likely to create a financial exclusion risk and also give rise to severe reputational risk.

The wholesale termination or restriction of enterprise relationships may be counter-productive

The FIC, counter-intuitively, views such a wholesale termination or restriction of enterprise relationships as an example of inadequate risk management. Estate agency enterprises are encouraged, rather, to:

- take specific account of the level of money laundering and terrorist financing risk for each individual client; and
- implement the appropriate risk mitigation measures that are applicable to that client.

Avoiding the risk by refusing services or terminating or restricting business relationships should only be used a measure of last resort when an estate agency enterprise is forced finally to concede that the money laundering and terrorist financing risks in respect of specific clients cannot be adequately or effectively mitigated.

CDD and knowledge of the client

Client due diligence refers to the knowledge that an estate agency enterprise has of its clients as well as the understanding by the enterprise of the business that the client is conducting with it. Where CDD measures are properly implemented estate agency enterprises are in a better position to manage their relationships with clients and timeously identify possible attempts by clients to exploit the estate agency products and services of enterprises for illicit purposes. The effective application of CDD, thus, constitutes a key element in the combating of money laundering and terrorism financing.

Estate agency enterprises must conduct CDD

The FIC Act has considerably expanded the principle of client identification and verification by imposing an obligation on estate agency enterprises themselves to conduct CDD. Both the application of CDD and the obligation placed on estate agency enterprises to apply a risk-based approach means that an increased discretion has been granted to enterprises to determine the implementation of appropriate anti-money laundering and terrorism financing measures in different circumstances.

Flexibility is now granted to enterprises to choose not only the type of information they will use to establish the identities of clients but also the means by which they will verify the identities of those clients. The mandatory risk assessment process enables estate agency enterprises themselves to decide on the appropriate level, and type, of CDD that is to be applied to clients and/or business relationships and/or single transactions. Estate agency enterprises will also determine when they consider persons to be prospective clients in respect of whom CDD measures must be applied always bearing in mind that the lower the risk is perceived to be the less CDD will be required and vice versa.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must clearly indicate, and fully describe, the CDD measures which the enterprise will apply when establishing and verifying the identity of clients and how these measures may either be weakened or strengthened having regard to identified money laundering and terrorism financing risks.

Enterprise relationship

An enterprise relationship is considered to be:

- an arrangement between a client and an estate agency enterprise;
- for the purpose of concluding transactions;
- on a regular basis.

A time duration element in respect of the engagement by the enterprise with the client is, thus, contained in the definition. Estate agency enterprises must themselves determine what will constitute a business relationship and a transaction within the specialised context of their particular business model.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must clearly indicate the manner and the time when the enterprise will determine that a particular person is a prospective client or a client, both in respect of a business relationship as well as a single transaction.

The single transaction threshold

The FIC Act defines a single transaction as:

- a transaction;
- other than a transaction concluded in the course of a business relationship;
- where the value of the transaction, which value is determined by the Minister of Finance in the regulations from time to time, is presently **not less than R5 000,00**.

A single transaction, thus, is regarded:

- an occasional or 'once-off' enterprise transaction of less than R5 000;
- where there is no expectation, on either side, that engagements will reoccur over a period of time.

Estate agency enterprises must themselves determine what constitutes a single transaction in the context of the conduct of their particular enterprise. Enterprises need not carry out the full scope of CDD measures in respect of clients who conduct a single transaction as defined.

Such a single transaction might, for instance, occur where a consumer simply requests an estate agency enterprise to provide a valuation of a single residential property without that consumer giving, or intending to give, the estate agency enterprise a mandate to market the property for sale.

Anonymous clients and clients acting under false or fictitious names

The single transaction threshold does not affect the obligations prescribed by section 20A. Even where a single transaction is below the threshold of R5 000 an estate agency enterprise may still not deal with an anonymous client or with a client using an apparently false or fictitious name. The enterprise should, in such cases, obtain and record at least some information describing the identity of the client, even if that information is not verified. This would include, for example, the full name and identity number of the client and a contact number. The enterprise should also request sight of the client's identification document and make and retain a copy thereof.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must record the manner in which it will comply with section 20A in dealing with anonymous clients or with clients using apparently false or fictitious names in respect of enterprise relationships and single transactions whether above or below the R5 000 threshold.

Establishing and verifying the identity of clients

Section 21 provides that estate agency enterprises must, when establishing a business relationship or entering into a single transaction, establish and verify the identity of:

- the client; and
- any person representing the client; as well as
- any other person on whose behalf the client is acting, if applicable.

Enterprises, after applying their processes to establish and verify a client's identity, should feel confident that they know, with sufficient certainty, precisely who the client is in the context of the enterprise risk assessment for that client engagement.

In establishing a client's identity the enterprise must obtain a range of information concerning the client. The necessary information will generally be provided by the client in responding to questions posed by the enterprise as an intrinsic part of its client on-boarding process, in the case of a business relationship, or its client engagement process, in the case of a single transaction.

The estate agency enterprise must also corroborate the identity of the person by comparing this information with information contained in source documents or electronic data issued, or created, by reliable and independent third-party sources.

Estate agency enterprises must choose the type of information by means of which they will establish and verify the identity of clients. The nature and extent of these two processes will be determined by taking account of the assessed money laundering and terrorism financing risks associated with the relevant business relationship or single transaction.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully describe how the enterprise will undertake the identification and verification of clients as well as how these measures may be lessened or intensified based on the assessed money laundering and terrorism financing risk of such clients.

Establishing and verifying the identity of natural persons

A natural person's identity can be determined with reference to such basic attributes as the person's:

- full names;
- date of birth; and, in most cases,
- unique identification number issued by a government source (such as a South African identity number, a passport number or the number of a refugee permit, work permit, visitors' visa, etc.)

These basic attributes will generally be used by estate agency enterprises in their processes to establish the identity of natural persons.
This basic information may also be supplemented by other attributes including, for instance, the person's:

- physical appearance or other biometric information;
- place of birth;
- family circumstances;
- place of employment;
- enterprise and/or residential addresses;
- contact particulars such as telephone numbers, e-mail addresses and social media;
- contacts with the authorities in the form of, say, a SARS tax number;
- details held by another estate agency enterprise; and
- any other attributes that an estate agency enterprise wishes to include in its identification processes.

The nature of any other identification attributes required by an estate agency enterprise will largely depend on the extent to which the enterprise relies on the verification of the client's identity to mitigate money laundering and terrorism financing risk. Regardless of the method that is applied, it is important that identity verification be done using original information obtained from a reliable and independent third-party source.

Estate agency enterprises must carefully evaluate the adequacy of the corroboration of a person's identity attributes. They must, thus, determine the level of confidence they have that particular corroboration methods provide certainty and, particularly, accuracy regarding the relevant identity attributes. It is self-evident that information sources which have been created or generated by the client are not to be regarded as being reliable.

Original sources of identity information

Original sources of identity information are always preferable. These sources include government-issued or controlled sources of information such as:

- South African identity documents;
- smart-card identity documents;
- drivers licenses;
- foreign identity documents;
- passports;
- asylum seeker or refugee permits;
- work permits;
- visitors visas; and
- underlying electronic databases where the information evidenced in identity documents is kept.

Original sources of this nature can undoubtedly provide a high level of confidence when corroborating the basic identity attributes of natural persons. Estate agency enterprise should, therefore, endeavour to make exclusive use of government issued or controlled sources to verify the basic identity attributes of clients. Only in exceptional cases should they use information obtained from sources other than original information sources and then only provided the enterprise is confident that, in so doing, it can still adequately manage all money laundering and terrorism financing risks.

The "electronic footprint"

The corroboration of a person's identity attributes may also be done in documentary or electronic format. Many personal identity attributes will accumulate over time and be contained in the person's "electronic footprint". The FIC, as a result, encourages estate agency enterprises to use information in electronic format to corroborate a prospective client's information against multiple third party data sources. It goes without saying that estate agency enterprises using electronic data sources to verify a prospective client's identity remain fully responsible and accountable for compliance with the FIC Act. The use of electronic data sources in the verification process does not grant an automatic indemnity from any regulatory action relating to compliance by the enterprise with these requirements. Estate agency enterprises must, therefore, apply due diligence in choosing electronic solutions to verify the identities of prospective clients.

Using electronic data sources

When using electronic data sources enterprises must apply the same test that as for documentary sources, namely, that:

- the sources are reliable and independent third-party sources; and
- as far as possible, the original source of the relevant information.

Estate agency enterprises must, similarly, determine the level of confidence which they feel justified in placing in particular electronic sources of corroboratory information. Solutions that allow prospective clients in any way to manipulate source information are emphatically not to be regarded as credible information sources for the verification of the particulars of clients.

There would certainly be a greater level of confidence in corroboration from electronic sources if enterprises can use information that has been obtained from multiple sources and across time such as, for instance, records of:

- the Department of Home Affairs;
- the Companies and Intellectual Property Commission;
- the South African Revenue Service;
- eNaTIS; and
- the Master of the High Court.

Establishing the identity of legal persons, trusts and partnerships

Section 21 also applies to clients who are legal persons, including companies, trusts and partnerships. Section 21B requires estate agency enterprises to apply, in addition to the section 21 requirements, a range of further due diligence measures so as to establish:

- the nature of the client's enterprise;
- the ownership and control structure of the client;
- the beneficial ownership of the client; and
- the identity of the beneficial owners of the client.

Legal persons

The FIC defines a legal person as any person, other than a natural person, who establishes a business relationship or enters into a single transaction with an estate agency enterprise including a legal person incorporated as a company, close corporation, foreign company or any other form of corporate arrangement or association but excluding a trust, partnership or sole proprietorship.

Attributes underlying the identity of a legal person

Attributes underlying the identity of a legal person will include:

- the name under which the legal person is incorporated;
- the form of the legal person, that is, whether the legal person is a company or a close corporation;
- the registration number under which the legal person is incorporated, if applicable;
- the address of the registered office of the legal person;
- the powers that regulate and bind the legal person;
- the directors or members of the legal person, as the case may be;
- the senior management of the legal person, such as its chief executive officer and chief financial officer;
- the trading name of the legal person if that name is different from the name under which it was incorporated;
- the enterprise address of the legal person if that address is different from the address of its registered office; and
- the income tax and/or value added tax numbers of the legal person.

The attributes used by an estate agency enterprise to establish the identity of a legal person must be sufficient to prove the existence of that legal person.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must describe the nature and amount of the attributes that it will use in establishing the identity of a legal person. This will depend on the extent to which the enterprise intends relying on the verification of the client's identity as a means to mitigate money laundering and terrorism financing risk in each particular instance.

The verification must always be done using original information that has been obtained from a reliable and independent third-party source. Estate agency enterprises should, therefore, when verifying the identity of individuals, ensure that they use sources of information that have been created, or are controlled, by the public sector enterprises that have already been listed above.

Enterprises must, in addition, establish the nature of the enterprise of the legal person including its ownership and control structure as well as the identity of the beneficial owner of the legal person. Enterprises must implement all reasonable steps to verify the identity of that beneficial owner.

The beneficial owner of a legal person

"Beneficial owner", in respect of a legal person, is defined in the FIC Act as the natural person(s) who, independently or together with another person or persons, own the legal person or exercises effective control over the legal person.

The elimination process to determine the beneficial ownership of a legal person

Section 21B(2) provides for an elimination process to be followed by estate agency enterprises in determining the beneficial ownership of a legal person. The process is as follows:

- Enterprises must determine the identity of the natural person who, either independently or together with another person, has a controlling ownership interest in the legal person. The percentage of shareholding with voting rights in the legal person is often a good indicator of control, since a shareholder holding a significant percentage of the shareholding will, in many instances, be able to exercise control. Ownership of at least 25% of the shares with voting rights in a legal person will usually be sufficient to exercise control over the legal person.
- If the ownership interests either do not indicate a specific beneficial owner or if doubt exists as to whether the person with the controlling ownership interest is in fact the beneficial owner, the enterprise must establish the identity of the natural person exercising control over the legal person by other means. The enterprise might, for example, investigate the persons exercising control by voting rights attaching to different share classes or, perhaps, through shareholders agreements.
- If it is still not possible to identify the natural person who exercises control over the legal person, the enterprise should determine the identity of the natural person who exercises control over the management of the legal person such as investigating the capacity of an executive officer, a non-executive director or an independent non-executive director, director or manager to do so.

After determining the identity of the beneficial owner of a legal person the estate agency enterprise must take all necessary reasonable steps to verify the identity of that person. The enterprise must, again, apply such identification measures as are commensurate with the assessed money laundering and terrorism financing risk. Required information should be obtained by reasonably practical methods with reference to both the accuracy of the required verification and effort level involved in obtaining the verification.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully describe the different measures that it will use in verifying the identity of the beneficial owner of a legal person so as to ensure that it is satisfied that it knows the identity of the beneficial owner of the legal person concerned.

Understanding the concept of beneficial ownership

The Financial Action Task Force (FATF) has developed a useful guidance note that assists in the better understanding the concept of ultimate beneficial ownership. In that note FATF distinguishes between the concepts of legal ownership and control as follows:

- legal ownership means the natural or legal persons who own the legal person; while
- control refers to the ability to take relevant decisions within the legal person and impose those resolutions.

If, for example, a company is a subsidiary of another company, the beneficial owners will be the natural persons behind the holding company. If there is a chain of ownership controlling the holding company, the ultimate holding company in that chain will be regarded as the beneficial owner. Persons who act on behalf of someone else are not considered to be beneficial owners since they are, ultimately, used by someone else to exercise effective control over the company.

The FATF definition of beneficial owner extends beyond legal ownership and control by taking account of the notion of ultimate, or actual, ownership and control. The definition focuses on the natural, and not the legal, persons who actually own and take advantage of the capital or assets of the legal person. The definition identifies the persons who effectively exercise control over the legal person, whether or not they occupy formal positions within that legal person, rather than simply the natural or legal persons who appear, on paper, to be legally entitled to do so.

Partnerships

As partnerships are not incorporated entities they do not have separate legal personality. Estate agency enterprises are, nevertheless, required to establish the identities of any partnerships who are their clients.

The enterprise must determine how the partnership is generally known and whether it is identified by any unique name or description. Reasonable steps must be taken to verify this information and the enterprise must implement measures commensurate with the assessed money laundering and terrorism financing risk of the partnership. The enterprise might, for instance, wish to view:

- the partnership agreement establishing the partnership and governing its membership and functioning;
- business correspondence of the partnership;
- promotional material advertising the business of the partnership, etc.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully describe the measures that the enterprise will use in verifying the identity of partnerships who are its clients.

Establishing the identity of the partners in a partnership

All the partners in a partnership are the beneficial owner of that partnership. Section 21B(3), thus, requires estate agency enterprises, in addition to fulfilling the requirements of sections 21 and 21A, to establish the identity of every partner in a partnership including, specifically, members of:

- partnerships *en commandite* (where the liability of certain partners, who contribute a fixed amount but remain undisclosed as partners, is limited according to the partnership agreement establishing and governing the partnership);
- anonymous partnerships (where the names of the partners are not disclosed to non-partners); or
- any similar partnership.

The express reference by the FIC Act to these latter types of partnership clearly indicates the intention that estate agency enterprises must establish the identity of every person who either contributes to a partnership or may benefit from a partnership when the enterprise does business with such a partnership. Probably the most reliable source document for indicating the details of the various partners is the partnership agreement concluded between them since this agreement establishes the partnership and governs its membership and functioning.

Section 21B(3), in addition, requires estate agency enterprises to establish the identity of the partner, if any, who exercises executive control over the partnership. Enterprises should, thus, determine the notion of 'control over', as opposed to 'benefit from', in a partnership. They need, furthermore, to establish the identity of each natural person who is authorised to enter into a single transaction or establish a business relationship with the enterprise on behalf of the partnership. Estate agency enterprises must take reasonable steps to verify the names of such natural persons in light of the assessed money laundering and terrorism financing risk in each individual case so that the enterprise is satisfied that it knows the identities of the relevant natural persons.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully describe the different verification measures that it will implement in establishing the identity of each individual partner of a partnership.

Trusts

Since trusts, like partnerships, are not incorporated entities, they have no legal personality. A trust may be a trust *inter vivos* or created during the lifetime of a person or a trust *mortis causa* or created by the will of a person and which comes into effect after the death of the founder of the trust. The administration of trusts is regulated by the Trust Property Control Act of 1988.

The FIC Act defines a 'trust' as any trust contemplated in the Trust Property Control Act excluding, however, trusts established:

- by virtue of a testamentary disposition (*mortis causa*);
- by virtue of a court order;
- in respect of persons under curatorship; or
- by the trustees of a retirement fund in respect of benefits payable to the beneficiaries of that retirement fund.

Section 21B(4) deals with the identification and verification requirements for *inter vivos* trusts. It should be noted that until the trust has been registered by the Master of the High Court it can have no legal effect. The trustee(s), similarly, must obtain the authority of the Master of the High Court to perform their functions. Estate agency enterprises must, therefore, establish the unique identifying trust reference number from the Master's Office where the trust was registered. If the enterprise is dealing with a foreign trust it should obtain a letter of authority, or other official document, from the competent trust registering authority of that foreign jurisdiction.

As always the enterprise must implement reasonable steps to verify the information commensurate with the assessed money laundering and terrorism financing risk in each individual case. Of particular importance would be the trust deed which establishes the trust and governs its functioning together with the information controlled, and documentation issued, by the relevant office of the Master of the High Court.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully describe the measures that it will use to verify the identity of a trust and establish the information required by section 21B of the FIC Act.

The beneficial owner of a trust means all the natural persons who may benefit from the trust arrangement or who may control decisions relating to the management of the trust property or who are otherwise associated with the trust.

Section 21B(4) requirements

Section 21B(4) requires estate agency enterprises, over and above the requirements of sections 21 and 21A, to establish:

- the identity of the founder(s) of the trust;
- the identity of each trustee and each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the enterprise on behalf of the trust, and
- the identity of each beneficiary referred to by name in the trust deed or other founding instrument in terms of which the trust is created; or
- if the beneficiaries are not referred to by name in the trust deed or other founding instrument in terms of which the trust is created full particulars of how the beneficiaries of the trust are to be determined.

The Protection of Personal Information Act of 2013 and its impact on the identification and verification requirements of the FIC Act

The processing by estate agency enterprises of the personal information of clients for purposes of compliance with the requirements of the FIC Act must be done within the boundaries of the Protection of Personal Information Act (POPI Act).

While the POPI Act does provide for the processing of the personal information of a client for purposes of FIC Act compliance, enterprises should nonetheless exercise caution when verifying the identity of clients by using third party data sources since such data sources may entail the obtaining of personal information about a client without the knowledge or consent of that client as the POPI Act requires.

The timing of the verification

As has been noted, a client's identity and, where applicable, the identity of the beneficial owners and other persons associated with a client, must be verified in the course of the enterprise conducting a single transaction or entering into a business relationship with the client.

An estate agency enterprise may, thus, initiate the processes for the conclusion of a single transaction or for entering into a business relationship while still verifying the identity of the relevant persons. The enterprise must, however, ensure that the verification process is duly finalised prior to concluding a transaction in the course of the resultant business relationship or performing any act designed to give effect to a resulting single transaction.

Enterprises may, for instance, accept a mandate from a prospective client to:

- establish a business relationship; or
- conclude a single transaction; or
- take any similar preparatory steps with a view to establishing a business relationship or concluding a single transaction;

prior to completing the verification of the identity of the prospective client and any other relevant persons. The estate agency enterprise must, however, be careful, in so doing, not to incur any unmitigated money laundering and terrorism financing risks such as where the enterprise receives funds from a client before completing the verification and which funds may have to be returned or, alternatively, the enterprise makes funds available to a client before the verification process is completed.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully describe the manner and procedures that it will use to identify clients and verify their identities and also provide details of the timing of the verification process as well as of the mitigation of money laundering and terrorism financing risks where a single transaction is conducted or a business relationship is established before completion of the verification.

Obtaining and understanding information on the proposed business relationship

Section 21A requires estate agency enterprises to ascertain from the prospective clients both the nature and intended purpose of a business relationship as well as the source of the funds that the prospective client will use in the course of the business relationship. The purpose of this provision is to ensure that the enterprise clearly understands the nature of the client and of the envisaged business relationship that will be entered into between the client and the enterprise.

Compliance with section 21A ensures that an estate agency enterprise can form a well-founded view concerning the expected frequency and the nature of transactions to be conducted in the normal course of the resulting business relationship. This understanding contributes to a better appreciation by the enterprise of the money laundering and terrorism financing risk associated with that particular business relationship.

In most instances both the purpose and intended nature of the business relationship will probably be self-evident having regard to the nature of the products or services that the client requires from the estate agency enterprise.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must record the manner and type of the section 21A information that it requires including the nature and details of the enterprise/occupation/employment of the client, the expected source and origin of the funds that are to be used in the business relationship and the anticipated level and nature of the activity to be undertaken in the course of the business relationship.

The information obtained by the enterprise from a prospective client must be sufficient to enable the enterprise to form a clear understanding of both the client and the intended business relationship. The enterprise may accept any information that it obtains at face value as section 21A does not require the enterprise further to verify the veracity of that information.

Performing an ongoing due diligence

Section 21C provides for the initiation of ongoing due diligence measures flowing from the obligation of an enterprise to understand the purpose, and intended nature, of a proposed business relationship.

Additional section 21C measures

Such additional due diligence measures might include:

- scrutinising all transactions undertaken throughout the course of a relationship;
- ensuring that the transactions being conducted in the course of a business relationship are consistent with the estate agency enterprise's knowledge of the client and the client's business and risk profile including, where necessary, the source of any funds used; and
- ensuring that the information which an estate agency enterprise has about a client always remains accurate and relevant.

The conduct of an ongoing due diligence helps to identify the activities of clients during the course of the business relationship, especially if there is a suspicion that these activities are not consistent with the estate agency enterprise's knowledge of the client or with the purpose and intended nature of the business relationship.

These activities must also be assessed arising out of the possibility that the enterprise may subsequently have grounds to report a suspicion of a money laundering or terrorist financing to the FIC. Estate agency enterprises should pay particular attention to complex or unusually large transactions as well as to transactions that exhibit unusual patterns or which appear to have no apparent business or lawful purpose.

The intensity and frequency of any ongoing due diligence measures concerning an established business relationship will be determined by the understanding that the estate agency enterprise has of the money laundering and terrorism financing risks associated with that business relationship.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must include a full description of how it will initiate and conduct the ongoing due diligence in terms of section 21C; the processes in place for the monitoring of enterprise relationships; the manner in which it proposes examining complex or unusually large transactions and unusual patterns of transactions having no apparent business or lawful purpose; and how it will keep written findings of those transactions.

Doubts concerning the veracity of previously obtained information

Section 21D provides for the measures that estate agency enterprises must take if, during the course of the relationship or where a subsequent suspicion of money laundering or terrorism financing has arisen, they become doubtful of the veracity, or adequacy, of the client due diligence information previously obtained.

Enterprises must, in such event, repeat the section 21 and 21B verification processes in accordance with the enterprise Risk Management and Compliance Programme and, to the extent deemed necessary, re-verify that information.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must, as required by section 21D, clearly indicate the manner in which, and the processes by which, the enterprise will confirm client information when doubts subsequently arise concerning the veracity of previously obtained information regarding that client.

Inability to conduct a client due diligence

Section 21E prohibits estate agency enterprises from entering into, or maintaining, business relationships or from concluding single transactions if they are unable to perform the necessary CDD.

In considering the matter an objective approach must be adopted since there may be valid circumstances that make it reasonable for the enterprise to delay the discontinuation of a business relationship while actively assisting the client to remedy the failure. The reasonableness or otherwise of such a delay depends on the circumstances of each individual case.

If a client refuses to provide any requested documentation or information, the enterprise must advise that client of the potential implications of such failure and give the client adequate time within which to respond. If the client still fails to comply with the request the business relationship must immediately be discontinued.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must, as required by section 21E, indicate the sequence of attempts to be made to obtain the required CDD information or to apply other CDD measures; the stage in the process when it will conclude that it is not able to conduct an appropriate CDD of the client; and the manner in which it will terminate an existing enterprise relationship when it is unable to complete necessary CDD requirements.

Foreign prominent public officials and domestic prominent influential persons

Sections 21F, 21G and 21H deal with the position of persons occupying prominent positions in the public and private sectors. Estate agency enterprises must establish effective measures to enable them to both know and understand the business of such clients.

Business relationships with domestic prominent influential persons are not inherently high-risk

Since business relationships with domestic prominent influential persons are not regarded as being inherently high-risk, enterprises must consider each such relationship on its own particular merits when determining whether there is any valid reason to conclude that there will be a higher risk of money laundering and terrorist financing abuse. If the enterprise concludes that there will be a higher risk it must apply the same requirements as those prescribed for foreign prominent public officials, as indicated below.

Business relationships with foreign prominent public officials are presumed to be high-risk

In contradistinction to the situation with domestic prominent influential persons, business relationships with foreign prominent public officials are always presumed to be high-risk. Where estate agency enterprises deal with foreign prominent public officials, or their immediate family members and the known close associates of such prominent public officials, senior management approval must always be initially obtained when establishing the business relationship.

Enterprises must take all reasonable measures to establish, although not necessarily to verify, the source of wealth and of the funds of the client and must conduct an enhanced and ongoing monitoring of the business relationship. All information thus obtained must be included in the client profile that will be used as the basis for the mandatory enhanced and ongoing monitoring.

The appropriate level of senior management approval that is necessary is determined both by the size, structure and nature of the enterprise as well as the level of increased risk associated with the business relationship. A senior manager who approves a business relationship with a prominent public official must have sufficient seniority and oversight within the enterprise to take informed decisions on issues that directly impact its risk profile.

Senior management must base the decision on whether to approve a business relationship with a prominent person based on the level of money laundering or terrorist financing risk the enterprise might be exposed to if it were to enter into that business relationship and how well equipped the enterprise is effectively to manage that risk.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must clearly indicate and describe who within the enterprise has the responsibility and authority to take final decisions on entering into business relationships with prominent persons and how the reasons for any decision to approve or refuse to enter into such business relationships are to be fully documented in writing.

When determining the source of wealth estate agency enterprises should consider:

- the funds and property generating the total net worth of the client; and
- the origin and the means of transfer of funds involved in the transaction such as, for example, occupation, enterprise activities, proceeds of sale, corporate dividends, etc.

Schedule 3A lists the positions of domestic prominent influential persons.

Domestic prominent influential persons in terms of Schedule 3A

The Schedule 3A list includes:

- the President or Deputy President;
- a government minister or deputy minister;
- the Premier of a province;
- a member of the Executive Council of a province;
- an executive mayor of a municipality;
- a leader of a political party, namely, the person identified by the party to occupy the position of the highest level of authority in the party;
- a member of the royal family or senior traditional leader;
- the head, accounting officer or chief financial officer of a national or provincial department of government;
- the municipal manager of a municipality;
- the chairperson of the controlling body, the chief executive officer or a natural person who is the accounting authority, the chief financial officer or the chief investment officer of a public entity listed in Schedule 2 or 3 of the Public Finance Management Act;

- the chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of a municipal entity;
- a constitutional court judge or any other judge;
- an ambassador or high commissioner or other senior representative of a foreign government based in South Africa;
- an officer of the South African National Defence Force above the rank of major-general;
- the chairperson of the board of directors, chairperson of the audit committee, chief executive officer or chief financial officer of a company which provides goods or services to an organ of state;
- the head, or other executive directly accountable to that head, of an international organisation based in South Africa.

Foreign prominent public officials include:

- the Head of State or head of a country or government;
- member of a foreign royal family;
- government minister or equivalent senior politician or leader of a political party;
- senior judicial officials;
- senior executives of state owned corporations; or
- high-ranking members of the military.

The client is the most valuable source of information in determining whether that person occupies a prominent position. If there is either a need to conduct a more thorough check or there seems to be a likelihood that an enterprise will have prominent persons as clients, estate agency enterprises can augment the information obtained from the client by utilising commercially available information sources providing information on prominent and politically exposed persons.

The use of commercially available information sources to establish whether a person occupies a prominent position will not, however, grant automatic indemnity from regulatory action relating to FIC Act compliance obligations by the enterprise. It remains fully the responsibility of the enterprise to ensure that any commercial databases used to identify persons in prominent positions are sufficiently comprehensive to detect such persons and are functionally usable for that purpose.

Dealing with a family member or known close associate of prominent persons

Estate agency enterprises must also determine whether they are dealing with a family member or known close associate of a prominent person regardless of whether or not the prominent person is a client of the enterprise. There is generally less information available to enterprises concerning family members and known close associates of prominent persons. This makes the determination of whether a client, or prospective client, falls within these categories more challenging for the enterprise. Enterprises should refer to what is publicly known of a prominent person's sphere of influence to determine if a client is a family member or known close associate of a prominent person.

Determining family members or known close associates of prominent persons

Enterprises can also:

- make use of commercially available sources of information outlining associations of prominent persons;
- monitor the media;
- use credible third-party sources of information and information that is available from other enterprises within the same group which are doing enterprise in other countries; and
- apply existing processes in place for the ongoing monitoring of business relationships.

It may happen that an existing client was not a prominent person, or immediate family member or known close associate of a prominent person, at the commencement of the business relationship but subsequently fits into one of these categories. An estate agency enterprise may also later become aware that a client is a family member or close associate of a prominent person after that person became a client of the enterprise. This may emerge, for instance, when the enterprise conducts its on-going due diligence of existing clients. Enterprises should, therefore, continually be alert to public information in respect of any possible status changes of clients.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must indicate how the enterprise will determine whether a prospective client is a foreign prominent public official or a domestic prominent influential person, including the sources of information that it will use in this regard; and how the money laundering and terrorist financing risks associated with enterprise relationships with officials and persons will be assessed and mitigated, including the processes that will be implemented for existing clients where the status of the client as a prominent person has changed after the commencement of the relationship with the client or where the enterprise was not previously aware of the client's status as a family member or close associate of a prominent person.

Record-keeping

Record-keeping is an essential component of any successful system to combat money laundering and terrorist financing. The records of the identity of clients, and their transaction activities, will sometimes be the only available evidentiary trail to assist law enforcement authorities in the detection, investigation and prosecution of illicit flows of funds and the subsequent confiscation of those criminal funds.

Record-keeping and CDD measures are the joint elements that bring greater transparency to the financial system. It is for this reason that the FIC Act requires estate agency enterprises to retain full records concerning their client identification and transaction activities.

Compliance with record-keeping requirements ensures that adequate information is captured by estate agency enterprises to reconstruct a trail of transactions and assist investigators to determine the flows of funds. Enterprises must fully understand their reporting obligations under the FIC Act when they determine the internal processes and systems that are required for record-keeping purposes. They must ensure that all relevant information is readily available and that reporting under the FIC Act is neither unduly delayed nor impeded due to a lack of available information.

The record-keeping requirement does not depend on risk levels but is applicable to the CDD, business transactions and other information collected, whatever the range of this information may be, by the enterprise.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must reflect all elements of the enterprise record management processes necessary to give effect to the requirements of the FIC Act.

Retaining client due diligence records

Section 22 requires estate agency enterprises to keep client due diligence records. Enterprises must, consequently, keep records of all the information pertaining to a client that was obtained for compliance with sections 21 to 21H, including a copy of, or references to, information provided to, or obtained by, the enterprise to verify the identity of the client.

Keeping transaction records

In terms of section 22A estate agency enterprises must keep transaction records of both single transactions and transactions concluded in the course of the business relationship with a client. Enterprises must, thus, keep records of every transaction it has with its clients. The transaction records must be sufficient detailed to enable the transaction to be reconstructed.

Transaction records

The necessary transaction records will include such information as the:

- amount of the transaction;
- currency of the transaction;
- date of the transaction;
- parties to the transaction;
- nature of the transaction;
- pertinent or relevant enterprise correspondence; and
- identifying particulars of all accounts and account files in respect of the transaction if the enterprise provided account facilities.

How records must be kept

Since the FIC Act does not prescribe the manner in which records must be kept they may be stored in accordance with an estate agency enterprise's established record management system including maintaining and storing the original documents, making and keeping a photocopy of original documents, scanning the original documents or storing the original documents in a computerised or electronic format.

Electronic format mechanisms useful for the storage of records include:

- internal networks;
- physical storage devices such as hard drives, CDs, DVDs, memory sticks, etc.:
- cloud storage;
- electronic document repositories; and
- fintech capabilities.

Implementing an appropriate record management system

In implementing an appropriate record management system estate agency enterprises must ensure that:

- they have unencumbered access to the relevant records;
- the records are readily available to the FIC and the Estate Agency Affairs Board, as the supervisory body, when required;
- the records can be reproduced in a legible format; and
- the FIC and the EAAB are provided with the details of the third party who is storing the records if they are stored off-site.

The records should include sufficient detail to facilitate their easy identification including, for instance, reference numbers on documents or letters, details of relevant dates, such as date of issue or expiry, and details of the issuer or writer of the record. Estate agency enterprises must ensure that records are stored in a safe, secure and tamper-proof environment and that safeguards are created to prevent any unauthorised access to original records and/or to electronically stored information.

Estate agency enterprises operating in groups of companies may implement group-wide record-keeping policies including the centralised storage of records bearing in mind that the same record-keeping principles will still be applicable.

Estate agency enterprises utilising the services of commercial third parties or intra-group centralised data for the storage of records must conduct regular assessments of such service providers to test their controls and business processes so as to be able to assure the FIC and the EAAB that they have easy access to and can and speedily retrieve any required data and/or documents.

The period for which records must be kept

- Section 22 records in respect of the establishment of a business relationship must be kept for a period of at least five years calculated from the date when the business relationship was terminated.

- Section 22A records of transactions concluded must be kept for at least five years as from the date on which the transaction in question was concluded.

- Records of a transaction or activity giving to a section 29 report must be kept for at least five years as from the date on which the section 29 report was submitted to the FIC.

- Estate agency enterprises must keep records which, to their knowledge, relate to ongoing investigations until such time as the relevant law enforcement agency has confirmed in writing that the matter has been finalised.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must fully detail the record management system it uses in compliance with the requirements of the FIC Act.

The Risk Management and Compliance Programme (RMCP)

Section 42 obliges estate agency enterprises to:

- develop;
- document;
- maintain; and
- implement;

a Risk Management and Compliance Programme.

The ability effectively to apply a risk-based anti-money laundering and terrorist financing approach largely depends on the quality of the Risk Management and Compliance Programme. The RMCP must sufficiently address, and counter, the money laundering and terrorist financing risks faced by the enterprise.

It must be borne in mind that a Risk Management and Compliance Programme comprises not only policy documents but also the procedures, systems and controls to be implemented by and within the enterprise. The Risk Management and Compliance Programme is, essentially, the foundation of all efforts by estate agency enterprises to comply with the FIC Act on a risk-sensitive basis.

Assisting the enterprise to comply with the Risk Management and Compliance Programme

In terms of section 42A the board of directors of an estate agency enterprise, which is a legal person having a board of directors, or the senior management of such an enterprise that does not have a board of directors, is required to ensure compliance by the enterprise, its management and staff, with the provisions of the FIC Act as well as the enterprise Risk Management and Compliance Programme.

An estate agency enterprise that is a legal person is required to:

- have a compliance function that assists either the board or senior management, as the case may be, in ensuring that the enterprise fully complies with the provisions of the FIC Act and the enterprise Risk Management and Compliance Programme; and
- assign a person having sufficient competence and seniority to ensure the effectiveness of the enterprise compliance function.

If the estate agency enterprise is a partnership it must appoint a person, or persons, with sufficient competence to assist the enterprise in complying with the provisions of the FIC Act and its Risk Management and Compliance Programme. In the case of an enterprise that is a sole proprietorship, the sole proprietor will assume responsibility for ensuring compliance with the FIC Act and the Risk Management and Compliance Programme.

Responsibility for compliance with the Risk Management and Compliance Programme

The board of directors, senior management or the person with the highest level of authority within the enterprise bears the ultimate responsibility of ensuring that it maintains an effective internal anti-money laundering and counter-terrorist financing structure through the application of an appropriate Risk Management and Compliance Programme. The board of directors and/or senior management should, therefore, not only insist on but also create a corporate culture of strict compliance within the enterprise.

The policies, procedures and processes of the enterprise must be:

- designed to limit and control the risks of money laundering and terrorist financing;
- fully consistent with the law; and
- fully adhered to by all enterprise management and staff.

The board of directors and/or senior management should not only be fully engaged in the necessary decision-making processes but also take full ownership of the risk-based measures adopted by the enterprise as it is they who will be held accountable if the Risk Management and Compliance Programme, or its application by the enterprise, is either inadequate or not fit for purpose.

Requirements of the Risk Management and Compliance Programme

The Risk Management and Compliance Programme must:

- describe the accountability of the board of directors or senior management;
- appoint a person with adequate seniority and experience to ensure compliance with the FIC Act;
- indicate how the function of managing the establishment and maintenance of effective anti-money laundering and counter-terrorist financing systems and controls will be discharged within the enterprise.

The Risk Management and Compliance Programme must also cover, among others, the:

- appropriate training on money laundering and terrorist financing so that management and employees are aware of, and understand, their legal and regulatory responsibilities and their role in handling criminal property and money laundering/terrorist financing risk management;
- appropriate provision of regular and timely information to the board of directors or senior management relevant to the management of the money laundering and terrorist financing risks of the enterprise;
- appropriate documentation in respect of risk management policies and the risk profile of the enterprise in relation to money laundering and terrorist financing including documentation concerning the application by the enterprise of those policies;
- appropriate descriptions of the decision-making processes to apply the different categories of CDD and other risk management measures including the escalation of decision-making to higher levels of seniority in the enterprise, where necessary; and
- appropriate measures to ensure that money laundering risks are taken into account in the day-to-day operation of the enterprise, including in relation to the development of new products, the taking-on of new clients and changes in the enterprise profile of the enterprise.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must clearly indicate the processes adopted and implemented by the enterprise to ensure full compliance with the requirements of the FIC Act in respect of the maintenance and implementation of such Risk Management and Compliance Programme.

The Risk Management and Compliance Programme must be commensurate with the size, complexity and the nature of the enterprise

The Risk Management and Compliance Programme of an enterprise must be commensurate with its size and complexity and the nature of the enterprise. A suitable Risk Management and Compliance Programme for an enterprise that does not offer a very wide range of products or services or does not deal with a diverse range of clients might, for instance, be relatively simple in contrast to that of a more complex enterprise. The Risk Management and Compliance Programme of an enterprise must indicate if any of the elements described in section 42 are not applicable to that enterprise and, if so, provide reasons why such processes are not applicable.

Factors impacting the nature and extent of internal systems and controls

The nature and extent of the internal systems and controls of an estate agency enterprise which form part of its Risk Management and Compliance Programme will depend on many factors including:

- the nature, scale and complexity of the business of the enterprise;
- the diversity of enterprise operations including geographical diversity;
- the client, product or services profile of the enterprise;
- the distribution channels used by the enterprise;
- the volume and size of enterprise transactions; and
- the degree of risk associated with each area of enterprise operations.

Estate agency enterprises operating in groups of companies may implement group-wide Risk Management and Compliance Programmes while taking care to ensure that the various elements of group-wide Risk Management and Compliance Programmes, including internal processes, systems and controls, are appropriate for the various different entities comprising the group and, where necessary, are adequately tailored in this respect.

Communication and review of the Risk Management and Compliance Programme

It is essential that the content and purpose of the Risk Management and Compliance Programme of an enterprise be widely communicated throughout the enterprise to increase the effectiveness of the implementation of the RMCP. Estate agency enterprises must also review their Risk Management and Compliance Programmes at regular intervals to ensure that they remain relevant to the operations and identified risks of the enterprise.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must clearly indicate how the enterprise will communicate the programme to management and staff.

The risk officer appointed by the enterprise is tasked with ensuring that management and staff are fully aware of all relevant FIC Act compliance functions. The enterprise RMCP must, accordingly, be freely accessible to all enterprise staff members so that they are aware of its contents, requirements, policies and procedures and appropriate training must be regularly provided.

Training relating to anti-money laundering and counter-terrorist financing compliance

Section 43 of the FIC Act mandates estate agency enterprises to provide ongoing training to all employees to enable such employees to comply with the provisions of the FIC Act and the Risk Management and Compliance Programme applicable to such employees.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must clearly indicate how the enterprise intends providing ongoing training to its employees to enable them to comply with the provisions of the FIC Act.

Implementation of the United Nations Security Council Resolutions on the freezing of assets

The FIC is responsible for administering targeted financial sanctions (TFS) measures adopted by the United Nations Security Council (UNSC). FATF recommendation 7, in fact, requires member countries to implement the targeted financial sanctions proposed by the UNSC for the combating the financing of the proliferation of weapons of mass destruction.
Targeted financial sanctions generally restrict the sanctioned persons and entities from access to funds and property under their control and from receiving financial services relating to such funds and property. The FIC Act requires estate agency enterprises to freeze property and transactions pursuant to any financial sanctions imposed in UNSC resolutions.

The Minister of Finance may publish a notice of the adoption of the UNSC Resolution in the Government Gazette while the Director of the FIC may likewise publish a sanctions list notice indicating the persons who are subject to the sanction measures. The notices remain in effect indefinitely unless they are revoked when longer necessary to give effect to the applicable UNSC resolutions. The notices by the Minister and the Director are public statements so that estate agency enterprises who have clients or prospective clients listed in the notices are thereby notified of the relevant sanctions. Enterprises which have sanctioned persons or entities as clients should draw the attention of the persons or entities concerned to the relevant sanctions notice.

The acquisition, collection or use of the property of persons or entities whose names appear in the sanctions list is prohibited. No financial services and/or products may be provided to those persons or entities. Estate agency enterprises may not transact with sanctioned persons or entities or process transactions for such persons or entities. The status quo, as it existed when the sanction in relation to the property or funds of the sanctioned persons or entities was imposed, must be maintained so that financial services may not be provided to the persons or entities concerned.

Estate agency enterprises must report the property in the possession or under the control of the enterprise which is owned or controlled by or on behalf of persons or entities identified in the sanctions list to the FIC. Estate agency enterprises that may come into contact with sanctioned persons or entities must screen those clients and prospective clients against the relevant sanctions lists at the time of the client-take-on process and subsequently as and when the UNSC adopts new targeted financial sanctions measures or expands existing ones.

Estate agency enterprises must, therefore, determine whether their client base or intended target market is likely to include sanctioned persons or entities. Doing so assists enterprises to determine the level of effort and resources required to ascertain whether any sanctioned persons or entities are clients or prospective clients of the enterprise.

Enterprises having enterprise relationships with foreign persons and entities are likely to be more vulnerable to dealing with sanctioned persons and entities than those that do not. Section 49A makes any failure to comply with targeted financial sanctions obligations by an enterprise a criminal offence. An averment by the enterprise that it relied on a commercially available screening capability or that it considered the risk of being exposed to targeted financial sanctions-related obligations as low is not an acceptable defence in response to any criminal charge.

Obtaining an updated sanctions list

The FIC maintains an updated sanctions list, which may be accessed from its website, reflecting the available identity particulars of persons and entities contained in the notices published by the Minister and the Director.

Reporting suspicious or unusual transactions to the FIC

Section 4 of the Prevention of Organised Crime Act, 21 of 1998, has criminalised money laundering, that is to say, the performance of any act regarding property that may result in the concealment or in disguising the nature and/or source of the proceeds of crime. South African law, in addition, provides for various additional control measures to facilitate the detection and investigation of money laundering. This specifically includes the FIC Act which is based on the following underlying principles, namely, that:

- intermediaries in the financial system must know with whom they are doing enterprise;
- the audit trail of transactions through the financial system must be preserved; and
- possible money laundering transactions must be brought to the attention of the FIC and the investigating authorities.

The FIC, as established by the FIC Act, is the government agency that collects, analyses and interprets information disclosed to, and obtained by, it to advance the fight against money laundering and terrorist financing. Section 29 provides that all suspicious or unusual activities and transactions must be reported to the FIC in the prescribed form.

Estate agency enterprises, as accountable institutions, are required to cooperate with the FIC in preventing money laundering and terrorist financing activities. Such reporting, in fact, is an essential element in the fight against money laundering and the combating of terrorist financing.

FATF guideline

The Financial Action Task Force has provided the following guidance in respect of the reporting of suspicious transactions:

"If a financial enterprise suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)".

The FIC Act imposes an obligation to report suspicious and unusual transactions and activities on any person who:

- carries on a business;
- is in charge of a business;
- manages a business; or
- is employed by a business.

As the term "business" is not defined in the FIC Act, its ordinary meaning, within the context of the FIC Act, is adopted, namely, that a business is any commercial activity or business excluding a charitable undertaking or a public sector enterprise. Any person who is associated with a commercial undertaking, whether as owner, manager or employee of that undertaking, is therefore obliged to report suspicious or unusual transactions and activities to the FIC.

Reporting suspicious and unusual transactions and activities

This reporting obligation arises when a person either knows of certain facts or ought reasonably to have known, or suspected, the existence of such facts.

An owner, manager or employee of a business undertaking will report to the FIC if that person:

- becomes aware of something; or
- circumstances arise in which that person can reasonably be expected to be aware of something; or
- circumstances arise in which that person can reasonably be expected to suspect something.

According to section 29(1) the "something" referred to could relate to:

- situations concerning the business itself; or
- situations concerning transactions to which the business is a party; or
- situations concerning an activity which does not involve a transaction between two or more parties; or
- the proceeds of an unlawful activity or activities; or
- an offence relating to the financing of terrorist and related activities; or
- the structuring of a transaction and/or activity which is so conducted as to avoid creating a reporting duty under the FIC Act.

Proceeds of unlawful activity

The concepts of "proceeds of unlawful activity" and "unlawful activity" are, for purposes of the FIC Act, defined with reference to the Prevention of Organised Crime Act. Thus the "proceeds of unlawful activity" means:

- any property or any service, advantage, benefit or reward;
- which was derived, received or retained, directly or indirectly, in South Africa or elsewhere;
- at any time before, or after, the commencement of the Prevention of Organised Crime Act;
- in connection with, or as a result of, any unlawful activity carried on by any person.

*"*Unlawful activity*"* means any conduct that constitutes a crime, or which contravenes any law, whether that conduct occurred in South Africa or elsewhere.

Section 29 refers to the making of reports in connection with suspicions concerning the proceeds of unlawful activities and money laundering or terror financing offences, as opposed to criminal activity in general. The FIC Act does not require that reports be made concerning suspected crimes or unlawful conduct by persons which are not money laundering or terrorist financing activities.

Say, for instance, a fraudulent cheque was presented to a bank for payment. This would constitute the crime of fraud and, while the matter would be reported to the criminal authorities, it would not be reported to the FIC. If the fraudulent cheque was actually paid by the bank then the moneys received become the proceeds of fraud. Any subsequent transactions involving those funds are transactions relating to the proceeds of unlawful activities and, possibly, money laundering transactions. Now a suspicious transaction report to the FIC is required.

Suspicion of unlawful or money laundering activities

The reporting requirement applies if there is a mere suspicion of unlawful activities or money laundering. As the concept of 'suspicion' is not defined in the FIC Act the ordinary meaning of the term must be applied. Suspicion is largely subjective in nature involving the perception, or belief, that something is wrong, even if this perception is not empirically proved. Suspicion might also include the view that something seems to be possibly, or probably, wrong without any valid proof that this is so. The concept of suspicion can, therefore, best be summarised as "I suspect but cannot prove".

Suspicion arises when the circumstances of a matter raise questions or cause a feeling of discomfort, apprehension or mistrust. While suspicion is subjective, section 29(1) of the FIC Act does create an element of objectivity in stating that the enterprise concerned "ought reasonably to have known or suspected" the existence of an unlawful state of affairs.

Ought reasonably to have known or suspected

Section 1(3) of the Prevention of Organised Crime Act elaborates the concept of "ought reasonably to have known or suspected" by providing that a person ought reasonably to have known, or suspected, a fact if:

- a reasonably diligent and vigilant person;
- with the same knowledge, skill, training and experience;
- as well as the knowledge, skill, training and experience that may reasonably be expected of a person in the same position;
- would have known or suspected that fact.

When considering whether a particular situation is suspicious all known circumstances relating to that situation must be assessed in the context of the usual enterprise practices and systems of the sector concerned. A suspicious situation might well involve several factors which, on their own, seem not to be significant but, when taken together, are sufficient to arouse suspicion.

The situation must be evaluated having regard to the nature of the enterprise concerned as well as usual transactions expected in a business of that nature. Account must also be taken of the suspicious person's enterprise, financial history, background and behaviour.

When the transaction must be reported

In terms of *s*ection 29(1):

- if a person knows, or suspects, that there is no apparent business, or lawful, purpose giving rise to the transaction; or
- the transaction appears to be unusual within the context of the sector; or
- it is unclear whether or not the purpose of the transaction is lawful;

the transaction must be reported to the FIC.

In identifying situations of this nature all background knowledge and information on the purpose of a particular transaction must be applied. The transaction should be evaluated against such relevant factors as its size and complexity as well as the client's enterprise, financial history, background and behaviour.

Suspicious activity reports, terrorist financing activity reports and transaction reports

Both suspicious or unusual transactions and activities must be reported to the FIC. The reports submitted will, therefore, either be activity reports, such as suspicious activity reports (SARs) and terrorist financing activity reports (TFARs), or transaction reports, such as suspicious and unusual transaction reports and terrorist financing transaction reports.

A suspicious activity report is submitted concerning the proceeds of unlawful activities or money laundering activity in respect of activities not involving a transaction between two or more parties or in respect of a transaction, or a series of transactions, where enquiries were made but are not yet concluded.

A terrorist financing activity report will, similarly, be submitted in respect of the financing of terrorism and related activities not involving a transaction between two or more parties or concerning a transaction, or a series of transactions, about which enquiries were made but not yet concluded.

Enquiries made but not yet concluded

Examples of enquiries made, but not yet been concluded, could concern aborted, incomplete, attempted, interrupted or cancelled transactions such as:

- a potential client refuses to provide the necessary client identification and verification documentation required by the FIC Act and the transaction does not proceed;
- a person attempts to deposit cash at the branch office of an estate agency enterprise and, upon enquiry as to the source of funds, refuses to provide any information and, now put on guard, does not deposit the cash as was intended;
- a person asks an estate agent whether it is possible to purchase a property and register it the name of a relative to hide assets from the SA Revenue Service but does not proceed with the transaction.

If undoubtedly suspicious transactions of this nature were concluded it is probable that the enterprise would have been used to facilitate money laundering. The matters, consequently, would have had to be reported to the FIC.

Suspicious or unusual transaction reports

Completed transactions to which the enterprise is a party necessitate the submission of a suspicious or unusual transaction report (STR) to the FIC. This applies whether in respect of a particular transaction or a whole series of transactions, such as, for instance:

- a transaction, or series of transactions, with the enterprise that has, or have, no apparent business or lawful purpose or that may be relevant to an investigation by the SA Revenue Service into tax evasion; or
- a client who, during the course of one day, deposits cash amounts of R5 000 at various branches of the enterprise in a total amount exceeding the cash threshold reporting amount of R24 999.00 so as, apparently, to avoid triggering a cash threshold report.

Completed, or not yet completed, transactions of this nature undoubtedly raise serious questions or, at the very least, give rise to a sense of discomfort, apprehension or mistrust. It would, therefore, be necessary to furnish the required reports regarding the matters to the FIC.

Indicators of reportable transactions

The FIC has furnished the following list of indicators for use as examples of the various factors that must be considered when evaluating particular transactions. The FIC cautions, however, that the indicators provided are neither exhaustive nor do they cover all possible situations.

The indicators provided must also not be viewed in isolation but should be considered in light of all circumstances relevant to the particular transactions.

Unusual transactions

- Deposits of funds with a request for their immediate transfer elsewhere.
- Unwarranted and unexplained international transfers.
- The payment of commissions or fees that appear to be excessive in relation to those normally payable.
- Transactions that do not appear to be in keeping with normal industry practices.
- The purchase of commodities at prices significantly above or below market prices.
- Unnecessarily complex transactions.
- Unwarranted involvement of structures, such as trusts and corporate vehicles, in transactions.
- Transactions that seem to be unusually large or otherwise inconsistent with the client's financial standing or usual pattern of activities.
- Buying or selling securities with no apparent concern for making a profit or avoiding a loss.
- Performing similar transactions (i.e. cash deposits) at multiple branches of the same enterprise on the same enterprise day.
- Performing transactions in a manner that attempts to conceal the underlying client and/or ultimate beneficiary of the transaction.
- An unwarranted desire to involve entities in foreign jurisdictions in transactions.

No monetary threshold in reporting suspicious or unusual transactions

There is no monetary threshold where the reporting of suspicious or unusual transactions is concerned. Once it has been determined that the situation is suspicious and that the transaction, or activity, relates to the proceeds of unlawful activities, money laundering or terror financing, that transaction or activity must be reported to the FIC – irrespective of the amount involved in the transaction.

Estate agency enterprises, like all accountable institutions, are obliged to monitor, detect and report suspicious or unusual transactions to the FIC. The FIC, to this end, recommends that estate agents map and document their estate agency products and services as this will assist them in identifying, and monitoring, potential money laundering and terrorist financing risks associated with the estate agency sector.

Situations where a suspicion may arise regarding particular activities

The FIC has also furnished a list of possible indicators appropriate to situations where a suspicion may arise regarding particular activities. These indicators, once again, must not be viewed in isolation but considered together with all circumstances relevant to the particular transaction or transactions.

Unusual enterprise

- A lack of concern about high commissions, fees, penalties etc., incurred as a result of a particular type of transaction or particular method of transacting.
- An attempt to conceal the underlying client performing the transaction and/or the ultimate beneficiary thereof.
- A client attempts to perform a transaction, which is interrupted, cancelled and/or reversed and which does not seem to have any apparent business purpose.

Knowledge of reporting or record-keeping requirements

- A client attempts to convince an employee of the business not to complete any documentation required for the transaction.
- A client makes inquiries indicative of a desire to avoid reporting.
- A client has unusual knowledge of the law relating to suspicious transaction reporting.
- A client seems to be very conversant with money laundering or terrorist financing activity issues.
- A client is quick to volunteer information that the funds are clean and/or are not being laundered.

Identification

- The use of a seemingly false identity in connection with any transaction, including the use of aliases and a variety of similar, but different, addresses and, in particular, the opening or operating of a false name account.
- Opening accounts using false or fictitious documents.
- A client provides doubtful or vague identification information.
- A client refuses to produce personal identification documents.
- A client changes a transaction after being requested to provide a form of identification.
- A client only submits a copy of personal identification documents.
- A client wants to establish identity by using something other than that client's own personal identification documents.
- A client's supporting documentation lacks important details such as contact particulars.
- A client inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be verified for some reason.

General

- A client provides insufficient, vague or suspicious information concerning a transaction.
- Accounts that show unexpectedly large cash deposits and immediate withdrawals.
- A frequent exchange of small denomination notes for larger denomination notes.
- Involvement of significant amounts of cash in circumstances difficult to explain.

Terrorism financing and activity reports

In terms of section 28A estate agency enterprises are required to file a report with the FIC if that enterprise:

- knows that it possesses or controls property linked to terrorism; or
- to entities that are sanctioned by the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 3 of 2004 (the POCDATARA Act).

Knowledge of the origin and ownership of the property is based on fact

Knowledge of the origin and ownership of the property should be based on fact with reference to an objective set of circumstances or facts. Section 28A, thus, applies to a purely factual situation, namely, that an estate agency enterprise has property in its possession or under its control that is linked to terrorism.

This situation must immediately prompt a report to the FIC. It is not necessary for there to be any activity relating to that property for the triggering of the report. An estate agency enterprise which files a report in terms of section 28A(1)(a) must objectively know that it possesses or controls property linked to terrorism.

Section 4 of the POCDATARA Act

It is to be underscored that section 4 of the POCDATARA Act expressly prohibits persons from dealing with:

- property associated with acts of terrorism;
- persons or organisations that carry out acts of terrorism; or
- entities that are sanctioned pursuant to the POCDATARA Act.

Any dealings with property identified in a section 28A report will, thus, also constitute a contravention of section 4 of the POCDATARA Act.

When an estate agency enterprise files a section 28A report the result will be the freezing of the property concerned. The enterprise must, in addition, forthwith cease to conduct business with the relevant entity. After having filed a section 28A report section 4 of the POCDATARA Act, in fact, makes it an offence for the estate agency enterprise to continue in any way to deal with the property.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must indicate the processes for dealing with instances where the enterprise is aware that it possesses or controls property linked to terrorism or to entities that are sanctioned by the POCDATARA Act, the filing of the section 28 report with the FIC and the subsequent freezing of the relevant property.

Submitting multiple reports to the FIC

It could sometimes be necessary for an estate agency enterprise to complete and submit reports to the FIC under both sections 28A and 29 in respect of the same client. The section 29 report would refer to the transaction or activity that the enterprise believes to be suspicious or unusual while the section 28A report would be in respect of property which is under the control of the enterprise and which the enterprise knows is connected to the financing of terrorist activities. It is also possible that a cash transaction which exceeds the prescribed cash threshold amount will be reportable to the FIC in terms of both sections 28 and 29.

The UN 1267 lists

Section 25 of the POCDATARA Act requires the President to give notice, by proclamation in the Government Gazette, of any entity designated by the United Nations Security Council (the UNSC) for the purposes of combatting or preventing terrorist and related activities. The UNSC publishes such sanction lists ("UN 1267 lists") in this respect. The UN 1267 lists may be accessed by enterprises from https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list.

To determine if they are dealing with a person appearing on the UN1267 list, estate agency enterprises must "screen" client(s) against the list. If a client's name appears on the UN1267 list the enterprise must ensure that it is an exact match. In so doing the enterprise should make use of all available information and, in addition, conduct such further research as may be necessary. If the enterprise determines that it does control relevant property it must report full particulars of the type of property concerned, including a description of the property, in the section 28 report to the FIC.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must indicate the measures in place for the enterprise to determine if it is dealing with a person who is on the UN1267 list and to establish the particulars and description of the property linked to terrorism or to entities sanctioned by the POCDATARA Act.

Failure to file a section 28A report with the FIC is an offence in terms of section 51A of the FIC Act. An estate agency enterprise that does not have the required measures in place may also be guilty of an offence in terms of section 4 of the POCDATARA Act.

Possible measures to counter the financing of terrorism

Possible measures that may be implemented, if required, to counter the financing of terrorism include the:

- automated real time screening of client databases at client take-on;
- ongoing screening of existing client databases to detect potential matches when there are changes to the UNSC sanction lists or to the status of existing client identification information; and
- screening of cross border payments by financial institutions, where applicable.

The effectiveness of screening processes is dependent on an efficient client identification and verification programme.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must indicate the measures in place to enable the enterprise to counter the perceived risk of being abused to finance terrorism or to promote the activities of terrorist organisations.

After having reported a transaction

After having reported a suspicious or unusual transaction to the FIC an estate agent may continue with, and finalise, that transaction (section 33) unless the FIC issues a written instruction to the estate agent not to proceed with the transaction (section 34). The FIC may issue a written instruction, known as an 'intervention order', to the estate agent not to proceed with a transaction, or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction, for a prescribed period. The intervention order remains valid for the period specified in the order.

The FIC may request additional information

After having received a section 29 report the FIC may request further information. In such a case the reporter must furnish the additional information that has been requested in accordance with the terms of the request.

In terms of section 37(1) a duty of secrecy or confidentiality may not prevent an enterprise or person from complying with the obligation to file a section 29 report. Section 37(2) does, however, protect the common law right of legal professional privilege as between an attorney and the attorney's client, or a third party and an attorney, for the purposes of legal advice or litigation which is pending, contemplated or has commenced.

Protection of persons who have submitted reports to the FIC

The FIC Act does protect persons who have submitted reports to the FIC. No criminal or civil legal action may be instituted against any person who, in good faith, has duly complied with FIC reporting obligations. The FIC Act also protects the identities of persons who have made reports. A reporting person cannot be forced to give evidence in any criminal proceedings concerning the report but may voluntarily choose to do so. If the reporting person elects not to testify, evidence regarding that person's identity is not admissible in any ensuing criminal proceedings.

Confidentiality of reports

A person who had made a report may not inform anyone, including the client or any other person associated with the reported transaction, of either the content of the report or the fact that a report was made to the FIC. The FIC Act, furthermore, prohibits a reporter or any other person who knows or suspects that a report was made from disclosing any information regarding that report save for information disclosed:

- to comply with the provisions of the FIC Act;
- for purpose of legal proceedings, including any proceedings before a judge in chambers;
- in terms of an order of court.

Any contravention of this prohibition is a criminal offence for which a maximum penalty of imprisonment for a period of fifteen years or a maximum fine of R100 million may be imposed.

A person who has made a report to the FIC may not inform anyone, including the client or any other person associated with the reported transaction, of the content of the report or even that such a report was made unless the information disclosed was done:

- within the scope of the powers and duties of that person in terms of any legislation;
- for the purpose of carrying out the provisions of the FIC Act;
- for the purpose of legal proceedings, including any proceedings before a judge in chambers;
- in terms of an order of court.

A contravention of this prohibition is a criminal offence for which a maximum penalty of imprisonment for a period of fifteen years or a maximum fine of R100 million may be imposed.

A person who should have reported suspicious or unusual transactions to the FIC and who is charged with a failure to do so, can raise the defence that such person duly complied with the Risk Management and Compliance Policy relating to the reporting of information or that the person reported the matter internally to the person responsible for ensuring FIC compliance. An employee who is required to report the matter to a superior, and has proof of having done so, will have a valid defence to such a charge.

In many situations a suspicious or unusual transaction or activity report may imply that the enterprise is dealing with the proceeds of unlawful activities falling within the scope of the money laundering offences provided for in the Prevention of Organised Crime Act. That Act, therefore, grants certain defences to such persons, which allows them freely to report their suspicions to the FIC while still being able to carry on their business activities without being exposed to any criminal liability.

Reactive rather than proactive reporting

There will be cases where reactive, rather than proactive, reporting to the FIC occurs. This generally happens when a report is lodged with the FIC only after an external prompt to do so was received.

External prompts that may result in reactive reporting

External prompts of this nature may arise after:

- receiving a subpoena in terms of the Criminal Procedure Act, or a similar process, to provide evidence concerning matters relating to business dealings with a particular client;
- receiving a request to confirm whether a person is a client of a business in terms of section 27 of the FIC Act in respect of a particular client;
- receiving an intervention order in terms of section 34 of the FIC Act in connection with a transaction involving a particular client;
- receiving a monitoring order in terms of section 35 of the FIC Act concerning the transactions of a particular client;
- receiving enquiries from government agencies, such as investigating authorities or the South African Revenue Service, about a particular client;
- discovering adverse information while conducting an on-going due diligence of clients;
- seeing information in the media that may adversely affect a particular client.

The occurrence of these external factors is likely to contribute to a suspicion or a sense of unease regarding the transaction and may result in the reactive lodging of a report. Such external factors must be considered with all the other factors impacting the particular transaction, or series of transactions as the external factors alone may not constitute sufficient reason to submit a report to the FIC in the absence of any suspicion regarding the transaction.

Lodging reports with the FIC

Section 29 reports must be filed with the FIC electronically by using the internet-based reporting portal provided for this purpose. Persons required to make reports should access the FIC website at www.fic.gov.za for this purpose. It is to be underscored that section 29 reports should never, under any circumstances, be posted to the FIC.

Section 29 reports must be sent to the FIC as soon as possible but within no more than fifteen days after a person has become aware of the facts giving rise to the raising of the suspicion.

The fifteen day period commences when a person became aware of the facts which eventually resulted in the report and may be even before a suspicion was fully formed. The fifteen day period includes any time necessary to complete internal transactional monitoring alert system processes and/or internal investigation and review processes required by the enterprise Risk Management and Compliance Policy.

The FIC will only condone the late submission of a section 29 report in exceptional cases. If it is apparent that it will not be possible timeously to submit the section 29 report, a written application for condonation of the late filing should immediately be made to the FIC. The application must provide sound reasons why the deadline cannot be met and give an indication as to when it is envisaged that the report will be submitted to the FIC.

When submitting a section 29 report the reporting party must:

- ensure that client information sets are comprehensively completed;
- provide valid ID/Passport information and other necessary client information;
- map and report on transactions where the client's account is debited and/or credited; and
- ensure that an appropriate descriptive narrative for both the "Reason/Reason for Reporting" and "Action/Action Taken" fields on the reporting form is completed.

Enterprises must provide all the information in their possession, under their control and available within their various operating systems, to the FIC. Where it is commercial practice for the enterprise to obtain information regarding clients, products, services and transactions, such information will be deemed to be readily available and must be provided to the FIC together with the section 29 report, even if that information was not verified, or otherwise confirmed, at the time when it was obtained.

The FIC reporting platform requires the completion of several mandatory fields. If any these mandatory fields are left blank the section 29 report will not pass a FIC validation check meaning that the reporter will not be able to submit the form. If a reporter does not have the required information to complete a mandatory field this may indicated by stating "not obtained".

After receipt of a section 29 report the FIC will conduct appropriate analytical work on the information provided. If the FIC has a reasonable belief that the information is necessary to investigate suspected unlawful activity the information is referred to the appropriate authority for further investigation, bearing in mind that the personal information of persons involved in making the report is protected from unauthorised disclosure.

Cash threshold reporting

In terms of section 28 accountable institutions, including estate agency enterprises, must report cash transactions above a certain prescribed threshold to the FIC. The reporting obligation arises when a transaction, or series of aggregated transactions, is concluded with a client and cash is either paid, or received, by an estate agency enterprise:

- to, or from, the client; or
- to, or from, a person acting on behalf of the client; or
- to, or from, a person on whose behalf the client is acting;

in an amount, or an aggregated amount, exceeding R24 999,99 being the currently prescribed cash threshold limit.

Definition of cash

'Cash' is defined, in section 1, as coin and paper money of the Republic, or of another country, that is designated as legal tender and that circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue and travellers' cheques.

The definition of cash does not include bearer negotiable instruments, a transfer of funds by bank cheque, bank draft, electronic funds transfer, wire transfer or other written order not involving the physical transfer of cash. These latter methods of transferring funds are not regarded as cash and, as such, are not reportable to the FIC under section 28.

If a transaction is partly a cash transaction then only the cash portion of that transaction must be reported to the FIC if that cash portion exceeds R24 999,99. Physical cash payments presented to, and received by or on behalf of, an estate agency enterprise are also reportable. Where an estate agency enterprise pays a client in physical cash this cash payment is also reportable if the amount paid exceeds R24 999,99.

It is to be underscored that the payment, or receipt, of cash includes paying or receiving cash in person or through a third party.

Submission of cash threshold reports to the FIC

Section 28 reports must be sent the FIC as soon as possible but, in any event, within no more than two days after:

- if a natural person, that person or the employees of that person; or
- if a legal person, the employees or officers of that legal person or other entity;

became aware that a cash transaction, or a series of cash transactions, has exceeded the prescribed threshold of R24 999,99.

Documenting cash threshold reporting procedures

Estate agency firms must consider, and properly document, their cash threshold reporting and aggregation processes to ensure that they strictly adhere to the two-day reporting time period. They should also conduct reviews and compile sample reports to ensure that their reports properly comply with FIC requirements in this respect.

The enterprise Risk Management and Compliance Programme

The enterprise Risk Management and Compliance Programme must clearly define, formalise, indicate and describe the cash and cash aggregation threshold reporting processes and provide for conducting reviews and compiling sample reports to ensure that cash and cash aggregation threshold reports fully comply with FIC requirements and that the reports include the particularity prescribed in the Money Laundering and Terrorist Financing Control Regulations.

Regulation 22C of the Money Laundering and Terrorist Financing Control (MLTFC) Regulations provides that it is mandatory that the full particulars that the estate agency enterprise is expected to have, or, alternatively, as much of the relevant information as is readily available, be provided.

Where readily available information is concerned, the particulars provided may include information that subsequently became available but which the enterprise may not have obtained when it established a particular person's identity or conducted a particular transaction. In this case the enterprise must provide all information presently within its control and/or which is available within its structures. If it is the commercial practice of an enterprise to obtain certain information in relation to clients, products, services and transactions, that information will be deemed to be readily available to the enterprise and must be provided, where applicable, when submitting a section 28 report to the FIC, even if that information was not verified or otherwise confirmed at the time when it was obtained.

It will be noted that the reporting platform of the FIC contains various mandatory fields that must be completed. The section 28 report will not pass a FIC validation check if these fields are not completed with the result that the reporter will not be able to submit the report. Should the required information not be available the reporter must indicate this fact by entering "not obtained".

Aggregate cash threshold reporting

An estate agency enterprise must report aggregates of smaller amounts which, when taken together, add up to an amount exceeding R24 999,99. The aggregation is also done where a series of smaller and larger amounts (in excess of R24 999.99) appear to be linked. The cash amount can, therefore, be made up of:

- a single cash transaction to the value of R25 000 or more; or
- an aggregation of many smaller amounts which, taken together, have a combined value of R25 000 or more. The aggregation period is not specified but the FIC recommends that a period of at least twenty-four hours be applied when considering aggregation for cash threshold purposes.

Estate agency enterprises must, consequently, ensure they sufficiently define and formalise their internal processes so that they can easily detect, aggregate and report on cash transactions exceeding R25 000 to the FIC. This ensures that enterprises have a consistent and measurable process that can be effectively applied to discharge their section 28 cash threshold reporting obligations.

According to the FIC, some indications that a series of smaller amounts have combined to form an aggregated transaction exceeding R24 999,99 will include:

- the period within which the series of smaller transactions take place;
- the fact that the series of transactions consists of a repetition of the same type of transaction e.g., cash payments or cash deposits; and
- the smaller amount transactions involve the same client or relate to the same enterprise relationship.

Individually listing aggregated cash transactions

Estate agency enterprises must take care to ensure that all aggregated cash transactions are individually listed on the aggregated cash threshold report (CTRA) since it is not permissible to summarise separate transactions as a single combined transaction. Say, for example, a client makes three cash deposits of R10 000 each into the trust account of an enterprise on the same day for three separate transactions.

As the aggregated cash amount is R30 000, which exceeds the cash threshold limit, the estate agency enterprise must submit an aggregated cash threshold report to the FIC listing the three cash deposits separately as follows:
Transaction 1 – cash deposit of R10 000
Transaction 2 – cash deposit of R10 000
Transaction 3 – cash deposit of R10 000

The FIC reporting system will detect the aggregated cash total of R30 000.

It has already been noted that section 29(1)(iii) requires that suspicious or unusual transactions, or a series of such transactions, be reported to the FIC. It is possible, therefore, that a cash transaction exceeding R24 999,99 could give rise to both a section 28 cash threshold report as well as a section 29 suspicious or unusual transaction report. Estate agency enterprises must be mindful of the fact that, while a cash transaction is not reportable in terms of section 28 if the cash value is less than R24 999,99, all cash transactions should, nevertheless, be carefully monitored. If a cash transaction that is less than R24 999,99 nevertheless seems to be suspicious or raises doubts, a section 29 suspicious or unusual transaction report must be submitted to the FIC.

Cash threshold transactions, whether single or aggregated, must be reported to the FIC according to whether cash was received or cash was paid.

Reportable cash threshold transactions

Some examples of reportable cash threshold transactions:

- Say an estate agency enterprise receives a cash amount of R20 000 from a certain client and, on the same day, the enterprise pays a cash amount of R29 000 to that same client in respect of a particular transaction.
- The enterprise then receives a further cash payment of R5 000 on the same day from the client – but this time in respect of a different transaction.
- The enterprise must report both the aggregated amount of cash that was received from the client in respect of both transactions, since the cash amount that was received exceeded the prescribed cash threshold limit and the cash amount of R29 000 that was paid by the enterprise to the client.
- The enterprise would, therefore, be required to submit two cash threshold reports to the FIC. The one report will be an aggregated cash threshold report in respect of the two cash transactions (R25 000) while the second report will be an ordinary cash threshold report in respect of the cash paid (R29 000).

As the above example illustrates it is not only prudent for, but also expected of, estate agency enterprises carefully to monitor their bank accounts on a daily basis to ascertain whether any cash payments have been made or received that exceed the prescribed cash payment threshold. The FIC, indeed, has requested banks to ensure that bank statements issued to their clients clearly refer to cash, as defined in section 1 of the FIC Act.
Doing so should enable banking clients more easily and readily to identify and distinguish all section 29 cash reportable transactions appearing in the bank statement.

Cash payments in foreign currency

Where a cash transaction which exceeds the cash threshold and, therefore, necessitates the submission of a cash threshold report to the FIC, comprises foreign currency, the estate agency enterprise concerned must refer to the exchange rate prevailing at the time when the cash was received to convert the value of the foreign cash payment amount into Rand. The estate agency enterprise may itself determine the source of the exchange rate that is to be used to convert the foreign currency into South African currency.

Cash payments exceeding the threshold

Section 28(b) deals with instances where cash that exceeds the cash threshold is received from:
- a client; or
- a person acting on behalf of a client; or
- a person on whose behalf a client is acting.

Take, for example, the case of a client of an estate agency enterprise who wishes to pay a cash amount of R25 000, as a deposit in respect of a transaction, to the enterprise. The enterprise requests that client to pay the cash sum of R25 000 into its trust account which is held at a particular bank. The client does so and the bank duly receives that cash amount into the trust account of the enterprise. As the bank is an accountable institution, it must submit a section 28 cash threshold report to the FIC. The enterprise then receives either its bank statement or a bank deposit slip from the client reflecting the cash transaction, which exceeded the prescribed cash threshold. Since the estate agency enterprise is also an accountable institution, it is now obliged to submit a section 28 cash threshold report to the FIC. This particular transaction will, therefore, be reported to the FIC by both the bank and the estate agency enterprise.

This example also clarifies the fact that where cash is received or paid by an estate agency enterprise into, or from, an account held in the name of another accountable institution there will be a duty on both of those accountable institutions to report the transaction to the FIC. There will, consequently, frequently be instances where two or more accountable institutions must submit a section 28 report to the FIC in respect of a single transaction that exceeds the prescribed cash threshold.

Filing the cash threshold report

Cash transaction and aggregated cash transaction reports must be electronically filed with the FIC using the internet-based reporting portal provided for this purpose. The portal may be accessed at www.fic.gov.za.

Registering with the FIC

Estate agency enterprises are reminded that, as accountable institutions, they must register with the FIC. Such registration provides estate agency enterprises with the necessary user credentials for use when electronically submitting cash transaction and aggregated cash transaction reports to the FIC. Enterprises should, accordingly, carefully consider the FIC registration requirements, which can be accessed from the FIC website, and ensure that they fully comply therewith so as to be able to discharge their reporting obligations in terms of section 28.

Using the FIC registration and reporting platform

The FIC has indicated that following general principles must be considered when using the FIC registration and reporting platform:

- users must be registered on the FIC's registration and reporting platform;
- reporters should save their web reports whilst moving between various sections of the report form and before the report is submitted;
- reporters should monitor the status of their submitted reports to ensure that the reports are successfully processed and that any failures/rejections are immediately remediated;
- reporters should download and save a copy of submitted reports for internal record keeping purposes; and

- reporters should ensure that any ICT related queries/incidents are logged with the FIC by means of the communicated channels and that they keep records thereof.

REFERENCES

The Financial Intelligence Centre Act, 38 of 2001, as amended.

The Money Laundering and Terrorist Financing Control Regulations, 2002, as amended from time to time

The Prevention of Organised Crime Act, 121 of 1998.

The Prevention of Constitutional Democracy against Terrorism and Related Activities Act, 32 of 2004.

Financial Intelligence Centre, Guidance Note 4A, "ON REPORTING OF SUSPICIOUS AND UNUSUAL TRANSACTIONS AND ACTIVITIES TO THE FINANCIAL INTELLIGENCE CENTRE IN TERMS OF SECTION 29 OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 38 OF 2001."

Financial Intelligence Centre, Guidance Note 5B, "ON CASH THRESHOLD REPORTING TO THE FINANCIAL INTELLIGENCE CENTRE IN TERMS OF SECTION 28 OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 23 OF 2001."

Financial Intelligence Centre, Guidance Note 6, "ON TERRORIST FINANCING AND TERRORIST PROPERTY REPORTING OBLIGATIONS IN TERMS OF SECTION 28A OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 38 OF 2001."

Financial Intelligence Centre, Guidance Note 7, ON THE IMPLEMENTATION OF VARIOUS ASPECTS OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 38 OF 2001."