Financial Services Board

FAIS NEWSLETTER

Volume 6

June 2008

IN THIS ISSUE

Disclaimer

This Newsletter does not absolve authorised FSPs of their obligation to acquaint themselves, interpret and comply with the provisions of the relevant money laundering legislations and related regulations, exemptions and guidance notes. Persons seeking more information or understanding on any provision relating to the afore-mentioned are encouraged to contact the FIC. Authorised FSPs are also encouraged to log onto the FIC's website at www.fic.gov.za for more information and access to documents referred to in this Newsletter.

INTRODUCTION

Combating organised crime, money laundering and suppressing the financing of terrorist activities is a major challenge faced by all countries today. South Africa has become more involved since re-admission to the international fraternity in 2004. For this reason various anti-money laundering legislation has been published.

The first part of this Newsletter addresses the key provisions of the relevant money laundering legislations and related regulations which will help the authorised Financial Services Providers ("FSPs") to beef up their efforts to combat organised crime and most importantly comply. The findings of the recent FICA theme visits conducted by the FAIS Supervision Department on authorised FSPs are discussed and published in the second part.

CURSORY OVERVIEW OF MONEY LAUNDERING

Definition of Money Laundering

Money laundering – refers to any act that obscures the illicit nature or the existence, location or application of proceeds of crime. Simply put, money laundering is the processing of proceeds of criminal activities to disguise their origin.

Money laundering is global in nature and is exacerbated by amongst others advancements in technology and online business transactions. It is a flexible operation that can adapt to any business environment in any jurisdiction. Money launderers have vast resources at their disposal and often receive professional assistance to carry out their activities. Countries with developing economies or those undergoing changes in the financial system serve as potential lucrative markets for these criminals.

Stages in the money laundering process

Money laundering is a multi-faceted process, but often takes place in 3 stages as follows:

The placement stage – is where cash derived from a criminal activity is first placed into the system through a financial institution or is used to buy an asset.

The layering stage – is the criminal's first attempt to conceal or disguise the source of the ownership of the funds.

The integration stage – is where money is integrated into the legitimate economic and financial system and is assimilated with all other assets in the system.

The goals of money laundering

- To place illegal money in the formal financial system without arousing suspicion.
- To transfer and/or move money around in a series of complex transactions, so it becomes difficult to trace its original source. Authorised FSPs are therefore encouraged to implement proactive measures designed to determine suspicious transactions, file reports, and minimise the likelihood of their business being used as conduits to launder money.

Why combat money laundering?

- It is an international requirement.
- Money laundering affects all legitimate businesses. Authorised FSPs are more at risk as criminals are constantly seeking financial products and services which could be utilised to launder ill-gotten gains.
- The impact of money laundering is felt by the entire society and every organisation is vulnerable.
- It affects the integrity of the financial system and the economy at large.
- Money laundering slows down economic development of a country.
- It is often deeply entrenched in the political and financial system of a country. The political and business sectors must therefore foster joint efforts to deal with it.

FINANCIAL ACTION TASK FORCE ("FATF")

FATF is an international body responsible for overseeing and combating money laundering and other aspects of financial crime and funding of terrorism. It develops standards to combat these crimes. In 1990, FATF issued a Forty Point list of Recommendations on money laundering countermeasures intended to serve as standards. These standards prescribe a range of actions designed to improve national regime, enhance the financial system and strengthen international cooperation against financial crime. The standards were revised in 2003.

After the September 11 attacks, FATF strengthened measures to combat organised crime by expanding its mandate beyond money laundering and issued the Eight Special Recommendations on terrorist financing in 2001.

To fight crime, FATF created Financial Intelligence Units ("FIUs") for member countries. The FIUs are specialised national agencies designed to attack financial crime in its various modes through the exchange of information, sharing of expertise and other forms of cooperation. In South Africa, the Financial Intelligence Centre ("FIC") was entrusted with this obligation.

Note that South Africa became a member of FATF in 2003. By becoming a member, we committed ourselves to implement and comply with the international AML/CFT standards of FATF. In so doing, we also joined global efforts to combat organised crime.

MONEY LAUNDERING LEGISLATIONS IN SOUTH AFRICA

South Africa's statutory framework to combat money laundering and suppress the financing of terrorism is vested in the Financial Intelligence Centre Act, 38 of 2001 ("FICA") and Prevention of Organised Crime Act, 121 of 1998 ("POCA"). These legislations enable South Africa to meet international standards, and also empower law enforcement agencies to combat organised crime more effectively.

POCA defines the general money laundering offences, whereas FICA gives rise to detailed money laundering control obligations for accountable institutions (*Accountable institutions are persons and entities listed under* ***Schedule 1***). The most important provisions of FICA and POCA are discussed in detail hereunder.

Financial Intelligence Centre Act, 38 of 2001

It is important to note that currently, FICA does not empower the FIC to supervise the accountable institutions. The supervisory functions are performed by all supervisory bodies listed under ***Schedule 2***. Each supervisory body is responsible for enforcing compliance with money laundering legislations by the accountable institutions under its regulation or supervision.

FICA provides for:

- The establishment and operation of the FIC and MLAC (Money Laundering Advisory Council);
- Creation of money laundering control obligations for specific persons and institutions;
- Regulation of access to information.

Objectives of the FIC

The FIC was established in 2002 in terms of section 2 of FICA. Its objectives are:

- To assist in the identification of the proceeds of unlawful activities;
- To combat money laundering activities;
- To make information collected by it available to investigating authorities, supervisory bodies, intelligence services, and SARS in order to facilitate the administration and enforcement of relevant legislations;
- To exchange information with its counterparts and similar bodies in other countries regarding money laundering activities and similar offences;
- To regulate access to specific information.

Money Laundering Control Obligations

FICA creates four money laundering control obligations for all accountable institutions as follows:

- Duty to identify and verify clients;
- Duty to keep records of business relationships and transactions;
- Reporting duties and obligations to give and allow access to information;
- Adoption of measures designed to promote compliance by accountable institutions;

MONEY LAUNDERING LEGISLATIONS IN SOUTH AFRICA

I. Duty to identify clients

Client identification and verification procedures are crucial elements of the money laundering control system. If carried out effectively, they make it more difficult for criminals to use false identities in their attempt to disguise as clients of the accountable institutions. Authorised FSPs are therefore encouraged to undertake proactive measures designed to assist them to detect these false pretences and report them accordingly.

i. Identification and verification of new clients:

The duty to identify clients became effective on 30 June 2003. Section 21(1) of FICA requires accountable institutions to identify new clients and verify their particulars before any transaction may be concluded or any business relationship is established with them unless they qualify for ***Exemption 2***.

It stipulates that an accountable institution may accept a mandate from a prospective client and proceed to establish a business relationship or conclude a single transaction with that client (*Please refer to this exemption for details of persons who may qualify for it and the conditions that must be met*).

ii. Verification documents:

The Money Laundering Control Regulations prescribe the identification and verification requirements for clients of accountable institutions ranging from SA citizens & residents, Foreign nationals, Close corporations, South African companies, Foreign companies, Partnerships and Trusts. It was established during the recent FICA onsite visits that some authorised FSPs accepted questionable documents from clients that cannot objectively and reasonably serve to achieve verification of their identities.

Note that the best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit (*Please refer to* ***Regulation 2 to 16*** *for full particulars of the information that should be obtained and verified from clients as well as the verification procedures to be followed*).

The information obtained from legal persons such as Companies, Close corporations, and Trusts must be verified by comparing it against the registration documents of these legal entities.

The identification procedures in respect of the legal persons referred to above must also be extended to directors, shareholders, members and trustees. Documents serving to confirm their authority to act on behalf of these legal entities must also be obtained.

iii. Identification and verification of current clients:

Section 21(2) of FICA requires a similar approach discussed under section 21(1) to be applied in respect of all current clients (C*urrent clients are those persons and institutions with whom the accountable institution had business relationships on 30 June 2003*).

It states that if an accountable institution had established a business relationship with a client before FICA took effect, it may not conclude further transactions in the course of that business relationship, unless prescribed steps are taken to ensure the identities of the clients are established and verified. The accountable institutions were given until 30 June 2004 to comply with this requirement.

MONEY LAUNDERING LEGISLATIONS IN SOUTH AFRICA

Due to certain hardships created by this requirement, and realising that many accountable institutions were not going to meet the client re-identification deadline, ***Guidance Note 1*** and a number of exemptions were published for Banks, Members of an exchange, Investment managers, Management companies of Collective Investment Scheme etc.

iv. Additional measures when a person represents or acts on authority of another

Regulation 17 states that if a person wants to establish a business relationship or to conclude a single transaction with an accountable institution on behalf of another person, the accountable institution must in addition to the normal identification and verification requirements, obtain from that person information which provides proof of that person's authority to act on behalf of the client. Information that can be obtained includes Mandate, Power of attorney, etc.

v. Verification in the absence of contact person (non face to face clients)

Regulation 18 stipulates that if the accountable institution obtained identification and verification information from a natural or legal person without contact in person with such a natural person or representative of that legal person, the accountable institution must take reasonable steps to establish the existence and verify the identity of that natural person or legal person. Authorised FSPs are encouraged to establish procedures for dealing with non face to face clients and must incorporate them into their main client acceptance procedure manual.

vi. Maintenance of correctness of particulars

Regulation 19 requires accountable institutions to take reasonable steps, in respect of an existing business relationship, to maintain the correctness of particulars which are susceptible to change and which were provided to it as part of the client identification and verification process. This can be seen as a proactive measure implemented from a risk management perspective to mitigate potential risks. The concept of risk based approach is discussed in detail below.

vii. Risk based approach

Guidance Note 1 and FATF's revised Recommendations strongly advocate a risk based approach to client identification. Recommendation 5 requires accountable institutions to identify and verify current clients on the basis of materiality and risk. If correctly interpreted, it would mean that this requirement applies to high risk clients and transactions only. They will have to be subjected to a higher degree of due diligence than lower risk clients.

It is important to note that a risk based approach as to what is reasonable in the circumstances can be used to obtain satisfactory evidence of clients' identity. The extent and number of checks and balances applicable can vary depending on the perceived risk. The risk based approach can be applied to the following scenarios:

MONEY LAUNDERING LEGISLATIONS IN SOUTH AFRICA

a. Client Profile

Regulation 21 advocates building a client profile whenever it is reasonably necessary (subject to guidance from the FIC), if the accountable institution wants to obtain additional information from an existing or prospective client –

- concerning a business relationship or single transaction which poses a particularly high risk of facilitating money laundering activities, or
- to enable it to identify the proceeds of unlawful activity or money laundering activities.

The information which must be obtained must be adequate to reasonably enable the accountable institution to determine whether the transactions involving such a client are consistent with the institution's knowledge of that client or match the client's business activities, and must include particulars concerning the client's source of income and/ or source of funds.

Undoubtedly, a risk based approach can assist accountable institutions to focus on the potential risks posed by clients. As mentioned earlier, Regulation 21 requires accountable institutions to obtain more information about clients, business relationships and transactions that pose a high risk of facilitating money laundering activities. The CIV and KYC procedures can be used to obtain this information. They are valuable tools that can assist accountable institutions to manage client risks, including money laundering risks. The accountable institution can use these tools to profile a client and to identify transactions that deviate from this profile.

By obtaining information prescribed under section 21 of FICA, accountable institutions are simply building a client profile. Client profiling enables accountable institutions to monitor client behavior and match it against that of other clients with a similar behavior. It also enables the institution to anticipate certain transactions by the client. After receiving information, the degree of due diligence performed on a client can then be aligned to the level of money laundering risk posed by that client.

Note that KYC and CIV procedures can also be used as the basis for suspicious activity reporting. Regulation 21 requires business entities to obtain sufficient information regarding high risk clients and transactions to enable them to identify potential suspicious transactions. Therefore, they can identify and report suspicious transactions when they know their clients and understand their business.

b. Politically Exposed Persons ("PEPs")

PEPs are defined as individuals who are or have been entrusted with prominent public functions such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials.

Except for banks, there is still no guidance from the FIC as to how this requirement should be dealt with by accountable institutions so it can be incorporated into their procedures. However, by becoming a member of FATF, South Africa committed itself to implement and conform to international standards.

MONEY LAUNDERING LEGISLATIONS IN SOUTH AFRICA

Authorised FSPs are therefore encouraged to implement this requirement from a risk management perspective, and apply proactive measures designed to determine potential suspicious transactions that could possibly emanate from PEPs and report them accordingly.

The issue of PEPs is addressed under FATF's revised Recommendations. In terms of Recommendation 6, accountable institutions must in addition to the normal Customer Due Diligence procedures -

- Have appropriate risk management systems to determine whether the customer in question is a PEP or not;
- Obtain senior management approval for establishing a business relationship with such customers;
- Take reasonable steps to establish their source of wealth and source of funds;
- Conduct enhanced ongoing monitoring of the business relationships with such customers.

Authorised FSPs are required to manage their relationship with PEPs including their family members and other close associates to ensure that those relationships are not abused to launder proceeds of crime.

II. Duty to keep records

Section 22 requires accountable institutions who establish a business relationship or conclude a transaction with a client, to keep records of a single transaction or of additional transactions concluded in the course of a business relationship. It also prescribes full particulars and details of the information that must be kept as records. As in FAIS, records may be kept manually or by electronic means.

i. Record keeping period

Section 23 prescribes the period for which records may be kept. It states that the documents used to identify and verify clients as well as records of all transactions must be retained for a period of at least five years from the date on which the business relationship was terminated.

ii. Outsourcing record keeping:

In terms of Section 24 (1), the record keeping obligation may be outsourced to a third party provided the accountable institution is given free and easy access to these records. Note that outsourcing this function to a third party does not discharge the accountable institution from the record keeping responsibility. Section 24(2) states that the accountable institution will still be held liable for the third party's failure to comply with this obligation.

Section 24(3) stipulates that if the accountable institution appoints a third party to keep records on its behalf, then particulars of the third party keeping records on behalf of the accountable institution must be provided to the FIC. The full particulars and details of the information which must be furnished to the FIC regarding the third party carrying out the record keeping obligation is prescribed under Regulation 20.

iii. Accessibility of records:

In terms of section 26 of FICA, the accountable institution must give an authorised representative from the FIC access and reasonable assistance where necessary to records kept by or on behalf of the accountable institution.

MONEY LAUNDERING LEGISLATIONS IN SOUTH AFRICA

It is important to note that the record keeping obligation can have an impact on Exemption 2 which exempts certain accountable institutions from conducting identification and verification procedures on further transactions concluded in a business relationship. Contrary to this, the record keeping obligation requires accountable institutions to keep records of a single transaction or of additional transactions concluded in the course of a business relationship. Accountable institutions are also required to file reports if there is anything suspicious about these transactions and business relationships.

III. Duty to report Suspicious and Unusual Transactions

The duty to report suspicious and unusual transactions is imposed on all persons who carry on business, are in charge of or manage a business, or are employed by the business.

FICA prescribes different methods of reporting as follows:

- Section 28 reporting of cash transactions involving amounts above a prescribed limit;
- Obligation to report conveyance of cash to or from South Africa in excess of a stipulated threshold in terms of section 30;
- Obligation to report electronic transfer of money to and from South Africa in excess of the prescribed limit in terms of section 31; and
- Section 29 suspicion or unusual based reporting.

The first three types of reporting are not important for purposes of this discussion as the prescribed limits, and the manner in which these reports must be filed have not been determined by the FIC.

i. Suspicious or unusual based reporting:

Section 29 requires all business organisations, their managers and employees of such businesses to identify and report suspicious and unusual transactions to the FIC. Failure to file such a report amounts to an offence that carries a penalty.

ii. Reporting format:

Regulation 22 deals with the reporting format. It states that suspicious transaction reporting can be internet based or by a method developed by the FIC. Full particulars of the information to be contained in the STRs is prescribed under Regulation 23.

iii. Reporting period:

Regulation 24 deals with the reporting period. The report must be sent to the FIC as soon as possible, but no later than 5 days after the suspicious transaction was determined.

iv. Protection of persons filing STRs:

In terms of section 38, persons filing STRs are guaranteed protection against criminal and civil liability for complying in good faith with the provisions of FICA.

In terms of section 33, an accountable institution may continue with the reported transaction unless the FIC specifically orders such a person not to proceed with the transaction.

Note that there are authorised FSPs who continue to submit STRs to the FAIS Department or make enquiries with this Office about the outcome of their reports.

MONEY LAUNDERING LEGISLATIONS IN SOUTH AFRICA

It must be emphasised that STRs are confidential documents that must be submitted directly to the FIC. No one, other than the relevant FIC staff, is supposed to have sight of these reports or know of their existence.

It is important to note that suspicious transaction reporting can have an impact on Exemption 2, which exempts certain accountable institutions from conducting identification and verification procedures on further transactions concluded in a business relationship. Contrary to this, the suspicious transaction reporting obligation requires accountable institutions to file reports of a single transaction or of transactions concluded in the course of a business relationship if the accountable institution has knowledge or reasonable grounds that these transactions and business relationships facilitate money laundering.

IV. Measures to promote compliance with the requirements of FICA

i. Formulation and implementation of internal rules

Section 42 requires accountable institutions to formulate and implement internal rules concerning:

- Client identification and verification;
- Record keeping;
- Steps taken to determine and report suspicious transactions;
- Such other matters as may be prescribed from time to time.

Internal rules must be made available to every employee involved in transactions to which FICA apply, and on request, a copy thereof must be made available to the FIC and relevant supervisory bodies (*Refer to **Regulation 25, 26 and 27** for full particulars of the information that must be contained in the internal rules*).

ii. Training of employees:

Sec 43(1) requires accountable institutions to provide training to its employees to enable them to comply with the provisions of FICA and internal rules applicable to them.

Note that FICA does not prescribe the format of training required. Both formal training and FICA awareness campaigns are recognised. These methods are both designed to raise the level of awareness of employees regarding their obligations. As in FAIS, record of training attended must be kept as proof.

iii. Appointment of a compliance officer:

Section 43(2) requires accountable institutions to appoint a person with a responsibility to ensure compliance by –

- the accountable institution with its obligations under FICA,
- employees of the accountable institution with the provisions of FICA as well as internal rules applicable to them.

Compliance officers appointed in terms of FAIS can be entrusted with the above responsibility. In the absence of a compliance officer, this duty is deeply embedded with the money laundering officer or management.

MONEY LAUNDERING LEGISLATIONS IN SOUTH AFRICA

Prevention of Organised Crime Act 121 of 1998

Objectives of POCA:

- To criminalise racketeering and creates offences relating to activities of criminal gangs;
- To criminalise money laundering and creates a number of serious offences in respect of laundering and racketeering;
- To create a general reporting obligation for businesses coming into possession of suspicious property;
- To create a mechanism for criminal confiscation of proceeds of crime and for civil forfeiture of proceeds;

Money laundering offences under POCA:

POCA creates the following money laundering offences:

- offences involving proceeds of all forms of crime; and
- offences involving proceeds of a pattern of racketeering

Section 2 of POCA deals with a number of offences in connection with receipt, retention, use or investment of proceeds of a pattern of racketeering activity.

The general money laundering offences that are created under POCA are dealt with under sections 4, 5 and 6 as follows:

Section 4 deals with offences relating to knowing or ought reasonably to have known.

A person who knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities, commits an offence in terms of section 4, if he enters into any agreement, arrangement or transaction in connection with the property, (whether legally enforceable or not); or performs any other act in connection with the property (whether independently or in conjunction with another person), which has the effect or is likely to have the effect:

- of concealing or disguising the nature, source, location disposition, movement and ownership of this property including interest therein; or
- of enabling or assisting a person who committed an offence to avoid prosecution, or remove property such property.

Section 5 deals with offences for assisting another person to benefit from the proceeds of unlawful activities. It states that a person commits an offence if he knows or ought reasonably to have known that another person has obtained the proceeds of unlawful activities, and enters into a transaction, agreement, or arrangement in terms of which:

- the retention, or control by or on behalf of that other person of the proceeds of the unlawful activity is facilitated; or
- the proceeds are used to make funds available to that person, to acquire property on his behalf or to benefit him in any other way.

Section 6 deals with the acquisition, possession or use of proceeds of unlawful activities. It states that a person who acquires, uses, or possesses property and who knows or ought reasonably to have known that it is or forms part of proceeds or unlawful activities of another person shall be guilty of an offence.

FINDINGS OF THE RECENT FICA THEME VISITS

Introduction

Recently, the FAIS Supervision Department conducted FICA theme visits to a number of authorised FSPs. The objective was to assess the FSPs' level of compliance *vis a vis* the combating of money laundering and the financing of terrorist activities. A standard questionnaire with a set of predetermined questions was used to carry out these assessments.

During the visits, the focus was not on exposing non-complying FSPs, but rather to gauge how the industry was making effort to comply and assist them to identify specific areas where it was felt deserved further attention.

A remarkable response was received from the industry, considering the number of years that FICA has been in operation, and the fact that the majority of the FSPs are regulated for the first time under FAIS. To this end, we wish to extend our warmest appreciation to all FSPs who participated in these assessments.

It is important to note that the assessments were not only confined to compliance with money laundering legislations. Due to a holistic view being adopted, findings relating to other pieces of legislation were also noted and raised accordingly with the FSPs. The findings were grouped and summarised under FICA, FAIS and general good business practice.

The assessments covered the following key topics:

(a) Compliance structures in respect of AML/CFT

(b) Identification and verification procedures

(c) Record keeping procedures

(d) Training structures in respect of FICA and other AML/CFT

(e) A risk based approach in respect of policies and procedures regarding –

- Non face to face clients
- The identification and reporting of suspicious and unusual transactions
- The verification of clients' source of income and/or funds
- The identification and management of relationships with Politically Exposed Persons

(f) Policies and procedures in respect of the risk management framework

(g) Establishment and implementation of internal rules

A total of 170 FSPs were visited over a four-month period in two separate phases as follows:

- The first phase saw 33% of the FSPs being visited.
- The remaining 67% were assessed in phase two

Of the 170 visits undertaken, 7% were High Impact FSPs, 31% Medium Impact and 62% consisted of Low Risk FSPs.

FINDINGS OF THE RECENT FICA THEME VISITS

The common findings observed during the visits were summarised and are discussed below. These issues were raised with the individual FSPs and were rectified. Authorised FSPs are therefore encouraged to pay special attention to them.

1. FICA FINDINGS

(a) Full compliance with FICA

Most of the FSPs who were found to be fully compliant with all the provisions of FICA were predominantly from the High and Medium Impact sectors. The success was to a large extent attributed to senior management being more engaged in and taking active interest in money laundering activities. These FSPs had a strong compliance culture in place that was driven by top management and was shared by all employees at the lower levels of the hierarchy.

(b) Non-compliance with the FICA

Only 2% of the FSPs visited were found not to have made any concerted effort at all to comply with FICA. Some of those interviewed indicated that they were either in the process of retiring or wanted to quit the financial services industry due to the alleged high costs of compliance or burden of too much regulation.

The non-compliant FSPs were afforded the opportunity to rectify the situation. They will be visited again this year when the risk based onsite visits commence.

(c) Failure to establish and verify the identities of new clients

Some of the FSPs failed to carry out the identification and verification measures to new clients in contravention of section 21(1) of FICA and did not qualify for an exemption. In many instances, it was found that the FSPs failed to obtain relevant documents prescribed in terms of FICA from new clients, or accepted questionable copies of documents such as copies of IDs from clients that were either not certified or were not endorsed as having been sighted as part of the verification process.

Authorised FSPs are encouraged to desist from concluding transactions or entering into business relationships with new clients without taking the necessary steps to ensure that proper identification and verification procedures are carried out.

(d) Failure to establish and verify the identities of existing clients

There were FSPs who failed to meet the 30 June 2004 deadline, in that they failed to verify the identities of existing clients who concluded further transactions in the course of a business relationship since FICA took effect, and did not qualify for an exemption. It was found that certain verification documents prescribed in terms of FICA in respect of business written before FICA came into operation was not on file.

FINDINGS OF THE RECENT FICA THEME VISITS

Most of the FSPs interviewed indicated that they have not succeeded to meet this requirement because;

- Their clients were unable to provide information or documentation which could serve to verify their particulars.

- The time spent and costs involved in obtaining the documents were discouraging. Many FSPs were focusing on writing new business and/or servicing existing clients, and had not devoted some time to carry out this exercise.

- They had long standing and close personal relationships with their clients, hence it was deemed not necessary for them to perform the required KYC and CIV procedures as these clients were all known to them.

- Some of their clients were uncooperative, and in some cases there were no appropriate means in place that could be utilised to compel them to provide the information.

If not exempted, the identification and verification procedures should be carried out for further transactions concluded in the course of the business relationships even if these were entered into prior to 2001. The affected FSPs were encouraged to make thorough follow ups on these documents and were advised to ensure that reminders in that regard were sent out more frequently.

(e) Failure to attend FICA training by employees

Some of the FSPs visited had not attended FICA training envisaged under section 43 of FICA or failed to provide formal training to employees engaged in business transactions to which FICA apply.

The FSPs that failed to meet this requirement indicated that they were inundated with too much regulation or were either too old or busy to study.

Note that untrained employees could lag behind when changes to the legislation take place. They could also fail to implement all the obligations contemplated under FICA and fail to combat money laundering effectively.

Training should be provided to all employees dealing with business transactions to which FICA apply to ensure that they keep abreast of developments. Refresher courses can also be attended regularly, and can incorporate amendments to FICA, Exemptions, Regulations and any new Guidance Notes that could be issued from time to time.

(f) Failure to keep records of training attended

Still on the subject of training, there were certain FSPs who alleged to have attended training but could not provide records of such training as proof. Some indicated that their businesses were too small and they knew what FICA entailed, hence it was not necessary to attend training.

Failing to keep records of training attended amounts to a contravention of section 18 of FAIS as well as section 22 of FICA.

It is recommended that proof of all training attended by employees be recorded in a training register as this is also a requirement under FAIS. This will add credibility to the business of the FSPs. Training manuals and certified copies of certificates can also be kept in line with the FAIS compliance framework.

FINDINGS OF THE RECENT FICA THEME VISITS

(g) Failure to have separate procedures for non face-to-face clients

Another common observation was that FSPs were entering into non face-to-face business transactions with clients in addition to the normal business scenario involving direct interaction with clients, but did not have separate procedures to carry out this type of business. This resulted in situations such as uncertified copies of ID documents being faxed and accepted by some of the FSPs.

The implication of this is that there is no consistency as employees follow different procedures to sign new clients. Regulation 18 of the FICA Regulations states that accountable institutions must apply customer identification measures to non face to face clients that are as effective as those applied to customers who were available for interview. It also stipulates that adequate measures must be applied to mitigate the higher risk applicable to this type of business.

Authorised FSPs are encouraged to establish and document client acceptance procedures, and make them available to all employees to ensure that they are aware of the procedures to be followed prior to accepting new clients. These procedures must provide for business transactions concluded on-line and must stipulate the detailed step by step verification measures to be followed.

(h) Failure to have procedures for dealing with STRs

Some of the FSPs visited were not aware of this obligation and did not have appropriate internal controls and procedures in place to deal with this matter internally, and ensure that STRs are generated and furnished to the FIC.

Failure to have procedures for dealing with, generating and reporting suspicious transactions amounts to a contravention of section 29 of FICA. This could create the impression that FSPs colluded with clients to assist them to launder money, and could have a negative impact on their reputation.

A formal documented policy and/or procedure for dealing with suspicious or unusual transactions must be put in place. The reporting format prescribed by the FIC must be used. This will ensure that in the unlikely event that the FSP cannot continue business, the successor will be aware of the procedures to be followed in respect of this requirement, thus ensuring business continuity.

(i) Failure to verify clients' source of income and funds

It was noted from the visits that most of the FSPs failed to obtain particulars concerning the clients' source of income and/or source of funds involved in a particular transaction or business relationship.

FINDINGS OF THE RECENT FICA THEME VISITS

In terms of Regulation 21, this requirement can assist the accountable institutions to determine whether transactions involving a client are consistent with their knowledge about that client or whether the transactions fit the client's profile. This requirement helps to mitigate the risk of money laundering and can be applied as a proactive measure from a risk management perspective.

Authorised FSPs are encouraged to consider verifying clients' source of funds or income. This will assist them to embark on a robust approach and become vigilant towards the identification of proceeds of unlawful activities, file reports and combat money laundering activities.

(j) Failure to risk profile clients

A significant number of the FSPs were not following a risk based approach in respect of the identification and verification of clients' information. Clients and business transactions were not classified into risk categories in terms of the potential risk they posed to the business. Higher risk clients and transaction were therefore not subjected to an intensive Customer Due Diligence process.

As mentioned earlier, the concept of risk profiling stems from Regulation 21 of the FICA Regulations which advocates building client profiles. Applying a risk based approach to the verification of the relevant particulars implies that the FSP will be better placed to accurately assess the potential risks. The FSP will also be able to make an informed decision based on its risk assessment as to the appropriate methods and levels of verification that should be applied in a given circumstance.

Going forward, FSPs are encouraged to incorporate risk profiling procedures into their processes. Risk profiling clients can yield positive results for the FSP. Applying different CDD procedures for the different types of clients can assist the FSP to identify and mitigate potential risks, hence reducing or preventing money laundering risk.

FSPs are further encouraged to consider aligning their CDD procedures to the potential level of money laundering risk posed by each client. High risk clients must be subjected to a detailed and higher degree of due diligence than low risk clients.

(k) Failure to have procedures for dealing with PEPs

The majority of the FSPs interviewed did not have documented procedures or policies in place to deal with PEPs and their related ones. Many pleaded ignorance and apportioned the blame to the lack of guidance on this matter.

Note that FSPs who correctly identify PEPs and their relatives, and apply the necessary procedures before signing them, can reduce the risk of their businesses being utilised to launder and conceal proceeds of illegal activities and other undisclosed business interests including gifts.

"PEPs" are categorised as high risk clients. FSPs must consider establishing and documenting a client acceptance manual and incorporate it into needs analysis procedures.

FINDINGS OF THE RECENT FICA THEME VISITS

The client acceptance procedure must contain the requirements for dealing with “PEPs”. The procedures must be documented and made available to all employees, to ensure that they are aware of the procedures to be followed prior to accepting new clients.

(l) Failure to formulate and implement internal rules

Another common finding was that some of the FSPs visited did not have internal rules in place. Some have shown no complete understanding of these rules as they only kept them on file in order to comply.

Failure to have internal rules amounts to a contravention of section 42 of FICA. Awareness must also be created amongst employees involved in transactions to which FICA apply about these internal rules.

(m) Utilisation of generic documentation

Most of the FSPs utilised a standard risk management plan, internal rules, or similar documents. In most cases, these were generic documents drafted by the external compliance officers or broker networks and were furnished to all FSPs to whom a compliance service was rendered.

There was no concerted effort on the part of the FSPs to customise the documents in line with their business needs. In some instances the documents were placed on file and the FSPs together with their employees had no idea as to what they entailed. Generic documents contain a lot of information, some of which may not be relevant to the type of business carried out by certain types of FSPs.

Some of this information may be confusing to staff. Management must ensure that the documents referred to above are customised. They must further ensure that they are simplified and easy to understand by all employees. The documents should be tailor made to suit the operations and business needs of the FSP. All employees engaged in transactions to which FICA apply must be made aware about the existence and contents of these documents.

2. FAIS FINDINGS

(a) Dormant FSPs with unutilised licences or financial products

During the visits, there were FSPs who were dormant and had not rendered any financial services since being issued with a licence or had unutilised financial products on their licences.

Having a FAIS licence and being dormant at the same time, could lead to clients being misled as the FSP might utilise the licence to engage in unregulated activities or sell unregulated products. This could create the impression that these activities or products are regulated by the FSB.

Unutilised licences must be surrendered to this Office. The licences of dormant FSPs were lapsed in terms of section 9 of FAIS. The licence conditions of those FSPs with unutilised financial products were amended to cancel unutilised products. Going forward, FSPs are encourage to inform this Office if they are no longer rendering financial services or are authorised for certain financial products that they are not rendering services on.

FINDINGS OF THE RECENT FICA THEME VISITS

(b) Failure to establish a compliance function/framework

Another common observation is that there were FSPs, especially from the low risk impact, who still did not have a compliance function envisaged under section 17 of FAIS. There was an incorrect perception on their part that since they were not required to appoint a compliance officer, there was no need on their part to establish and maintain a compliance framework.

Failure to establish a compliance function as part of the risk management framework can lead to withdrawal of authorisation to act as an FSP.

(c) Failure to submit statutory returns and compliance reports

We also came across FSPs who did not comply with the provisions of section 17 and/or 19 of FAIS as they had not submitted the financial statements and compliance reports from 2005 to 2007. Most of them alleged that they were not simply aware of this requirement, as they were not informed by their compliance officers.

Failure to submit statutory returns and compliance reports creates a serious risk to clients, and the Registrar is entitled to take further regulatory steps which could include suspension or withdrawal of the licence of non complying FSPs. These FSPs can also be subjected to penalties.

(d) Failure to have internal controls

There were also certain FSPs who did not have internal controls in place. Paragraph 12 of the General Code of Conduct advocates the establishment of the internal controls and control objectives. These controls assist the FSP to conduct business in an orderly manner. They also provide reasonable assurance on the safety, effectiveness and efficiency of the institution's operations and compliance with requirements. Failure to have internal controls poses a serious risk to clients and other stakeholders. They could suffer potential losses as a result of theft, fraud, dishonesty, negligence, poor administration, misconduct etc.

Authorised FSPs are encouraged to consider establishing and maintaining internal controls as part of the risk management framework. This will assist them to identify potential risks and mitigate them. Depending on the size of the business, the internal controls can also be audited.

(e) Failure to have a gift policy or gift register

Some of the FSPs visited did not have policies in place with regard to the treatment and disclosure of gifts. Paragraph 3(1)(c) of the General Code of Conduct advocates disclosure of non cash incentives and other indirect considerations. Gifts could be perceived as a token of appreciation on the part of clients for receiving assistance from FSPs to launder proceeds of illegal activities. This could have a negative impact of the FSP's reputation.

FINDINGS OF THE RECENT FICA THEME VISITS

Authorised FSPs are encouraged to document policies for handling gifts and must circulate it to all employees. A gift register can also be kept to record all gifts received from clients.

(g) Failure to have a risk management plan

Another common finding was that most of the FSPs did not have a documented risk management plan to address all potential risks that could impact on the day-to-day business operations as required under section 11 of the General Code of Conduct. The risk management plan must spell out all the potential risks faced by the institution, and must also prescribe the procedures to be followed in order to mitigate or manage them.

This document is important for the successful running of a business institution. It sets out the expectations of management and contains tools and techniques to identify, measure, monitor and control potential exposures to risks that could impact on the viability of the business.

Going forward, FSPs are encouraged to prepare a risk management plan that is simplified and easy to understand by all employees. It should address all types of potential risks that could affect the running of the business.

(h) Failure to have backup facilities or keep clients' records offside

There were also FSPs who had no proper or adequate facilities in place to ensure client information was backed up frequently, or did not store clients' records offside. Thus in case of a disaster, the continuity of business could be seriously affected. It was noted that some FSPs did backups once a week, and this posed a serious risk of clients' information being lost.

Some FSPs kept backups onsite and had no alternative plans to keep copies of backups offsite. Security of information, backups and recovery procedures are very crucial. Important client information must be backed up. FSPs must have contingency and recovery plans in place that enable it to resume operations offsite in a reasonable time if disaster strikes or primary location shuts down.

(i) Failure to safeguard clients' records and prevent unauthorised access

We also came across FSPs who did not have measures in place to control access to records and clients' information on the system. In most instances, computers had no passwords and there was no audit trail. This posed a serious risk of clients information being changed or wiped out, thus accountability was questionable.

Failure to control access to clients' information poses a serious risk and could impact on the confidentiality and secrecy requirements advocated under paragraph 3(2) of the General Code of Conduct, as well as on record keeping obligations.

(j) Failure to consider electronic record keeping as an alternative means of keeping records

A significant number of FSPs kept all clients' information and other records physically in the filing cabinets or store rooms with no backups. They had no computers or IT facilities to consider electronic recordkeeping or keeping physical records outside the premises. Note that destruction of hard copy files intentionally or accidentally could impact on the continuity of the business as it could be difficult to retrieve lost information.

FINDINGS OF THE RECENT FICA THEME VISITS

Electronic record keeping should be considered as an alternative in order to lower the risk. FSPs may create electronic back-ups and store them off-site.

3. GENERAL FINDINGS

(a) Failure to have segregation of duties and functions

There should be independent oversight of all major business activities and reasonable separation of operational duties and functions. There were FSPs who did not have organisational and functional charts spelling out segregation of responsibilities to avoid a conflict of interests. The implication of this is that employees might not be aware of the necessary reporting requirements, leading to confusion that could otherwise be avoided.

Good business practice advocates for the drawing up of the organogram setting out the reporting lines. Functional charts must also be drawn up to specify segregation of duties and responsibilities. These charts can also serve as key performance indicators for current and future employment positions.

These controls will ensure that employees are held accountable for their actions. The charts must be drawn up for all existing positions.

(b) Failure to have a documented succession plan

An overwhelming number of FSPs did not have a documented succession plan, depicting the way forward in the event of some form of demise befalling the current key individuals. In most instances, the FSPs had some informal verbal arrangements in place with other family members, friends or fellow business associates.

Failure to have a succession plan could impact negatively on the continuity of the business which could cause unnecessary inconveniences to clients. FSPs are encouraged to incorporate succession or contingency plans in their procedures for ease of handling clients' business in the event of a tragedy. This must be implemented from a risk management perspective and in the best interests of clients.

(c) Failure to have a documented business plan

Most of the FSPs had no business plan in place. Some indicated that the business plan was not documented because they knew their businesses fairly well. In the event of new business partners and employees coming on board, they may not be aware of the goals, objectives and expectations of management, resulting in them working to achieve different goals. They could also utilise different procedures to achieve organisational objectives. This could also create confusion to employees and affect performance management. A business plan must be documented and copies thereof must be made available to all employees.

(d) Failure to have client acceptance procedures

Another common finding was that there were FSPs who did not have a client acceptance procedure. This could lead to a situation where prescribed verification documents being obtained. FSPs are encouraged to have a detailed document setting out the steps that must be followed prior to signing new clients, including KYC principles and sign off by a different person.

IMPORTANT DEFINITIONS AND GLOSSARY

''*Business relationship*'' means an arrangement between a client and an accountable institution for the purpose of concluding transactions on a regular basis.

"*Pattern of racketeering*" refers to the planned, ongoing, continuous or repeated participation or involvement in any offences referred to Schedule 1 of POCA.

''*Single transaction*'' means a transaction other than a transaction concluded in the course of a business relationship.

''*Transaction*'' is defined in section 1 of FICA as meaning "a transaction concluded between a client and the accountable institution in accordance with the type of business carried on by that institution". Please refer to ***Guidance Note 2*** for a detailed definition of transaction in relation to client identification, examples of transactions, the type of activities which might be regarded as transactions, and the exclusions of certain acts from the ambit of transaction.

GLOSSARY OF TERMS

AML/CFT	Anti Money Laundering and Combating the Financing of Terrorist activities
CIV	Client Identification and Verification
CDD	Customer Due Diligence
FAIS	Financial Advisory and Intermediary Services Act, No. 37 of 2002
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act, No. 38 of 2001
FSB	Financial Services Board
FSP	Financial Services Provider
PEPs	Politically Exposed Persons
POCA	Prevention of Organised Crime Act, No. 121 of 1998
KYC	Know Your Client
STR	Suspicious Transaction Report

WHAT IS NEW?

FOR YOUR INFO

1. The FAIS compliance report has been published. All Category I FSPs with compliance officers must submit reports by 15 August. For more information refer to our website.
2. Amendments to the General Codes were published in April. FSPs should familiarise themselves with these new disclosure requirements which include an obligation on FSPs to at least on an annual basis to report to clients.
3. The date on which levies will be calculated will change to 31 August 2008 and the levy will be payable by 31 October 2008. A general circular will be send to all FSPs.
4. The FSB has consulted for the past 18 months on changes to the Determination of Fit and Proper requirements and final consultation on proposed draft is under way. All industry bodies were invited to comment on the new proposals that will be effective from the end of 2008. More details will be send to all FSPs later during the year.

CONTACT DETAILS

Physical address:
Kasteel Park
Nassau Building
Jochemus Avenue
Erasmuskloof
Pretoria

Telephone : (012) 428-8145
Facsimile : (012) 422-2973
Website : www.fsb.co.za

Postal address:
Registrar of Financial Services
P O Box 35655
Menlopark
0102

COMMENTS & SUGGESTIONS

We invite comments on this Newsletter and suggestions as to which topics you wish us to address in the coming publications. Any person who wishes to be included in the FAIS Newsletter circulation must forward an e-mail to faiscomment@fsb.co.za. The FAIS Newsletter is for free.

FSB Contact Centre: Are you aware that the Financial Services Board is dedicated to resolving all your queries? The following toll free numbers may be used to contact the FSB Contact Centre:

0800110443 or 0800202087

Per e mail: info@fsb.co.za

Website: All the important information applicable to financial services business is posted on our website. You are encouraged to frequently visit our website for latest information and updates. Our website address is www.fsb.co.za. On the homepage click on the word "FAIS".

DEO AND SUPPORT

Name	Title	Telephone	E-mail Address
Gerry Anderson	Deputy Executive Officer: Market Conduct and Consumer Education	012-428 8114	gerrya@fsb.co.za
Denise Wolfe-Botha	Executive Secretary	012-428 8119	denisew@fsb.co.za
Loraine Van Deventer	Legal Advisor	012-428 8178	lorainew@fsb.co.za
Noxolo Nkebe	Receptionist	012-428 8145	noxolon@fsb.co.za

FAIS ENFORCEMENT DEPARTMENT

Name	Title	Telephone	Email Address
Manasse Malimabe	Head: FAIS Enforcement	012-428 8137	manassem@fsb.co.za
Adri Jansen van Vuuren	PA to Manasse Malimabe	012-428 8058	adriv@fsb.co.za
Lesedi Letwaba	Manager	012-428 8176	lesedil@fsb.co.za
Tshepo Mogale	Senior Analyst	012-367 7271	tshepo@fsb.co.za
Buzwe Mfikili	Analyst	012-367 7265	buzwe@fsb.co.za
Diphapang Molope	Analyst	012-428 8139	diphapang@fsb.co.za
Constance Dibakwane	Analyst	012-428 8056	constanced@fsb.co.za
Lawrence Muravha	Analyst	012-367 7288	lawrencem@fsb.co.za
Maud Mazibuko	Analyst	012-367 7291	maudm@fsb.co.za
Prince Nemutanzhela	Analyst	012-367 7289	princen@fsb.co.za
Dineo Motswakae	Admin Assistant	012-367 7290	dineom@fsb.co.za

FAIS SUPERVISION DEPARTMENT

Name	Title	Telephone	Email Address
Wendy Hattingh	Head: FAIS supervision	012-428 8101	wendyh@fsb.co.za
Thabile Mahlangu	PA to Wendy Hattingh	012-428 8139	thabilem@fsb.co.za
Tefo Moatshe	Manager	012-428 8098	tefom@fsb.co.za
James Molefe	Manager	012-428 8087	jamesm@fsb.co.za
Charene Nortier	Manager	012-428 8054	charenen@fsb.co.za
Ronel Reyneke	Specialist Analyst	012-422 2809	ronelr@fsb.co.za
Julia Matebane	Senior Analyst	012-428 8059	juliam@fsb.co.za
Brenda Morty	Senior Analyst	012-428 8181	brendam@fsb.co.za
Diketso Mashigo	Senior Analyst	012-367 7279	diketso@fsb.co.za
Nare Setati	Senior Analyst	012-428 8079	nare@fsb.co.za
Bonolo Nare	Senior Analyst	012-367 7274	bonolo@fsb.co.za
Nelize Goch	Analyst	012-428 8110	nelize@fsb.co.za
Unathi Mbanga	Analyst	012-422 2874	unathi@fsb.co.za
Puseletso Mogapi	Senior Analyst	012-367 7255	puseletsom@fsb.co.za
Moses Maleka	Analyst	012-422 2895	moses@fsb.co.za
Lesego Malehopo	Analyst	012-367 7297	lesegom@fsb.co.za
Thiro Moodliyar	Analyst	012-367 7275	thiro@fsb.co.za
Dash Pillay	Analyst	012-367 7296	dashentranp@fsb.co.za
Martha Swart	Analyst	012-367 7285	marthas@fsb.co.za
Yanda Molefe	Junior Analyst	012-367 7276	yandam@fsb.co.za
Wendy Louw	Junior Analyst	012-367 7273	wendyl@fsb.co.za
Annie Nkewu	Analyst	012-422 2897	annien@fsb.co.za
Mpho Sesele	Junior Analyst	012-367 7272	mphos@fsb.co.za
Yvonne Ngwenya	Junior Analyst	012-367 7262	yvonnen@fsb.co.za
Mfundo Xoko	Analyst	012-422 2848	mfundox@fsb.co.za
Tladi Molebatsi	Analyst	012-422 2872	tladim@fsb.co.za
Sam Matabane	Junior Analyst	012-367 7254	chikane@fsb.co.za
Stephan Kemp	Junior Analyst	012-367 7295	stephank@fsb.co.za
Phuti Senyatsi	Admin Assistant	012-367 7257	phuti@fsb.co.za
Itumeleng Nnene	Admin Assistant	012-367 7260	itumelengn@fsb.co.za

FAIS SUPERVISION DEPARTMENT (CONT)

Name	Title	Telephone	Email Address
Freddy Tshwana	Analyst	012-367 7286	freddyt@fsb.co.za
Pieter Oosthuysen	Analyst	012-367 7298	pietero@fsb.co.za
Dhanesh Sukdea	Senior Analyst	012-367 7287	dhaneshs@fsb.co.za
Steve Chitwa	Department Assistant	012-367 7254	stevec@fsb.co.za
Genevive Abrahams	Admin Clerk	012-367 7263	genevivea@fsb.co..za
Yolande Wepener	Admin Clerk	012-367 7268	yolandew@fsb.co.za
Meshack Magavha	Admin Assistant	012-367 7261	meshackm@fsb.co.za
Akashen Rampesadh	Admin Assistant	012-367 7292	akashenr@fsb.co.za

FAIS REGISTRATION DEPARTMENT

Name	Title	Telephone	E-mail Address
Felicity Mabaso	Head: FAIS Registration	012-428 8186	felicitym@fsb.co.za
Thabile Mahlangu	PA to Felicity Mabaso	012-428 8139	thabilem@fsb.co.za
Jabhile Mbele	Manager	012-428 8047	jabhile@fsb.co.za
Thoko Magagula	Senior Analyst	012-367 7269	thoko@fsb.co.za
Khehla Mavuso	Senior Analyst	012-367 7270	khehla@fsb.co.za
Innocentia Sibambo	Analyst	012-428 8089	innocentias@fsb.co.za
Michelle Fourie	Analyst	012-428 8145	michellef@fsb.co.za
Marianne Horne	Analyst	012-367 7282	marianneh@fsb.co.za
Janet Smit	Analyst	012-422 2880	janet@fsb.co.za
Karien Nel	Analyst	012-428 8147	karien@fsb.co.za
Constance Masilela	Analyst	012-428 8198	constanm@fsb.co.za
Thembi Mthenjane	Junior Analyst	012-422 2879	thembim@fsb.co.za
Johannes Nkutshweu	Junior Analyst	012-428 8185	johannesn@fsb.co.za
Phillipine Munyai	Analyst	012-422 2860	phillipinem@fsb.co.za
Moloko Rabosiwana	Analyst	012-422 2975	molokor@fsb.co.za
Hopolang Thupana	Junior Analyst	012-422 2974	hopolangt@fsb.co.za
Ruby Mosime	Analyst	012-367 7251	rubym@fsb.co.za
Genevieve Miles	Admin Assistant	012-422 2904	genevivem@fsb.co.za

FAIS REGISTRATION DEPARTMENT (CONT)

Name	Title	Telephone	E-mail address
Trishen Foolchand	Admin Clerk	012-367 7253	trishenf@fsb.co.za
Moses Mthimunye	Admin Clerk	012-367 7284	mosesmu@fsb.co.za
Ephy Sebopa	Admin Clerk	012-367 7258	ephy@fsb.co.za
Monni Mapheto	Admin Clerk	012-422 2849	monni@fsb.co.za
Solomon Sefako	Admin Clerk	012-367 7256	solomons@fsb.co.za
Matthews Ntlatleng	Admin Clerk	012-428 8191	matthewsn@fsb.co.za
Thabang Marokane	Admin Clerk	012-367 7280	thabang@fsb.co.za
Isaac Lebese	Admin Clerk	012-367 7253	isaacl@fsb.co.za