BANKING SECTOR MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

SOUTH AFRICAN RESERVE BANK
Prudential Authority

Produced by the Publishing Section of the South African Reserve Bank

Executive summary

The Prudential Authority (PA) of the South African Reserve Bank (SARB) is responsible for anti-money laundering (AML) and combating the financing of terrorism (CFT) supervision of banks, mutual banks and life insurers. The PA has to ensure that the aforementioned accountable institutions (AIs) comply with the requirements of the Financial Intelligence Centre Act 38 of 2001, as amended (FIC Act).

1 AML/CFT inspections are conducted in terms of section 45B of the Financial Intelligence Centre Act 38 of 2001, as amended.

The money laundering (ML) and terrorist financing (TF) banking sector risk assessment (SRA) was compiled by the PA to assist it in the furtherance of its understanding of ML and TF risk within the banking sector in South Africa. This SRA thus reflects the ML/TF risks identified within the banking sector during 2018 and 2019.

Through the distribution of a survey and interacting with banks directly, the PA sought to ascertain the banks' understanding of the ML/TF inherent risk and control risk in its environment. The SRA did not take into consideration the holistic residual risk rating afforded by means of the questionnaire, as this was not deemed completely reflective of the effectiveness of the controls that needed to be considered by the PA.

The PA considered its own ratings held in respect of banks via its risk-based tool. The quantitative data was overlaid with the information that the PA had available in respect of AML/CFT inspections that had been conducted, and included considerations of the highlighted threats and vulnerabilities impacting upon the banking sector that have emerged in recent years. The threats and vulnerabilities within the sector that have been taken into account are based on available data, information supplied by banks and research conducted by the PA. With reference to international best practice documentation, ratings of either very high, high, medium or low risks were assigned to respective areas. The SRA provides an assessment of ML/TF risks and identifies key ML/TF vulnerabilities within the banking sector.

With regard to the use of cash products, some banks responded in the affirmative that products offered by the bank were cash intensive. Few banks responded that there were products on offer that did not necessarily have a limit on the amount of money that could be withdrawn as cash abroad. It would seem that the South African banking sector does offer products that enable the facilitation of cash pay-outs or withdrawals, which seem to align with certain perceptions that South Africa is a cash-intensive economy. The identification of unusual or suspicious activities within businesses that are banked as clients and are cash intensive may be more difficult to detect if there is insufficient information held in respect of these entities.

It is important to note that the risk ratings assigned should not be construed as an indication of the financial strength and/or stability of any bank within the banking sector.

Following the gathering of information, research conducted, as well as the responses to the risk assessment surveys and other statistical data requests from banks, it is evident that the overall risk rating would be of medium to high risk. The overall risk rating took into account what has transpired in South Africa over the years, as well as specific threats and vulnerabilities facing the sector, the materiality of the sector in terms of size, and the volume of transactions and sum of money flowing through banks.

Key observations

Some of the key observations are as follows:

- Completeness of client information captured on banks' systems should be ensured, as this might impact on banks' ability to understand their organisational ML/TF risks.
- The ability of banks to obtain beneficial ownership (BO) information in respect of clients is not always straight-forward, which affects the ability of banks to comply with their compliance obligations in terms of the FIC Act. In other cases, a bank may on-board an inter-vivos trust or facilitate a transaction to or from these clients; this provides an opportunity for money

launderers to transfer wealth from one person's estate to another, and to conceal the identity of the true source of funding received by beneficiaries.

- The on-boarding of clients within complex group structures and understanding who an ultimate controller is (not necessarily an owner) also presents difficulty for some banks in terms of obtaining beneficial ownership information.
- Of the 34 banks, 18 indicated that they have terminated or restricted banking relationships with a particular geographical area regarded as presenting an unacceptable level of ML/TF risk.
- In terms of suspicious and unusual transaction reporting, the majority of banks have automated transaction monitoring systems; however, some banks mentioned that there may be improvement required to enhance rules or increase system effectiveness/efficiency.
- Correspondent banking relationships are important for South African banks, and South African banks processing payments on behalf of foreign banks must ensure that they conduct adequate due diligence in respect of the bank on behalf of whom they process transactions.
- Certain banks that offer trade finance services do screen goods against dual-use goods lists, and investigations do occur where appropriate.
- Based on information received, the following shows those industries which banks have exposure to:

No.	Industries	No. of banks per industry	Percentage of high exposure industries
1	Charities and/or non-profit organisations	18	58%
2	Real estate agents	8	26%
3	High-value goods dealers	11	35%
4	Intermediaries/commission agents	9	29%
5	Agriculture and/or forestry	10	32%
6	Mining and quarrying	13	42%
7	Money services bank (MSB)	4	13%
8	Precious metals and stone dealers	12	39%
9	Utilities	9	29%
10	Another country	9	29%
11	Information and communication	22	71%
12	Shipping	21	68%
13	Transport	14	45%
14	Casinos, including the internet gambling	4	13%
15	Arms dealers	8	26%
16	Private military firms	6	19%
17	Digital/virtual currency providers	3	10%
18	Gas sector	9	29%
19	Healthcare and pharmaceuticals	13	42%
20	Manufacturing of dual-purpose goods	12	39%
21	Atomic power	6	19%

Vulnerabilities mentioned

- The use of cryptocurrencies, specifically persons using the system to convert digital to legal tender (currency);
- Having many systems in place, but poor functioning of systems that limits the ability of a bank to have a single-client view;
- Systems which do not enable system continuity and stability;
- Lack of automated controls to address ML/TF risks;
- Products and services offered which are linked to a cash-based economy;
- The non-face-to-face nature of certain products that increases the risk posed to an institution;
- Limited resources and capacity constraints;
- The difficulty in obtaining beneficial ownership information;
- The offering of advance payment trade;
- Inadequate information sharing between financial institutions;
- Incorrect risk profiling of persons;
- The increase in the propensity for fraud due to on-boarding via digital means;
- The inability of an institution to conduct customer due diligence as required; and
- The susceptibility of a bank to becoming a victim of cybercrime.

Risk events observed

- Not identifying the abuse of the single discretionary allowance;
- Internal fraud, including unauthorised activities;
- External fraud;
- Laundering of funds linked to bribery and corruption;
- Clients conducting business below the respective thresholds with the purpose of evading detection;
- Operation of ponzi and pyramid schemes;
- Activities of criminal syndicates, including the use of mule accounts and third-party accounts;
- The abuse of non-face-to-face verification procedures;
- Failure to provide effective, timely training to all employees;
- State-capture investigations;
- The VBS Mutual Bank scandal;
- The Panama and Paradise Papers;
- The abuse of cryptocurrencies;
- The abuse of card-related products;
- Product and information technology (IT) development;
- IT system security that is breached or circumvented by third parties; and
- Process or IT system failures resulting in transactions and/or clients not being adequately screened.

The importance of effective suspicious and unusual detection cannot be overemphasized. Effective alert investigations will also play a pivotal role in detecting reportable suspicious transaction or activity reports, and will ensure resources utilised are dealing with high-quality alerts for investigation as opposed to numerous false positives.

Customer due diligence is important as it will enable banks to identify outlying activity versus normal and expected activity regarding the profile of a customer. It is equally important to ensure that the due diligence measures undertaken by banks, once a domestic prominent influential person (DPIP) is identified, occurs as swiftly as possible to allow for the creation of a profile in respect of a DPIP, to enable the early detection of unusual or suspicious activity.

It would be beneficial for South African banks if they were to have access to a publicly available national list that reflects the relevant details of individuals or entities that conclude contracts with pertinent government departments. The limited databases and public information on DPIPs and their relatives and/or close associates may create identification and risk-rating challenges for banks.

Understanding the source of funds used by a client, as well as obtaining accurate information regarding the nature and purpose of business relationships held with a bank is a critical contributing factor enabling one to identify suspicious or unusual activity that is reportable.

Rating

This rating of medium to high risk is a rating for a point in time and it is possible that the rating will change in due course given that the government has increased its focus and efforts to address matters of corruption and state capture. Banks are required to mitigate risks they are aware of and to be vigilant in this regard. Being able to detect suspicious and unusual transactions effectively and as early as possible, and reporting these timeously to the FIC will enable the eventual desired result and promote the objectives of the FIC Act.

The introduction of the application of a risk-based approach as evidenced in the recent amendments to the FIC Act will see banks being supervised with a view to determine how key risk areas have been identified and if there are effective controls in place to manage and mitigate such risks. Once second-round inspections have been conducted for all banks, the PA will be in a better position to provide insight on whether there has been an improvement in the AML/CFT controls employed by banks.