Suruhanjaya Sekuriti
Securities Commission
Malaysia

The Reporter

2024 Issue

Executive Summary

CONTENTS

With the welfare of investors at the forefront of the Securities Commission Malaysia's (SC) mandate to regulate and develop Malaysia's capital market, the SC strives to continuously ensure that there are in place, relevant and effective measures of investor protection. This includes implementing new measures to create investor awareness around the various risks posed by the carrying on of unlicensed activities and raise levels of financial and investment literacy.

While investment in digital assets has been gaining popularity in recent years, there has also been an increase in regulatory non-compliance and financial crimes in market activities involving digital assets. The first article discusses the risks associated with investing in digital assets, particularly in the absence of any regulatory and supervisory oversight over such activities. It then shares how the SC regulates investments in digital assets, including supervisory and enforcement actions taken in relation to such activities. This article also sheds some light on what investors should consider before investing in digital assets.

In light of the recent revisions to the *Guidelines on Conduct for Capital Market Intermediaries*, the second article delves into what these revisions entail as well as their rationale and objective. In this regard, emphasis has been placed on ensuring that capital market intermediaries are providing good outcomes to investors by giving priority to the interest of investors. In line with peer regulators, the SC has also taken the initiative to require capital market intermediaries to give more attention to the protection of vulnerable investors in order to enable them to participate in the capital market without being disadvantaged.

The SC is cognisant that while sophisticated investors may be able to assume greater investment risks due to their investment knowledge or wealth, they are still susceptible to mis-selling by unscrupulous issuers and should therefore be afforded a certain level of protection. The third article highlights the SC's concerns in relation to offers of shares by unlisted public companies to sophisticated investors, as well as efforts made by the SC to offer some level of protection to sophisticated investors.

Finally, the fourth article examines the SC's observations on the state of compliance of anti-money laundering, counter terrorism financing and counter proliferation financing laws by relevant capital market intermediaries as well as best practices in this area. The article also provides a glimpse into emerging trends of money laundering tactics being used in the capital market.

Please share your comments, feedback or ideas for future editions via email to the Editorial Team at **reporter@seccom.com.my**

Unpacking the Landscape of Digital Asset Investments in Malaysia

Introduction

Over the past decade, digital assets such as cryptocurrency have been famously (or in some cases – infamously) popularised as either 'not to be missed investment opportunities' or an alternative category of investment, among retail investors.

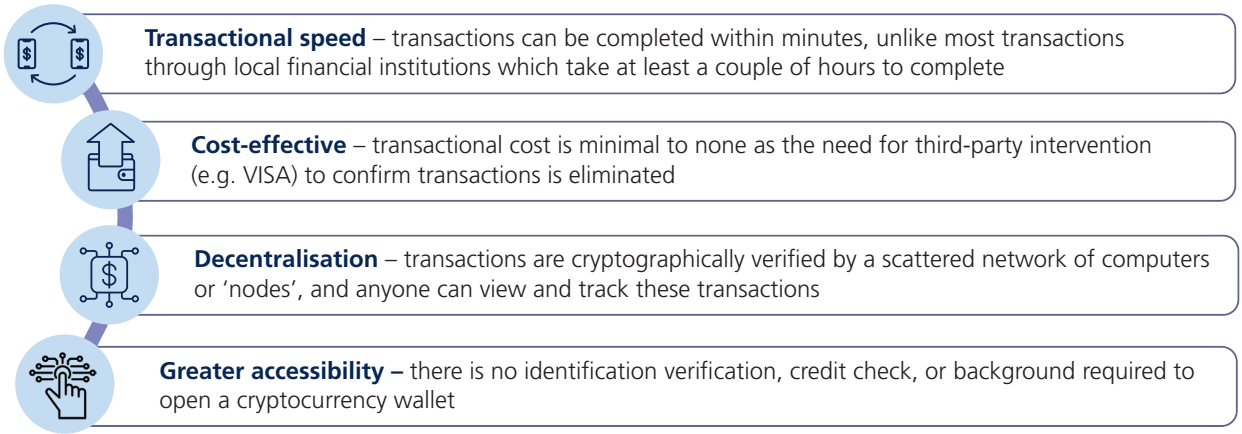
This article therefore seeks to highlight the attributes and risks associated with investing in digital assets and provide an overview of the trends and regulatory framework governing digital asset investments in Malaysia. 'Digital assets' for the purposes of this article refer to currency that is available exclusively in electronic form such as cryptocurrency and stablecoin (i.e. digital currency), as well as digital tokens, which are recorded using distributed digital ledger technology or 'DLT'.

Digital assets largely operate on a decentralised network, allowing people to buy and sell such digital assets directly through virtual wallets. These transactions are commonly verified and recorded on a distributed, cryptographically secured (and therefore, tamper-proof) ledger known as blockchain. Blockchain (which is a type of DLT) is essentially a virtual chain of blocks, each block of which contains details of each transaction and other information. The block becomes immutable, in that, data stored inside the block cannot be removed or replaced once it is added to the chain.

Digital assets are usually traded by investors on a digital asset exchange (DAX).

Common Attributes and Risks of Digital Asset Investments

Digital assets can be used as part of a diversified investment portfolio. In addition, there are many attractive aspects of investing in digital assets, including the following:[1]



[1] Nikita Tambe and Aashika Jain, *Advantages & Disadvantages of Cryptocurrency in 2024* (Forbes, 10 June 2024).

Be that as it may, the International Organization of Securities Commissions (IOSCO) has unfortunately highlighted that the increased exposure of retail investors to crypto-assets has also led to an increase in regulatory non-compliance and financial crimes including fraud, market manipulation and money laundering in crypto asset market activities.

Over the past few years, the digital asset landscape experienced significant turbulence, with the price of Bitcoin hitting an 18-month low of approximately US$16,500 as of January 2023. This low was followed by a string of negative events including the collapse of several exchanges, lenders, and asset managers such as OneCoin, Terra UST stablecoin, FTX exchange (FTX), and Three Arrows Capital in 2022.[2]

The case studies of OneCoin and FTX, as discussed below, serve as a cautionary tale, including to investors of what happens when there is inadequate, or worse, no regulatory or supervisory oversight over capital market activities such as digital asset trading.

OneCoin Case

OneCoin was the largest cryptocurrency-based Ponzi scheme which operated from 2014 to 2016. OneCoin was marketed as a legitimate cryptocurrency akin to Bitcoin, which allowed investors to use its coins for payments everywhere. In reality, OneCoin did not operate like other cryptocurrency on a decentralised ledger. Instead, the trading of OneCoin operated on its own internally managed exchange. Investors were convinced into buying OneCoin membership by purchasing membership packages which included educational courses and materials on cryptocurrencies, trading and investing.

OneCoin was eventually found to be fraudulent and could not be used for any actual purchase as claimed. In 2017, OneCoin shut down its exchange, leaving investors unable to cash out their coins and suffer losses. In the same year, the founder of OneCoin, Ruja Ignatova, mysteriously vanished and has not been found to this day.

FTX Case

Founded in 2019, FTX was a major crypto exchange led by Sam Bankman-Fried which quickly gained prominence. Headquartered in the Bahamas, FTX which largely targeted American investors, was an offshore exchange that was not accountable to any regulator and outside the regulatory oversight of the American regulators such as the Securities Exchange Commission (SEC) or the Commodities and Futures Trading Commission.[3] FTX essentially operated like an opaque financial black box through which billions of US dollars flowed, thus enabling it to undertake activities that would otherwise not be allowed.[4] FTX eventually collapsed due to a lack of liquidity, fraud and mismanagement of funds, leading to its bankruptcy filing in 2022. In the aftermath of its collapse, Bankman-Fried was convicted for multiple fraud charges and sentenced to 25 years in prison.

[2] *Digital Asset Data: 2023 Recap & 2024 Trends* (Digital Asset Research, 8 January 2024).
[3] MSNBC, The stunning collapse of FTX, explained by Zeeshan Aleem, 18 November 2022 at: FTX's collapse and Sam Bankman-Fried illustrate crypto's shadiness (msnbc.com).
[4] *Ibid*.

In addition to the risks associated with investing through operators that are not subject to any regulatory or supervisory oversight, an investor who intends to invest in digital assets must be mindful of the fact that similar to an investment in equities or bonds, trading in digital assets comes with its own set of risks. Here are some common risks associated with trading in digital assets:

High volatility

Digital assets tend to be highly volatile as their value can fluctuate rapidly over a short period in the digital asset market, resulting in potential substantial or total losses for investors.

Investing in digital assets is considered high-risk due to their speculative nature. Over the past years, many digital asset operators have faced severe financial difficulties, sometimes resulting in the suspension of withdrawal of investors' assets.

This risk is particularly amplified given that DAXs usually operate on a self-directed model (i.e. without any advice from a broker or financial adviser unlike in traditional financial markets).

Security risks

Investments in digital assets are exposed to a greater risk of cybersecurity threats and breaches (e.g. hacking, social engineering and phishing attacks). Accordingly, if a DAX or wallet is compromised, funds can be stolen.

There is also a risk of fraudulent schemes under the guise of cryptocurrency investments where investors are offered and subject to bogus coin offerings, Ponzi and pyramid schemes, and outright theft where the promoter simply vanishes with investors' money.

Drawing from the risks highlighted above, despite the attractiveness and ease of investing in digital assets, investors who have an appetite for digital asset investments are strongly urged to exercise diligence to ensure that the offering and trading of such investments are subject to regulatory oversight, and that they understand how such investments including their risks would impact them, before committing to such investments.

Malaysian Landscape

Regulatory Framework

The offering and trading of digital assets in Malaysia are regulated by the SC in that digital assets, which comprise of both digital currencies and digital tokens, are prescribed as securities for purposes of securities laws in Malaysia.[5]

Further, any person who operates or maintains a DAX (DAX operator) in Malaysia will also be required to be registered with the SC as a recognized market operator (RMO).[6] Upon registration with the SC, a DAX operator will be subject to continuing obligations pursuant to the *Guidelines on Recognized Markets* (RMO Guidelines) which among others, require the DAX operator to monitor and ensure compliance with the rules governing the management and operation of the DAX, ensure fair treatment of its users and the accuracy of all disclosures.[7]

---

5 Paragraphs 2 and 4 of the *Capital Markets and Services (Securities Regulations) (Digital Currencies and Digital Tokens) Prescription Order 2019.*
6 Section 34 of the *Capital Markets and Services Act 2007* read together with Part B of the RMO Guidelines.
7 Please refer to Parts C and G of the RMO Guidelines for the relevant obligations and requirements which a DAX operator is subject to.

It should be highlighted here that the SC may also regard a DAX who operates outside Malaysia to be operating in Malaysia if the DAX actively targets Malaysian investors.[8] The SC will consider a DAX to be actively targeting Malaysian investors if its operator or the operator's representative directly or indirectly promotes the DAX in Malaysia by, for example, advertising the DAX in any publication in Malaysia, or sending any direct mail or e-mail to Malaysian addresses to market or promote the DAX.[9]

A DAX that has been regarded by the SC to be operating in Malaysia will be subject to the requirements applicable to DAX operators in Malaysia as discussed above. Operators of foreign DAXs should therefore seek legal advice on the need for registration with the SC before it targets Malaysian investors.

On the other hand, Malaysian investors are advised to only trade on DAXs, whether operated locally or outside Malaysia, which are registered with the SC to benefit from the protection provided under Malaysian securities laws. Investors who have been solicited to invest in a digital asset offered on a DAX, located in or outside Malaysia, which is not registered with the SC are also advised to report such DAX to the SC for appropriate action to be taken.

Recent Trends in Relation to Investments in Digital Assets

There are currently six DAX operators registered with the SC, namely, HATA Digital Sdn Bhd, Luno Malaysia Sdn Bhd, MX Global Sdn Bhd, SINEGY DAX Sdn Bhd, Tokenize Technology (M) Sdn Bhd and Torum International Sdn Bhd (regulated DAXs).

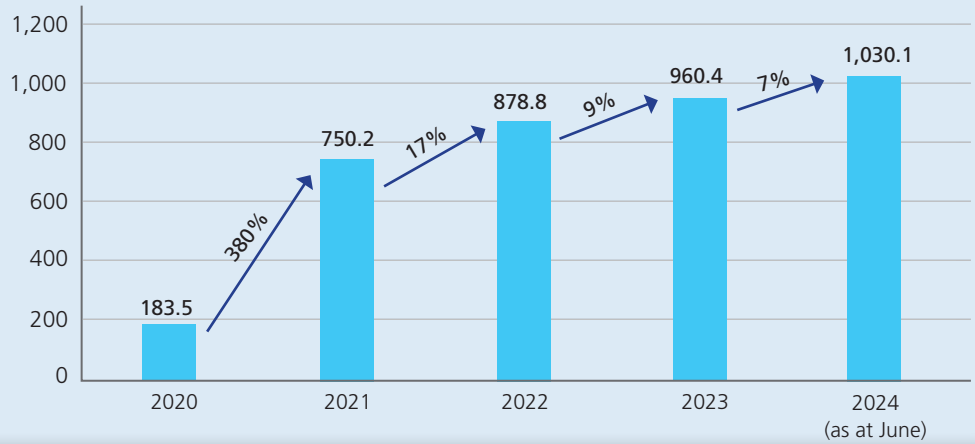
As at June 2024, there are 14 digital assets traded on the regulated DAXs in Malaysia.[10] There has been a growing interest in the different types of digital assets traded on the regulated DAXs in Malaysia since 2020, as illustrated in Table 1.

Table 1: Number of digital assets traded on regulated DAXs in Malaysia

Year	2020	2021	2022	2023	2024 (as at June)
Number of digital assets traded on regulated DAXs in Malaysia	4	5	9	11	14

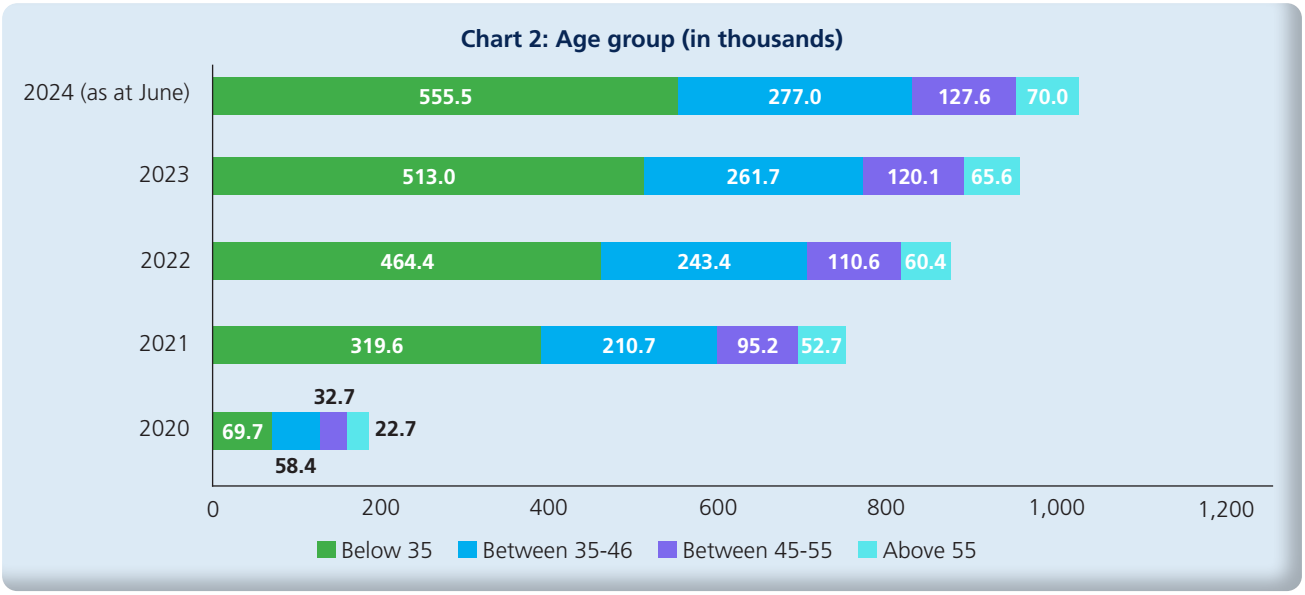
As at June 2024, the trading value of DAXs have accumulated to RM42.4 billion from only RM1.4 billion in 2020, signalling an increase in investors' appetite for trading on DAX in Malaysia, as demonstrated in Chart 1.

Chart 1: Total no. of customers (in thousands)



[8] Paragraph 1.11 of the RMO Guidelines.
[9] Paragraphs 1.13 and 1.14 of the RMO Guidelines.
[10] A list of the digital assets permitted to be traded on regulated DAXs in Malaysia is available on the SC's website at www.sc.com.my/digital-assets.

Chart 2, as set out below, further provides a breakdown of current statistics of investors investing in digital assets through the regulated DAXs in the last five years based on age demographic.

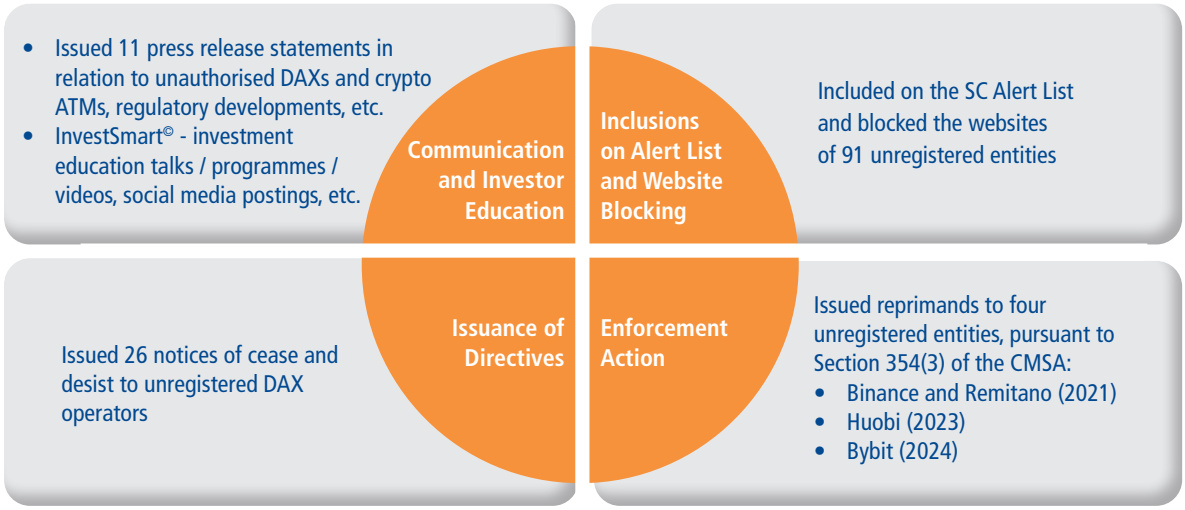


In this regard, trading in digital assets tends to be more popular among the younger generation, in particular individuals under 35. Unsurprisingly, this is because the younger generation tends to be more technologically adept and are often more willing to embrace innovative financial products and services. They also tend to be attracted to the potential high returns and the decentralised nature of digital assets, aligning with their desire for financial independence and control.

SC Intervention

In recent years, the SC has seen a rise of unregistered DAX operators targeting Malaysians, who have subsequently suffered monetary losses as a result of investing through such unregistered entities. Since 2020, the SC has received a total of 1,186 complaints and enquiries on cases involving unregistered DAXs.

In view of the growing concerns over such unregistered DAXs and complaints, which is further exacerbated by the increasing interest in digital asset investments as outlined above, the SC has taken the measures depicted in the diagram below as a means to better protect and educate investors in this area and maintain the integrity of the capital market.



Conclusion

While the SC will continue to undertake its role by, among others, taking robust measures to detect, prevent and tackle illegal activities involving DAXs, the public is also reminded to be responsible and appreciate the risks associated with any investment, and exercise judgement and caution before making investment decisions.

Message to DAX operators that are not registered with the SC

- Cease such unlicensed activities immediately and return all monies collected from investors.
- The act of operating a DAX without registration is an offence under securities laws. If in doubt as to whether SC registration will be required, please refer to the CMSA or seek legal advice.
- Those operating a DAX without being registered with the SC may refer to the RMO Guidelines for the steps, requirements and criteria to be registered with the SC.

Message to investors investing in digital assets

- Understand the risks associated with digital assets before investing in them.
- Invest only through DAX operators that are registered with the SC. Investors may refer to the up-to-date list of registered DAX operators on the SC's website at www.sc.com.my/digital-assets
- Manage risks by deploying a diversification strategy to ensure that investments are sufficiently managed.
- Contact the SC if you have any queries or complaints by calling 03-6204 8999 or email aduan@seccom.com.my

Enhancing Investor Protection Through Higher Standards of Conduct in the Capital Market

Introduction

Investor protection is an essential objective of the SC. The SC employs a holistic approach to investor protection which includes imposing conduct requirements on licensed and registered persons, and monitoring compliance with such requirements. Contravention of conduct requirements are met with swift enforcement action to deter future misconduct. The SC has also taken a proactive role to empower investors by carrying out various activities to promote investment literacy and to inform investors of their rights. In addition, the SC always reminds the public to only transact with licensed or registered persons (for purposes of this article, a 'capital market intermediary' or 'CMI'). This is because CMIs are subject to conduct requirements.

CMI conduct requirements seek to ensure that CMIs, when dealing with investors, will observe minimum standards of behaviour that will reinforce investor trust and confidence. These standards must continuously evolve to keep up with changes in societal expectations.

This article highlights the SC's recent efforts in raising the standards of conduct of CMIs through the revision of the *Guidelines on Conduct for Capital Market Intermediaries* (Conduct Guidelines).

Evolving Nature of Conduct Requirements

The Conduct Guidelines first came into force on 1 April 2022. As discussed above, conduct requirements must evolve to conform with societal expectations. Consequent to this, the SC issued the revised Conduct Guidelines which came into force on 1 October 2024.

Like the previous Conduct Guidelines, the revised Conduct Guidelines emphasises the need for CMIs to deal with investors in an honest and fair manner, giving due regard to investors' interests. This is important because many investors are reliant on the knowledge and skills of CMIs. Because of this reliance, the Conduct Guidelines imposes the duty to exercise reasonable care, skill and diligence on CMIs when dealing with investors. The revised Conduct Guidelines provides CMIs with examples of instances in which the SC would expect CMIs to observe the required standards. For example, CMIs that are distributing products are required to exercise reasonable care to ensure that the product is only promoted to its intended target market. The revised Conduct Guidelines also reinforces the requirement for CMIs to manage or mitigate a conflict of interest if it cannot be avoided.

The revised Conduct Guidelines also imposes new requirements on CMIs. For example, CMIs that rely on standard form contracts are required to take reasonable steps to explain to investors the implication of terms that can affect investors' rights and obligations. The revised Conduct Guidelines also sets out requirements for dealing with vulnerable investors and addresses risks arising from online transactions. These are further discussed below.

Outcomes of the Revised Conduct Guidelines

The revised Conduct Guidelines is expected to result in, among others, the following:

Investors Receiving Good Outcomes

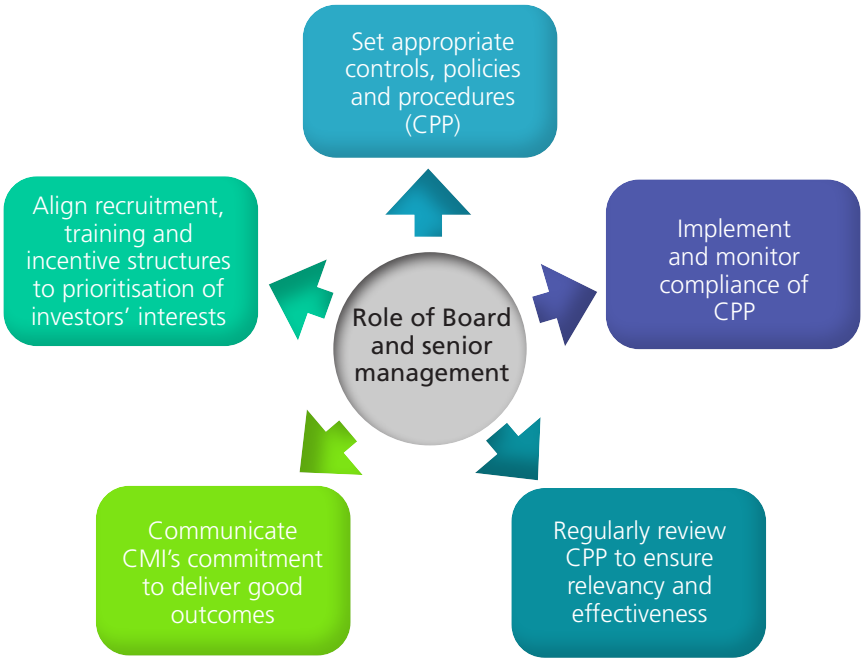
The standards of behaviour imposed by the revised Conduct Guidelines provides a baseline of the expected corporate culture of CMIs; one which gives priority to the interest of investors. Giving priority to the interest of investors ensures that investors always receive good outcomes in their dealings with CMIs.

As such, the revised Conduct Guidelines requires CMIs to focus on the delivery of the following outcomes:

1. investors know that they are dealing with CMIs whose values and beliefs embody fair and honest treatment of investors
2. investors are always provided with information that allows them to make informed decisions
3. CMIs will exercise reasonable care, skill and diligence in their dealings with investors
4. investors are provided with suitable personal advice
5. investors' complaints are dealt with in a fair, transparent, timely, efficient and effective manner
6. CMIs have appropriate and effective controls to protect investors' assets from any risk of loss arising from misappropriation, fraud or insolvency
7. CMIs have appropriate and effective controls to protect investors' infomation from any risk of loss, theft, misuse or unauthorised disclosure, access or modification

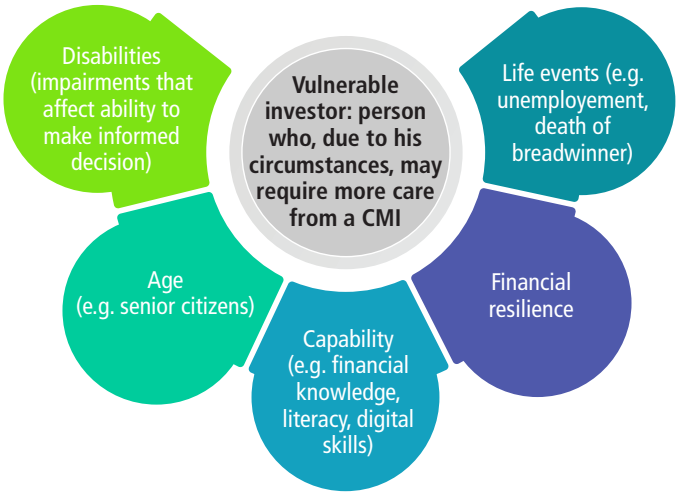
Role of the Board of Directors and Senior Management

Corporate culture is shaped by the tone at the top. For this reason, the revised Conduct Guidelines reinforces the essential role of a CMI's board of directors (Board) and senior management in inculcating a corporate culture where investors' interests are prioritised by delivering the good outcomes above. The revised Conduct Guidelines encourages a CMI's Board and senior management to ensure that the CMI's strategies, governance, leadership, processes, and people policies reflect the obligation to deliver good outcomes to investors. A snapshot of the role of the Board and senior management is set out below.

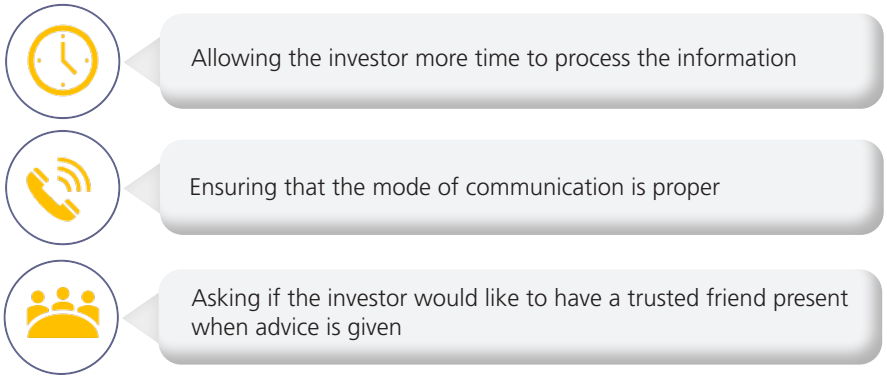


Protection of Vulnerable Investors

In recent years, regulators worldwide have been giving greater attention to the protection of vulnerable investors, particularly, elderly investors. In line with this development, the revised Conduct Guidelines sets out expectations on CMIs in their treatment of vulnerable investors. As a first step, CMIs are required to have in place CPP to identify and respond appropriately to vulnerable investors. As guidance, the revised Conduct Guidelines defines who are considered to be vulnerable investors and sets out indicators of vulnerability that CMIs should look out for.



Upon identifying an investor as vulnerable, a CMI is required to respond appropriately to ensure that the vulnerable investor is not deprived of the good outcomes above nor denied access to capital market products and services merely because of his vulnerability. Measures for responding appropriately may include:



In raising awareness about vulnerable investors, the SC hopes to work together with CMIs to create a level playing field for all investors. Nevertheless, in dealing with the CMI, investors are encouraged to be honest and forthcoming in disclosing their vulnerability to the CMI to enable the CMI to take appropriate action.

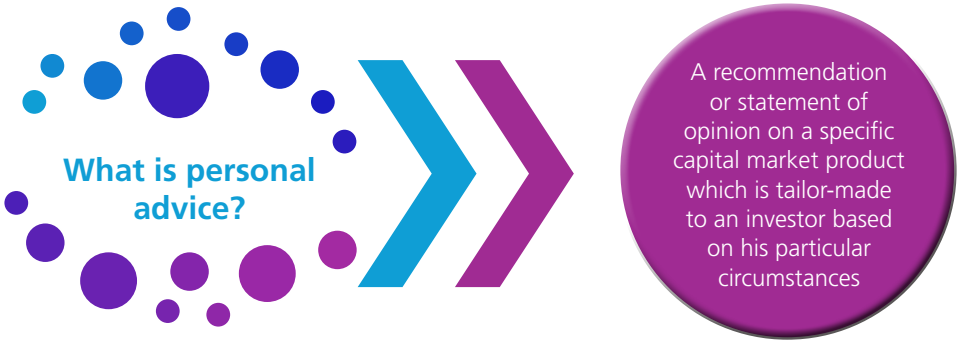
Investors Provided with Suitable Personal Advice

Personal Advice to Investors

The mis-selling of capital market products is a continuing concern. Mis-selling happens when investors are sold financial products which are not aligned to their objectives or needs. This is damaging to investors and results in a loss of trust and confidence.

The revised Conduct Guidelines sets out requirements that apply to CMIs when providing personal advice. These requirements build upon the framework in the *Guidelines on Sales Practices of Unlisted Capital Market Products* (SPG).[1] Essentially, the revised Conduct Guidelines requires CMIs to follow required steps before providing personal advice, as further discussed below.

It should be noted that personal advice is to be distinguished from the provision of information to investors. Where information is provided to investors, a CMI is only required to ensure that the information is not false or misleading.



[1] The provisions on suitability assessment in the SPG have been replaced by the specific requirements in relation to personal advice in the revised Conduct Guidelines which came into force in October 2024.

With the implementation of the revised Conduct Guidelines, investors can expect CMIs to take the following steps when providing personal advice on a face-to-face basis:[2]

It must be pointed out that the quality of personal advice provided to an investor is dependent on the information that is provided by the investor. In this regard, it is in the interest of the investor to be honest and forthcoming with information that is sought by the CMI for purposes of giving personal advice.

[2] Where personal advice is given on or through an online platform, a modified set of requirements apply. See paragraph 9.11 of the revised Conduct Guidelines.

Addressing Risks Arising from Online Transactions

Online platforms have provided investors with a new world of opportunities to participate in the capital market. However, it also brings with it a different set of risk to investors. Recognising the need to balance responsible digital innovation and investor protection, the revised Conduct Guidelines sets out principles and requirements to be complied with by CMIs providing capital market products or services on or through an online platform. The principles and requirements include the following:

Nevertheless, investors are encouraged to be vigilant when transacting on or through an online platform. If unsure, investors should always check on the authenticity of the platform before making an investment decision.

Conclusion

The standards proposed in the revised Conduct Guidelines are not novel as they are reflective of the standards that are expected of CMIs. The standards promote CMI resilience and reputation as they seek to minimise the risk of mis-selling, avoid reputational damage, reduce complaints and improve client retention.

Tightening Requirements for Unlisted Public Companies Seeking Funding from Sophisticated Investors

Introduction

Investor protection is inextricably linked to the principle that strong capital markets require investor confidence, failing which, investors would flee the market. As such, the mandate of the SC has been to take all reasonable measures to maintain investor confidence in the capital market by ensuring the adequate protection of investors.

The SC in carrying out the above mandate, utilises a variety of approaches which include educating investors, licensing those who act as intermediaries to investors and taking swift enforcement action to deter future misconduct. At times, this mandate also requires the SC to issue new rules that seek to further protect investors.

In protecting investors, it is important to note that Malaysia's securities laws, as with other jurisdictions, distinguishes the level of protection that is provided between sophisticated investors and retail investors. The level of protection afforded to retail investors is higher than that which is provided to sophisticated investors. Sophisticated investors are regarded as having more investment knowledge and are able to assume greater investment risks relative to their wealth or asset levels and therefore do not require the same level of protection as retail investors. An example of the differing levels of protection is in the disclosure of material information to investors.

The disclosure of material information to sophisticated investors is subject to a lighter level of regulation, compared to the information that is disclosed to retail investors. However, the SC is aware that the lighter level of regulation has been abused for purposes of perpetrating securities fraud[1]. This article discusses the issues relating to the lighter regulatory approach and the SC's efforts in mitigating such abuse.

Disclosure of Material Information to Investors

Disclosure of material information to investors is a fundamental part of fundraising regulation. Fundraising regulation as embodied in the CMSA seeks to balance companies' access to capital from the public while ensuring that investors are adequately protected.

In this regard, the CMSA requires that any distribution or offer of securities (including shares) be accompanied by a registered prospectus, unless exempted. The content of the prospectus is regulated with the view of ensuring that investors are provided with complete and accurate information on the company's business and the securities being offered, so that investors can make informed investment decisions. Registration of the prospectus with the SC also means that the SC vets through the information to be disclosed to investors in the prospectus.

[1] Securities fraud is an umbrella term for deceptive acts employed by a person to manipulate investors through the provision of false information, ultimately causing financial harm to investors for the perpetrator's personal gain.

Incomplete or inaccurate information disclosed in a prospectus can result in the issuer and those involved in the preparation of the prospectus to be subject to criminal and civil liability. The SC can also issue a stop order to prevent further distribution of a defective prospectus.

Disclosure of Information where Offer of Shares is Made only to Sophisticated Investors

Cognisant that preparing and registering a prospectus is costly and time consuming, the CMSA provides a list of exemptions which allow securities to be offered without incurring the level of resources needed for preparing a prospectus.

One such exemption is where an offer of shares is made to sophisticated investors by an unlisted public company (UPC). This is because, to subject an offer made by a UPC to sophisticated investors with the same regulatory requirements as those that are imposed on offers to retail investors, can be costly and time consuming. This can also result in an unreasonable funding barrier for UPCs that are genuinely seeking capital to run their business.

The Changing Dynamics

In respect of disclosure, the only requirement applicable to a UPC offering shares to sophisticated investors is the requirement to deposit a copy of its information memorandum (IM) with the SC. This deposit requirement only applies if an IM is in fact issued. Further, unlike a prospectus, the content of an IM is not regulated.

UPCs that have issued an IM but did not deposit a copy of the IM with the SC, would be committing an offence under the CMSA. The CMSA also provides that the IM issued shall be deemed to be a prospectus insofar as it relates to the liability of the issuer or his agents for any statement or information that is false or misleading or from which there is material omission.

Abuse of Existing Requirements

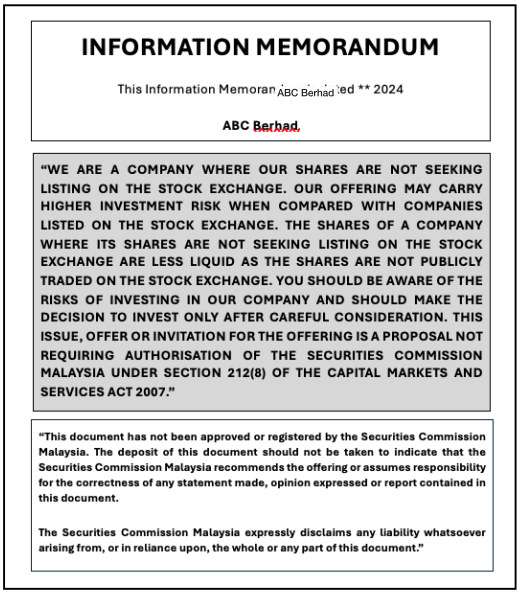
The SC has noted growing trends in which the amounts proposed to be raised by UPCs have increased significantly higher than the total amount raised from the public market. Unsurprisingly, the high amounts proposed to be raised by UPCs are not without issue. The SC reported an increasing number of complaints and enquiries in relation to the offer of shares by UPCs. In some cases, it was noted that the disclosures made by UPCs in their IMs were inadequate, vague or misleading, giving rise to public complaints and enquiries.

Examples of some disclosures made:

Set against this backdrop, the SC issued the *Guidelines on Offer of Shares by Unlisted Public Companies to Sophisticated Investors* (Guidelines) in 2021. The Guidelines addresses the concerns noted by the SC in relation to the offer of UPC shares to sophisticated investors.

- **Sophisticated investors have the misconception that the proposed offering has been approved by the SC.** To cure this misconception, the Guidelines mandates that the cover page of an issued IM must include a caution statement, highlighted in bold, stating that the offer of shares by the UPC has not been authorised by the SC and that the IM has not been approved or registered by the SC;

- **Sophisticated investors are not exercising sufficient due diligence to safeguard their own interests.** In this regard, the Guidelines mandates that the cover page of an issued IM must include a caution statement, highlighted in bold and in a prominent colour, stating that shares of a UPC are less liquid as they are not publicly traded and, in this regard, investors should be aware, among others, of the risks of investing; and



INFORMATION MEMORANDUM

This Information Memoran ABC Berhad ed ** 2024

ABC Berhad

"WE ARE A COMPANY WHERE OUR SHARES ARE NOT SEEKING LISTING ON THE STOCK EXCHANGE. OUR OFFERING MAY CARRY HIGHER INVESTMENT RISK WHEN COMPARED WITH COMPANIES LISTED ON THE STOCK EXCHANGE. THE SHARES OF A COMPANY WHERE ITS SHARES ARE NOT SEEKING LISTING ON THE STOCK EXCHANGE ARE LESS LIQUID AS THE SHARES ARE NOT PUBLICLY TRADED ON THE STOCK EXCHANGE. YOU SHOULD BE AWARE OF THE RISKS OF INVESTING IN OUR COMPANY AND SHOULD MAKE THE DECISION TO INVEST ONLY AFTER CAREFUL CONSIDERATION. THIS ISSUE, OFFER OR INVITATION FOR THE OFFERING IS A PROPOSAL NOT REQUIRING AUTHORISATION OF THE SECURITIES COMMISSION MALAYSIA UNDER SECTION 212(8) OF THE CAPITAL MARKETS AND SERVICES ACT 2007."

"This document has not been approved or registered by the Securities Commission Malaysia. The deposit of this document should not be taken to indicate that the Securities Commission Malaysia recommends the offering or assumes responsibility for the correctness of any statement made, opinion expressed or report contained in this document.

The Securities Commission Malaysia expressly disclaims any liability whatsoever arising from, or in reliance upon, the whole or any part of this document."

- **Sophisticated investors are being solicited by unlicensed persons who promote and market UPC share offerings.** The Guidelines mandates that agents appointed for promotional and marketing activities of UPC shares must hold a Capital Markets Services Licence for the regulated activity of dealing in securities. This is because licensed persons are subject to strict conduct requirements that are designed to minimise the risk of mis-selling to investors.

Further, to enable the SC to have better oversight over how funds raised by UPCs have been utilised, the Guidelines also requires UPCs to submit to the SC:

- a post-issuance notification no later than seven days after the commencement of the offering; and

- a post-issuance update report that is prepared on a quarterly basis, no later than seven days after the end of each quarter of its financial year, if the offering is ongoing.

The requirements imposed under these Guidelines are only applicable to UPCs whose shares are solely offered to sophisticated investors. These requirements do not apply to UPCs making an offer of shares through an equity crowdfunding platform registered with the SC. Furthermore, where UPC shares are also offered to retail investors, a prospectus will be required, and all applicable prospectus requirements will apply.

Conclusion

While the Guidelines issued has imposed additional requirements on UPCs that seek to raise funds from sophisticated investors, it is equally important for sophisticated investors to remain vigilant.

Sophisticated investors should do their homework and understand the risks associated with the proposed investment, before parting with their hard-earned money. In many cases, the promise of high returns will be conditional thus making it difficult to establish fraud in the event that the promised returns are not met. Caution should also be exercised where the IM states that the funds will be utilised for a business that is yet to be set up.

Should investors have any queries or complaints, please contact the SC at 03-6204 8999 or email at aduan@seccom.com.my

State of Compliance of Anti-Money Laundering Requirements in the Capital Market and Emerging Money Laundering Trends and Techniques

Overview and Recent Developments in the Anti-Money Laundering, Counter Terrorism and Counter Proliferation Financing Laws in the Malaysian Capital Market

Money laundering, along with terrorism and proliferation financing, continue to be a global phenomenon of critical importance, necessitating sustained vigilance and robust control measures. For this reason, authorities, regulators and key organisations worldwide have intensified their fight against these offences.

Put simply, the said offences generally entail the following activities:

Money laundering (ML)	Terrorism financing (TF)	Proliferation financing (PF)
Processing or concealing proceeds of crimes so that they appear to have originated from legitimate sources.	Dealing in funds or property (whether from a legitimate or illegitimate source) that are used either, to assist the commission of terrorist acts, or finance terrorists and terrorist organisations.	Providing funds or financial services which are used to develop nuclear, chemical or biological weapons and any related materials to weapons of mass destruction.

It is imperative to recognise that ML, TF and PF pose significant threats not only to international peace and security, but these offences also pose significant threats to the integrity and stability of the financial markets and economy. It is therefore crucial for countries to have in place and implement effective anti-money laundering (AML), counter financing of terrorism (CFT) and counter proliferation financing (CPF) policies and measures to combat these offences.

In Malaysia, the *Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001* (AMLA) is the primary piece of AML/CFT legislation. AMLA sets out, among others, the measures that are required to be taken to detect and prevent those criminal activities and the investigatory powers that authorities have in the prosecution of ML and TF cases. AMLA also empowers relevant regulatory or supervisory authorities such as the SC and Bank Negara Malaysia (BNM) to issue such directions and guidelines to the institutions under their regulation or supervision as they consider necessary in order to combat ML and TF.[1]

For this purpose, the SC (as the regulatory and supervisory authority of the capital market) sets out AML/CFT requirements and obligations relevant to capital market players under the *Guidelines on Prevention of Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Reporting Institutions in the Capital Marke*t (AML Guidelines). The AML Guidelines applies to persons licensed

[1] Section 83 of AMLA.

to carry on regulated activities or persons registered under the CMSA as specified under the First Schedule of the AMLA, which include persons licensed by the SC to carry on the regulated activities of dealing in securities, dealing in derivatives, fund management and advising on corporate finance, as well as recognized market operators and digital asset custodians registered with the SC under the CMSA (reporting institutions).

In June of this year, the AML Guidelines were amended to consolidate the requirements under the *Guidelines on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing of Capital Market Intermediaries* (PF Guidelines). The PF Guidelines were issued in April 2018 to essentially ensure capital market intermediaries' compliance with targeted financial sanctions (TFS) on proliferation financing obligations and restrictions under the *Strategic Trade Act 2010* (STA) and its subsidiary legislations.

In addition, the AML Guidelines were concurrently revised to introduce the following key amendments:

(a) Implementation of a risk-based approach application to proliferation financing risk;

(b) Requirements for trustees to disclose status when establishing business relations in customer due diligence measures for legal arrangement;

(c) Obligation on beneficiary institutions to ensure veracity of the beneficiary information received from the ordering institution;

(d) Prescription of additional minimum information required from customers and beneficial owners;

(e) Sanction screening for customers and beneficiaries; and

(f) Policies on the duration upon which internal suspicious transaction reports must be reviewed by the reporting institutions.

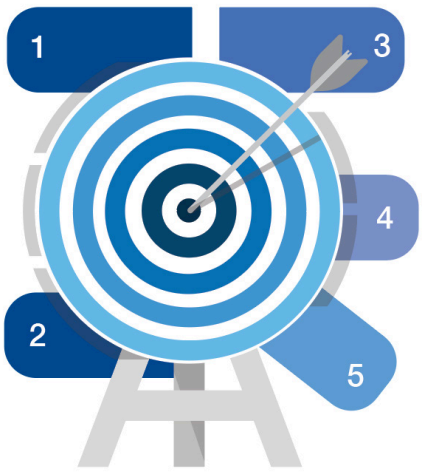
In its effort to ensure that policies and strategies remain robust in detecting and preventing illicit capital market activities, the SC, in 2023, undertook a thematic review on the state of compliance of the SC's revised AML Guidelines issued in 2021, by persons licensed by the SC to carry on the regulated activities of dealing in securities, dealing in derivatives and fund management (Reporting Institutions or RIs) through the issuance of questionnaires and follow-up on-site examinations. The thematic review focused on the following key areas:

GOVERNANCE

- Oversight of the Board and senior management
- Availability and comprehensiveness of AML/CFT policies and procedures
- Independent audit reviews conducted
- AML/CFT training and staff awareness of AML/CFT risks and measures

RISK-BASED APPROACH

- Business-based risk assessment
- Relationship-based risk assessment



CUSTOMER DUE DILIGENCE

- Onboarding of customers
- Third-party deposits
- Ongoing due diligence
- Transactions monitoring

ENFORCEMENT ORDERS

- Engagement with law enforcement agencies (LEAs)
- Processes for screening and freezing

TARGETED FINANCIAL SANCTIONS

- Maintenance and update of sanctions lists
- Screening of customers (at onboarding and ongoing)
- Freezing processes

The first part of this article provides a summary of the SC's findings and key takeaways in relation to the thematic review. The second part of this article highlights the emerging trends and techniques of ML activities in the capital market sector.

I. The SC's Observations and Key Takeaways from the Thematic Review

1. Governance

The Board and senior management of a reporting institution are central to upholding good governance and ensuring the effectiveness of the reporting institution's AML/CFT/CPF and TFS framework. In this regard, the Board is essentially responsible for setting the culture of safeguarding the integrity of the capital market. For this reason, it is crucial that the Board establish AML/CFT/CPF policies and procedures as well as ensure that they are implemented effectively by the senior management.

In addition to implementing the AML/CFT/CPF policies and procedures, the senior management of a reporting institution should also regularly report critical AML/CFT/CPF matters to the Board to ensure that the Board remains continuously informed of these matters and is able to take necessary measures to address or manage such matters.

The SC's Observations

Based on the review conducted, the SC has observed the following:

(a) RIs keep their respective Boards apprised of AML/CFT/CPF and TFS matters largely through reporting of key metrics such as the number of suspicious transaction reports (STR) lodged with the Financial Intelligence and Enforcement Department of BNM (FIED), number of names that matched against names listed in orders by LEAs and number of high-risk customers as well as the outcome of compliance programs and results of business-based risk assessments; and

(b) RIs have aligned their AML/CFT/CPF and TFS frameworks with requirements of the SC's revised AML Guidelines and PF Guidelines.

Key Takeaways

i. Ensure that the relevant AML/CFT and TFS policies and procedures **are updated in a timely manner** to ensure they remain relevant, effective and are aligned with regulatory developments, in complying with paragraph 6.2(c) of the AML Guidelines.

ii. Apprise the Board on AML/CFT and TFS matters, not only on statistics or RI-specific issues, but also on **any revisions to relevant guidelines and standards, global trends, red flags, typologies, etc,** in complying with paragraph 6C.1(e) of the AML Guidelines.

iii. Conduct independent **audit review regularly on AML/CFT and TFS** policies covering key risk areas such as the customer onboarding processes, risk profiling, ongoing due diligence and enhanced due diligence of customers, transactions monitoring parameters, quality of STR, record keeping, quality assurance, etc, in complying with paragraph 6A.1(b) of the AML Guidelines. Frequency and scope of the audit should be commensurate with the size, nature and complexity of business operations of the respective RIs.

2. Risk-Based Approach

A reporting institution must take appropriate steps to identify, assess and understand its ML/TF/PF risks in relation to its customers, countries or geographical areas, products and services offered, transactions or delivery channels used, and other relevant risk factors. In this regard, a strong risk-based approach (RBA) underscores a reporting institution's commitment to a robust and proactive AML/CFT/CPF framework. It also allows the reporting institution to allocate resources more efficiently, directing attention to higher ML/TF/PF risk areas, which in turn supports the detection, mitigation and prevention of ML/TF/PF activities within the reporting institution.

The RBA entails two assessments, namely the Business-based Risk Assessment (BbRA) and the Relationship-based Risk Assessment (RbRA).

The BbRA is a comprehensive exercise required to be undertaken by a reporting institution to assess vulnerabilities of the reporting institution's business against ML/TF/PF risks.

On the other hand, the RbRA or customer risk profiling is essential for a reporting institution to identify, assess, and understand the ML/TF/PF risks posed by its customers based on the nature and type of business of its customers. Both BbRA and RbRA are essentially required to enable the reporting institution to develop strategies that effectively manage and mitigate such ML/TF/PF risks.

The SC's Observations

In this area, the SC observed that most RIs have established, effectively implemented and regularly reviewed their RbRA frameworks enabling them to make informed decisions regarding the appropriate customer due diligence and ongoing monitoring mechanisms to be applied on their customers.

Key Takeaways

BbRA – Institutional Risk Assessment

i. **Conduct BbRA regularly**, or at a minimum, every two years or sooner if there are any changes to the RI's business model such as the growth of the business, offering of new products or services or latest trends and typologies in the sector (paragraph 8.2 of Appendix A, AML Guidelines).

ii. **Regularly review BbRA and its risk factors/parameters** in line with the RI's evolving risks (paragraph 2.4 of Appendix A, AML Guidelines). The BbRA should include among others:
   (a) Findings of the National Risk Assessment (NRA);
   (b) Comprehensive risk factors covering aspects such as the RI's customers, geographic location, and the products and services offered by the RI; and
   (c) Identification and assessment of the impact of specific risk factors/parameters of TF and PF risks.

iii. Conduct **ML/TF/PF risk assessments prior to the introduction of any new products, services and/or delivery channels (paragraph 7.1.5 of the AML Guidelines)**.

iv. Offer **adequate guidance on the methodology and results** of its BbRA to ensure applicability, accuracy and reasonableness, in complying with paragraph 3.1 of Appendix A, AML Guidelines.

RbRA – Customer Risk Profiling

i. Conduct RbRA using both **quantitative and qualitative methodology** incorporating relevant risk factors such as the RI's customers, geographic location, and products and services offered by the RI, in complying with paragraph 5.1 of Appendix A, AML Guidelines.

ii. Determine and assign relevant **risk weightages to identified risk factors based on materiality of such risks and the RI's circumstances when assessing the overall exposure to ML/TF risks from customers**, and not limit the RbRA to single-factor risk determination, in complying with paragraph 7.1.2(b) of the AML Guidelines.

iii. Consider both **TF and PF risk assessments** which may impact or apply to its customers, and products and services offered, in complying with paragraphs 7.1.1 and 7.3.1 of the AML Guidelines.

iv. **Regularly update the risk factors and parameters** used in its RbRA to ensure applicability based on its customers' pool, changes in customers' behaviour and global trends, in complying with paragraph 7.1.2(b) of the AML Guidelines.

3. Customer Due Diligence

In order to identify ML/TF/PF risks posed by a reporting institution's customers, the reporting institution is required to identify and verify the identities of its customers at the point of establishing its relationship with the customer. This process of establishing and verifying customer identities is generally known as customer due diligence or CDD. Implementing robust CDD measures ensures that a reporting institution has a comprehensive understanding of its customers' profiles and the ML/TF/PF risks posed by each of its customers or any transactions by such customers.

A reporting institution is also required to undertake enhanced CDD measures (Enhanced CDD) on a customer and, where applicable, the beneficial owner (BO), where the ML/TF/PF risks are assessed as higher risk. Examples of circumstances of higher risk include, among others, where the customer is a company that has nominee shareholders or which ownership structure appears unusual or excessively complex given the nature of the company's business, payments received from unknown or unassociated third parties, and where the customer is an individual who is a politically exposed person (PEP) (i.e. person who is or has been entrusted with prominent public functions e.g. Head of State or of government, senior politician, or senior government, judicial or military official), or is from a country identified as having inadequate AML/CFT/CPF systems or that is subject to sanctions, embargos or similar measures issued by international organisations such as the United Nations.

Key Takeaways

At Point of On-boarding	Enhanced CDD	Beneficial Ownership
i. Ensure that the minimum data points of information collected from customers are accurate to assist in identifying and verifying the identities of customers, in complying with paragraph 8.1.6 of the AML Guidelines; ii. Conduct thorough screening of each customer, including individuals acting on behalf of the customer, parties connected to the customer that are involved in the transaction, and BOs, in complying with paragraph 3.3 of Appendix D and paragraph 17.3 of the AML Guidelines; iii. Identify PEPs, and relevant family members or close associates of PEPs using reliable external databases and sources, in complying with paragraph 8.4.1 and paragraph 1.13 of Appendix B, AML Guidelines; and iv. Conduct robust customer risk profiling and the corresponding due diligence measures based on the risk profile identified, in complying with paragraph 8.2 of the AML Guidelines.	i. Undertake more rigorous verification processes in relation to customers assessed as higher-risk, including obtaining additional information on the customer's source of funds, conducting deeper investigations into the nature of the business activities or purpose of the customer's investments, in complying with paragraphs 8.3.1(a) - (c) of the AML Guidelines; ii. Where applicable, seek senior management approval before the onboarding of such customers (paragraph 8.3.1(e) of the AML Guidelines); and iii. Where monies are deposited by a third party into the customer's account with the RI (third party deposit), conduct relevant due diligence to determine the identity of the third-party payor, the relationship between the customer and the third-party payor, the reason for making deposits into the customer account and whether the third-party exercises trading authority over the customer's account (paragraph 7.6.3 and paragraph 2.6 of Appendix A1, AML Guidelines).	i. Record and keep documentation reflecting the shareholders identified through the cascading steps in paragraph 8.1.11 of the AML Guidelines (by reasonably exhausting all possible means) leading to the ultimate BO (paragraphs 8.1.11 - 8.1.13, and paragraph 1.1(b) of Appendix E, AML Guidelines); ii. Supplement the identification and verification of the ultimate BO with independent checks, via external databases or open sources, in complying with paragraph 1.1(b) of Appendix E, AML Guidelines; iii. Screen its customers' BOs during onboarding and on an ongoing basis against sanctions lists, in complying with paragraph 1.1(d) of Appendix E, AML Guidelines; iv. Risk profile or consider the ML/TF risks of its customers' BO(s) when risk profiling its customers (paragraph 1.1(c) of Appendix E, AML Guidelines); and v. Maintain a centralised database of BO information to ease identification of common BOs, in complying with paragraphs 1.1(a) and (b) of Appendix E, AML Guidelines.

4. Ongoing Due Diligence

In addition to undertaking CDD, a reporting institution is also required to perform ongoing customer due diligence (ODD) throughout the course of the business relationship with its customers whereby control measures implemented must be proportionate to the customers' risk profiles, with higher-risk customers being subjected to more frequent and detailed scrutiny.

The SC's Observations

The SC observed that RIs have implemented various measures for ODD including, updating of customer profiles, and transactions monitoring, as illustrated below.

Update of Customer Profile	Transactions Monitoring
	
• RIs periodically update customers' information and renew their risk profiles to ensure they remain accurate and are reflective of current risk factors and customers' circumstances. • Most RIs undertake a more frequent review for higher-risk customers (i.e. one to three years) while lower risk customers are subjected to a less frequent review (three to five years or upon a trigger event).	• There is an increasing trend in the adoption of automated systems for transactions monitoring. Currently, 80% of RIs utilise systems to perform this process. • RIs are transitioning towards incorporating behavioural-based and events-triggered parameters in their transactions monitoring scenarios, instead of solely relying on rules/threshold-based ones.

Further, the SC observed the following notable best practices that all reporting institutions are encouraged to undertake or have in place–

✓ Temporary suspension of a customer's account in the event the customer does not respond to the RI's request to update his profile.

✓ Screening of the customer database upon discovery of any publicly available adverse news that may affect the risk profile of any of its customers. For example, a RI should screen its customer database for name matches of key management personnel of any company in which competent authorities have performed raids, to determine whether such personnel have investment accounts with the RI.

Key Takeaways

In complying with paragraph 8.8 of the AML Guidelines, RIs should:

1. Take into consideration, changes to any information on BO in the renewal of a customer's ML/TF/PF risk profile;

2. Regularly review and update formulated parameters to ensure they remain relevant and appropriate to the RI's customer base and their risk profiles, product types and various distribution channels; and

3. Review transactions in their entirety across multiple accounts belonging to the same customer or BOs, or group of interconnected customers.

5. Targeted Financial Sanctions

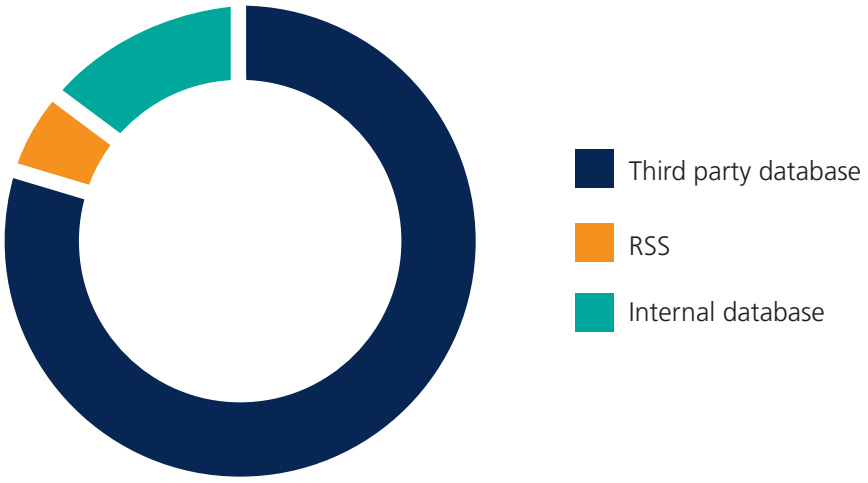
TFS imposed on countries as well as specifically identified individuals and entities (listed persons) under the relevant orders issued by the Ministry of Home Affairs (MOHA) and the various United Nations Security Council Resolutions (UNSCR), is a key component of the broader 'sanction regime' aimed at effectively disrupting financial transactions linked to known terrorist and proliferation networks. As such, it is essential for a reporting institution to also observe obligations in relation to TFS.

The SC's Observations

While RIs have formalised policies and procedures to conduct name screening of its customers and BOs against sanction lists at the onboarding stage and upon update of the sanctions lists, the sophistication of such screening varies across the RIs with some using automated systems and others manually conducting sanctions screening against the source data.

In terms of closure or clearance of alerts, most RIs require more than a day to review any name matches and clear alerts.

Methods for TFS screening across all RIs



Further, the SC observed the following notable best practices that all reporting institutions are encouraged to undertake or have in place:

- ✓ Conduct sanctions screening of individual transactions prior to making any payment or withdrawals to manage the risk of dissipation of funds.
- ✓ Undertake **'Delta (Δ) screening'** whereby changes to sanctions lists are screened against the entire customer database, and changes in the reporting institution's customer database is screened against the sanctions lists to ensure that reporting institutions have accounted for any updates in both the sanctions lists and the customer database.
- ✓ **Adoption of systems/technology** that allows combined permutations when performing screening which results in better quality alerts (e.g. combination of name matches, linguistic and mathematical edit distance-based algorithms, identification of typographical errors in names, etc).
- ✓ **Back testing of systems** to determine turnaround time for third-party providers to update sanctions lists.
- ✓ **Screening of BOs**.

Key Takeaways

Customer Screening

In complying with paragraph 14.4 of the AML Guidelines, RIs should:

i. Perform **sanction screening** and ensure **freezing of accounts** where there is a name match **without delay** from the update of sanctions lists;

ii. Implement **effective and efficient alert management system** to clear alerts raised from sanctions screening in a timely manner; and

iii. Implement relevant measures to mitigate the risk of dissipation of funds during the period of alerts clearing such as tagging of accounts with potential name matches after screening and exercising close monitoring, to ensure any activity in the relevant accounts will not result in breaches of TFS requirements.

Screening of Related Parties

i. **Conduct screening of parties related to a positive match** to determine if there are such persons in the RI's customer database e.g. through search of common addresses, common parent names, joint holder(s) of the relevant accounts, etc., in complying with paragraph 3.3 of Appendix D, AML Guidelines; and

ii. Upon determination of any related parties, review the relevant account and assess whether the account warrants a STR submission, in complying with paragraph 5.1 of Appendix D, AML Guidelines.

6. Law Enforcement Agencies

A reporting institution has the obligation to fully co-operate with relevant LEAs and, must comply with any investigation order issued by such LEAs under the AMLA in a timely manner. Such orders commonly require the reporting institution to undertake, among others, the following:

(a) Verify any information required to be disclosed to the LEAs under the relevant orders;

(b) Screen any transactions and respond to the LEA, as per requirements of the order;

(c) Review its customer's account, perform a risk re-rating and closely monitor the customer's account, where necessary; and

(d) Submission of STR to FIED, if required.

The SC's Observations

The SC observed the following notable best practices that all reporting institutions are encouraged to undertake or have in place:

✓ Incorporation of enforcement orders by LEAs into the RI's internal watchlist for a pre-determined duration for monitoring new customers.

✓ Screening of BOs against orders by LEAs.

II. Emerging AML Trends and Techniques

In addition to the thematic review undertaken, the SC has also observed various techniques used in perpetuating ML activities as highlighted below, and effective controls for detection and prevention that may be adopted by reporting institutions.

(a) Use of offshore money lenders to finance investments

Funds are initially transferred into an offshore account to be utilised as collateral to secure a loan from an offshore money lender. The procured loan is subsequently transferred to local clients for the purpose of subscribing to investments via private placement exercises, thereby making the funds appear legitimate.

In this scenario, the following indicators would suggest suspicious activity, and warrant further investigation:

(i) Recurring presence of a common customer in multiple private placement exercises;

(ii) Multiple customers sharing the same registered address, suggesting the possible use of fictitious identities to disguise beneficial ownership;

(iii) Transactions being inconsistent with the known financial profiles of customers i.e. where the value of the transaction is excessive in comparison with the financial position of the customer that is known to the reporting institution; and

(iv) Third-party financing from offshore entities with no clear business relationship with the customers for the purpose of subscribing for private placement shares.

Steps to be taken by reporting institutions in the above scenario may include:

- Reviewing the customer's profile with a view to better understand the reasonableness of the transaction i.e. customer's subscription, including assessing their latest employment and annual income as well as the possibility of additional sources of income or funds. This would assist reporting institutions to determine whether the customer's declared annual income is commensurate with the total value of the subscription.
- Determining the relationship between the third-party payor (financier) and the customer, and reason(s) for the financier making payments on behalf of the customers.
- Determining whether the third-party exercises trading authority over the customer to identify the true BO or the origin of funds.

(b) Use of shell companies to disguise beneficial ownership

Shell companies with no genuine business activities are often used to move illicit funds as they serve to hide, if not, obscure the true identity of their owners. The opacity of such transactions is further exacerbated by the use of complex corporate structures and nominee directors.

Money funnelled through shell companies often enters the financial system without raising suspicion, making it appear as if the transactions are legitimate business dealings.

The following indicators commonly raise suspicion and warrant further investigation:

Financial Irregularities

- Transactions that are large, repetitive, or involve large sums of cash without a legitimate business rationale.
- Company receiving loans from private third parties without any supporting loan agreements.

Use of Nominees

- Person appointed as executive director, but the executive director is not involved in the day-to-day operations or decision-making processes.

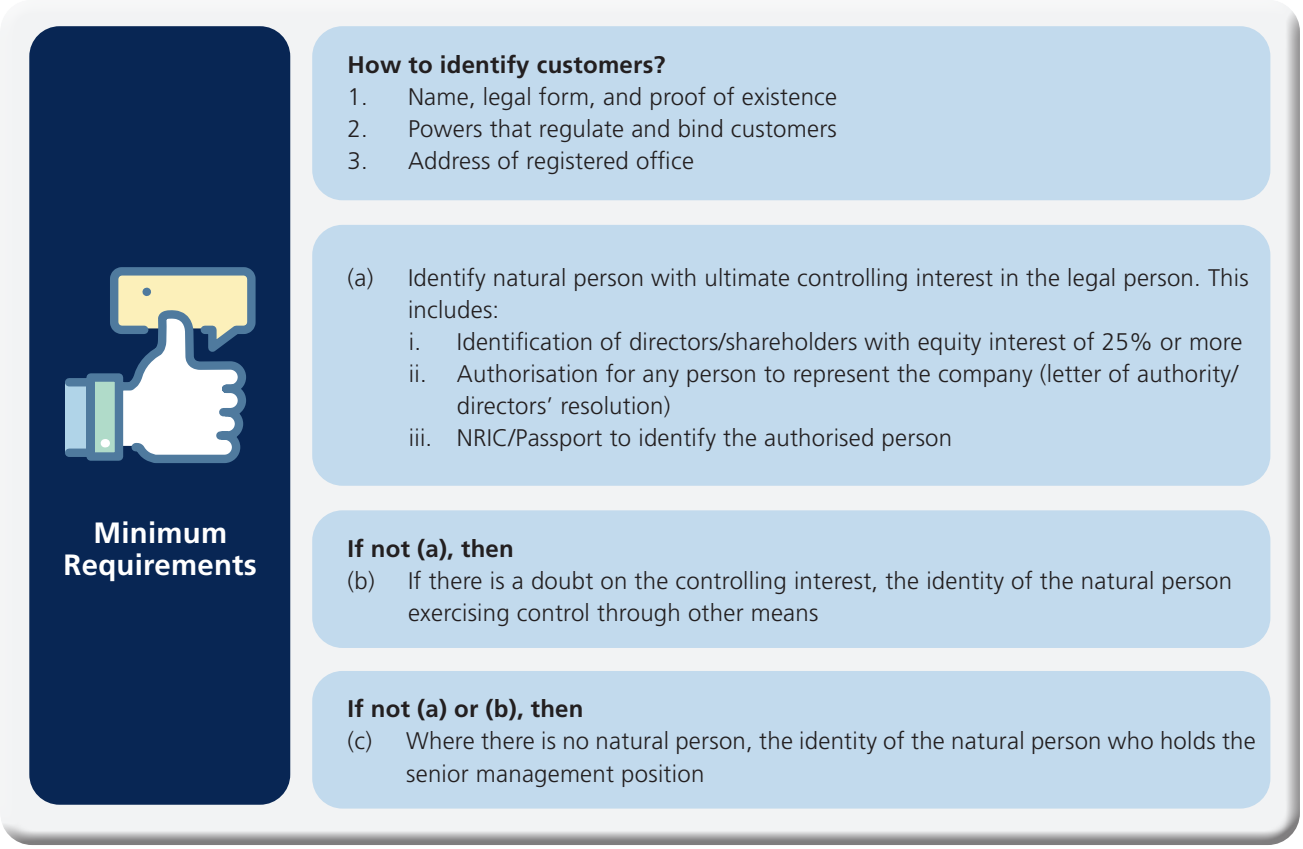
Transactions with No Apparent Business

- Funds from third party to the company owned by the other individual without any clear business purpose.

Dormant Company

- A company that has no employees, no physical presence, and only engages in transactions that appear to pass through the company without generating income.

Unveiling shell company schemes requires reporting institutions to identify the BO(s) who effectively control these entities behind the scenes. Below is a snapshot of the basic steps to be taken by reporting institutions to reveal such BO(s):

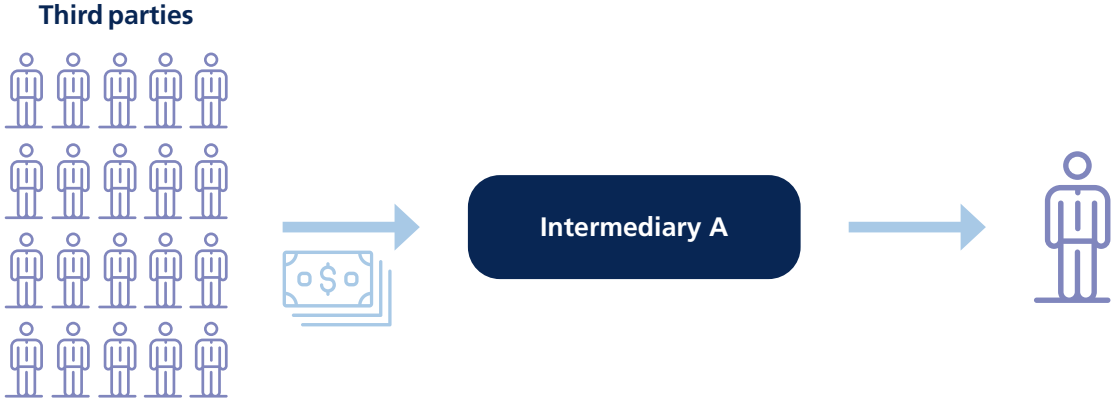


(c) Third-party Deposits

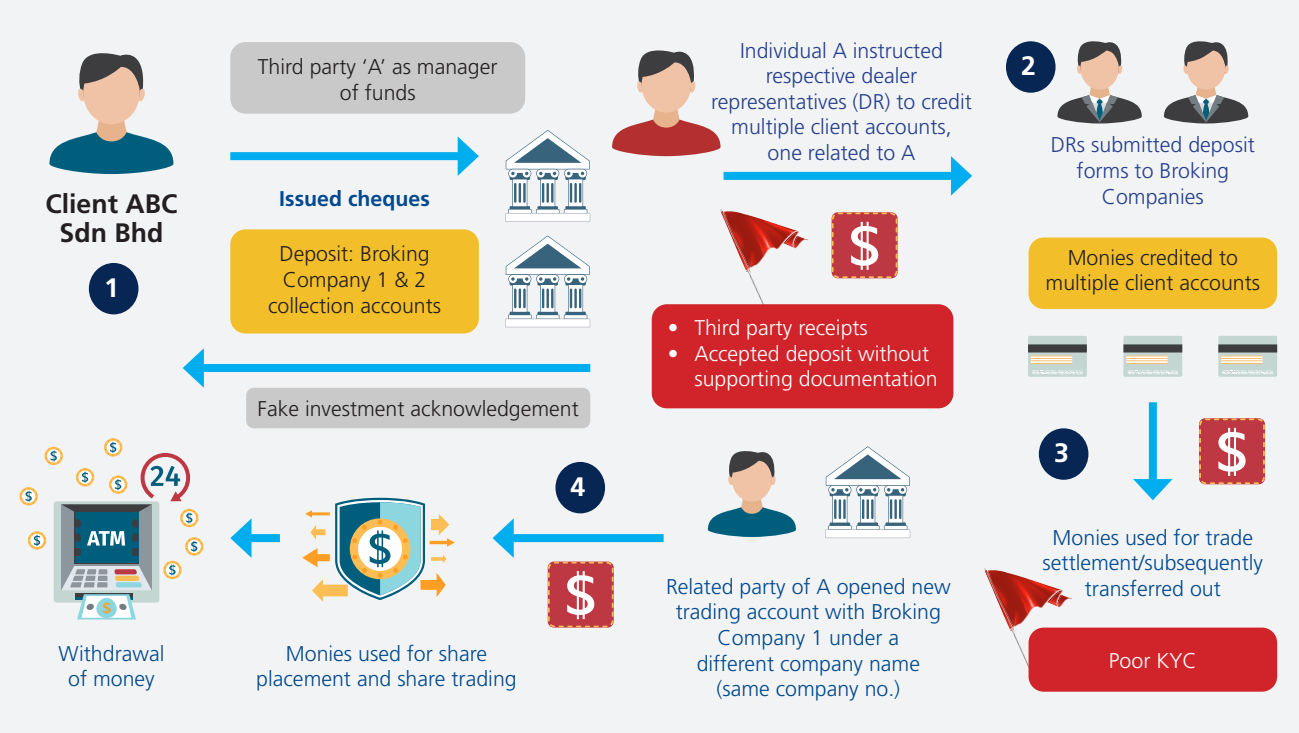
Third-party deposits can be used to integrate or legitimise illicit funds into the financial markets due to the complexity and opacity of the transactions involved. Third-party deposits involve transactions where the true BO or the origin of funds is obscured.

Common indicators of suspicious activity arising from third-party deposits are as follows:

(i) Multiple individuals making deposits into a single account, which is inconsistent with the account holder's profile

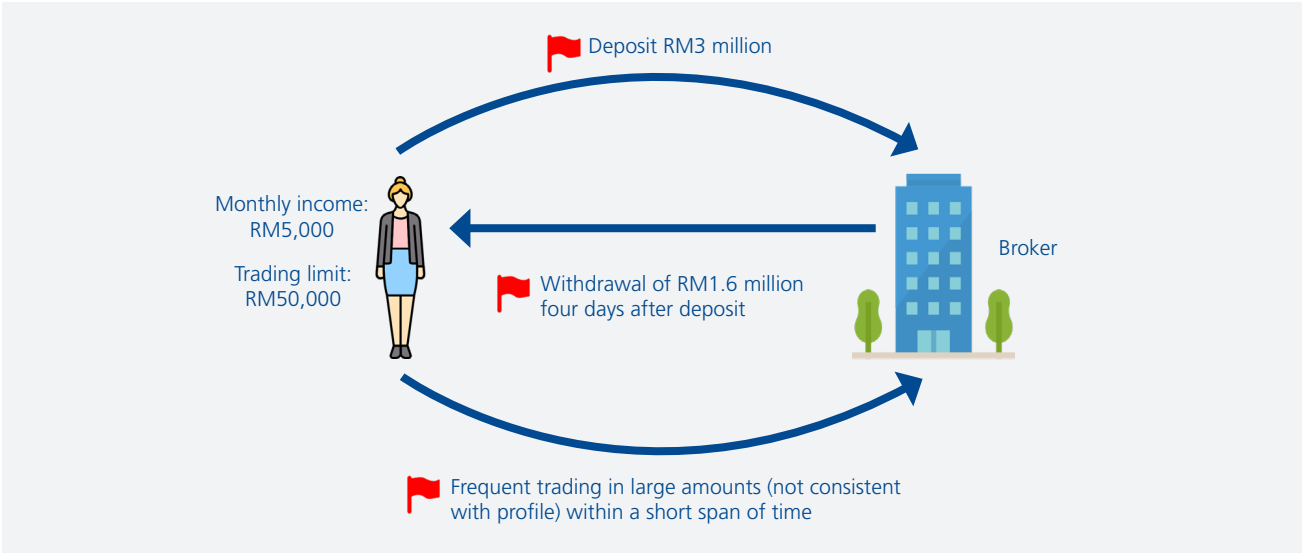


(ii) Deposits of large cheques or bank drafts from third parties



The pattern of third-party deposits and subsequent withdrawals raise red flags for potential ML activities.

(iii) Transactions that do not match the customer's known business activities resulting in unexplained source of wealth or income of the customer



The risks associated with third-party deposits in the context of ML are significant and multifaceted. Effective mitigation requires EDD practices to be undertaken by reporting institutions, and the use of advanced technology in screening such transactions.

In this respect, the SC expects reporting institutions to undertake the following measures:

Conduct a comprehensive risk assessment to determine the circumstances under which third-party deposits can be accepted

Establish and enforce clear, comprehensive, and effective policies and procedures in relation to third-party deposits

Perform due diligence on third-party deposits to ascertain:

- The identity of the third-party payor, including identification number, residential address, and contact number.
- The relationship between the customer and the third-party payor.
- The reason for making deposits into the customer's account.

Implement effective monitoring systems and controls to identify and accept third-party deposits, including obtaining relevant supporting documents from customers to verify the payor of the transactions. For example:

- Require a copy or image of the customer's cheque(s) to be submitted with the investment application/ transaction form to verify the payer's identity.
- Require a copy of the customer's original application form for remittance to be submitted with the investment application/transaction form to verify the issuer of the banker's cheque.
- Require a copy of the customer's transfer or bank-in slips, containing at minimum the depositor's name, to be submitted with the investment application/ transaction form to verify the transferor's identity.

Conclusion

While the SC remains steadfast in its commitment to continually develop and where necessary, strengthen its AML/CFT/CPF regulatory and supervisory framework as a means to preserve the integrity of the capital market, reporting institutions must also remain vigilant and agile in its efforts to effectively implement and update relevant policies and strategies in these areas in compliance with the relevant regulatory requirements and to address or mitigate the risks arising from the ever-evolving nature of ML/TF/PF activities, as discussed above.

FOR MORE INFORMATION

No opinions and articles published in *The Reporter* are exhaustive on the subject or topic they cover and are not intended to be a substitute for legal advice or opinion on the topic. Under no circumstances shall the SC be liable to any person for actions and decisions taken from reliance on any information contained in *The Reporter.*

If you have queries or comments, please contact:

Corporate Affairs Department
Securities Commission Malaysia
3, Persiaran Bukit Kiara, Bukit Kiara
50490 Kuala Lumpur
Malaysia

Tel +603 6204 8777
Fax +603 6201 5078
Email cau@seccom.com.my
Websites www.sc.com.my | ww.investsmartsc.my

@SecComMalaysia