

Scams and Unlicensed activities

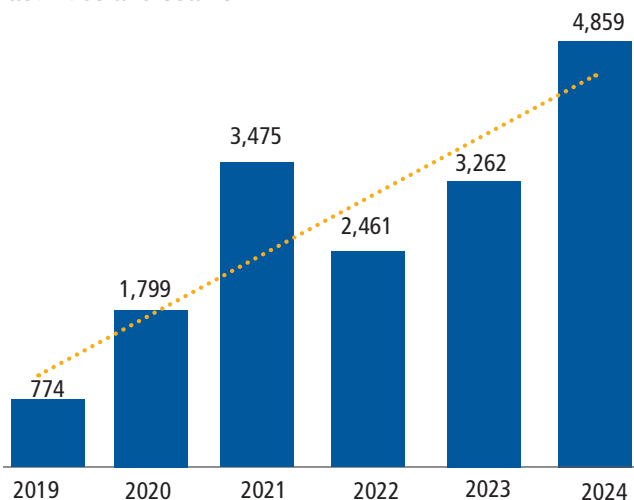
Complaints and inquiries on scams and unlicensed activities have been consistently rising with a 337% increase from 2019 to 2024. However, while the overall increase appears alarming, it is encouraging that more people are reporting scams and unlicensed activities without falling victims to these activities and scams before coming forth to the SC. Through the complaints and enquiries received, the SC managed to gain insight on the prevailing trends and emerging modus operandi. This in turn allowed SC to expeditiously take the necessary interventions so that the illegal activity can be curbed to avoid more people from falling victim.

Surveillance of Unlicensed Activities

In addition to complaints and enquiries received from the public, the SC also established a dedicated Surveillance of Unlicensed Activities (SUA) unit in 2022 to proactively address the rising risks posed by unlicensed market participants.

Over the years, the SUA unit has uncovered emerging trends, including the increasing use of social media platforms and influencers to promote unlicensed products and services, as well as the growing prevalence of deepfake technology being used to impersonate influential and prominent figures in fraudulent activities. The SUA unit has observed another notable shift in money transfer methods, with some schemes utilising third-party payment gateway services for financial transactions rather than transfers of money to personal bank accounts to avoid suspicion and evade detection.

CHART 4
Complaints and enquiries on scams and unlicensed activities and scams



As of 31 December 2024, the SC identified a total of 796 URLs (2023: 569 URLs) across various websites and social media for potential breaches related to the offering of unlicensed products and services to Malaysians. Among these, 59% originated from Telegram, 19% from Facebook, 13% from websites, 4% from Instagram and 5% from other sources including TikTok, X, and YouTube.

Broad Types Identified

The complaints and inquiries received by the SC and those identified through our surveillance can generally be divided into two categories:

- **Scams** – including various types of scams, such as those involving non-existent investment products.
- **Unlicensed activities** – where individuals or entities conduct regulated business without being licensed or registered with the SC.

Investment Scams

The primary difference between an investment scam and other types of scams lies in the nature of the deception and the focus of the fraudulent activity. For instance, in an investment scam, the deception revolves around financial investments where promises of high returns or low-risk opportunities that either do not exist or are not as they are represented. They exploit people's desire for financial gain by misleading them about the nature, profitability, or legitimacy of the investment.

Despite the widespread awareness of investment scams, there are still a number of people who continue to be exposed to and/or fall victim as represented in the continuous rise on the number of complaints. The reason for people to continue to fall for such scams can be due to several factors:

- **Lack of Basic Investment Knowledge:** A significant portion of the population does not have the basic understanding of investment principles. They may struggle to grasp complex financial instruments or recognise the red flags when it is a scam. According to a recent survey by the SC,⁷ many investors rely on third-party information sources, such as advice from friends or family, which can lead to poor decision-making.

⁷ Report titled *Understanding the Level of Vulnerability towards Investment Scams and Readiness for Retirement Planning*.

- **Greed and Desire for Quick Profits:** Scammers often manipulate their victims by promising high returns with minimal risk. This allure of quick money may appeal to individuals who may not fully understand the associated risks.
- **Trust in Authority:** Scammers frequently impersonate trustworthy figures, such as government officials, reputable organisations, or well-known personalities. This can mislead people into believing that the investment opportunity is legitimate.
- **Psychological Manipulation:** Scammers employ psychological tactics, such as creating a sense of urgency with 'limited-time offers' or using fake testimonials for social proof. These strategies can pressure victims into making hasty decisions.
- **Emergence of New Tactics:** While efforts are being made to raise awareness about scams, scammers are constantly evolving and developing new tactics such as getting victims to pay in the form of digital assets as the mode of payment compared to traditional fiat currency.

These factors contribute to the ongoing vulnerability of individuals to investment scams.

Emerging Scam Trends

The SC continuously monitors emerging trends and methods related to scams to ensure appropriate and timely interventions are taken. In 2024, some of the notable new trends observed by the SC are:

A. Use of Deepfakes

Scammers use deepfakes, generated by artificial intelligence (AI), to impersonate prominent individuals and reputable companies (including the SC's Intermediaries). These videos often feature public figures or well-known brands, lending false credibility to fraudulent schemes. The AI manipulates the video to closely match the voices and appearances of these figures, making fake investment opportunities seem legitimate. Typically, these deepfake videos promote investments supposedly backed by well-known companies. The scam posts include a 'Learn More' button or link, directing viewers to a sign-up page that collects personal information. Those who access the link are also asked to download an application, which puts them at risk of

cybercrime. Once signed up, potential victims are contacted by fraudulent agents who deceive them into transferring money into mule bank accounts.

B. Pre-IPO Investment Scams

Mostly involving private placement offerings, such scams are usually timed with upcoming IPO listings published on Bursa Malaysia's website. Perpetrators of these scams, posing as 'agents', usually create a public group on WhatsApp to promote these pre-IPO investments. Following this, potential victims will be added into said group unsolicited. These schemes may be accompanied by fake testimonials from other investors to appear credible. Payments for the 'subscription' will be required to be made to bank accounts of entities not related to the IPO and suspected of being mule bank accounts. On the IPO listing day, these 'agents' will proclaim that the IPO shares have been listed and had made profits, and that additional payments are needed for their shares to be allotted. This is to convince the victims to part with more money.

Arising from the above emerging concerns, the SC took out media releases on 4 July 2024 titled 'SC warns public on pre-IPO investment scams', and on 22 July 2024 titled 'SC warns public on deepfake investment scams'.

C. Scams using Company Mule Bank Accounts Instead of Bank Accounts of Individuals

The SC observed the use of companies incorporated with Suruhanjaya Syarikat Malaysia (SSM) as mule bank accounts. The fraudsters will use bank accounts of existing but dormant companies with no business operations to receive and transfer illicit funds.

In the past, the SC observed mostly the use of individual bank accounts as mules to disguise their operations. On this, the SC in 2022 took enforcement actions against 19 mule account holders. By operating under the guise of a legitimate business entity, scammers can create a false sense of trust and credibility, making potential victims more susceptible.

The observations above align with a global trend seen in other jurisdictions, indicating that the challenges faced by Malaysians are not unique but reflect issues occurring worldwide.

Arising from the above emerging concerns, the SC, where necessary, took out media releases on 4 July 2024 titled 'SC Warns Public on Pre-IPO Investment Scams',

on 22 July 2024 titled 'SC Warns Public on Deepfake Investment Scams' and on 9 December 2024 titled 'SC Alerts Public on Fake Investment Letters Using SC's Name'.

Measures Implemented to Curb Scams and Unlicensed Activities

The SC strengthened its monitoring and surveillance of scams and unlicensed activities offered online, including through websites and social media platforms. The SC undertook a proactive approach in combatting scams and unlicensed activities by conducting early intervention and disrupting the activities including inclusion in the SC's Investor Alert List, blocking of the websites and social media platforms as well as collaborating and co-ordinating with the relevant authorities. The SC had also adopted social media intervention strategies where messages will be publicly posted on social media pages of suspected scammers and unlicensed activities operators, to warn the operators that the SC is aware of their activities and that they are in breach of securities laws.

In addition, where the breach of securities laws is established, appropriate enforcement action will also be taken. Enforcement actions are taken based on several factors including but not limited to sufficient and conclusive evidence.

In addition to the above interventions, the SC in 2024 embarked on a new intervention approach namely by issuing notification letters to local banks alerting them regarding possible mule bank accounts involved in unlicensed activity cases uncovered by the SC.

The SC revises Guidance Note on Investment Advice to include Finfluencers

The SC observed concerns on the conduct of financial influencers or commonly known as finfluencers, whose activity (among others) may constitute providing of unlicensed investment advice. To strengthen and intensify investor protection, the SC has among others, updated its Guidance Note on the Provision of Investment Advice. The Guidance Note clarifies which finfluencers' activities may constitute investment advice and, consequently, must comply with the CMSA. Additionally, the SC has issued **warning letters** to the identified third-party Malaysian payment gateway operators involved in facilitating unlicensed activities. Accompanying this, the SC also published an informative infographic with Frequently Asked Questions and a checklist. The SC will continue to address any developments and trends through, among others, issuance of guidance to the public.

TABLE 18
Intervention efforts on scams and unlicensed activities

| Actions Taken | 2024 | 2023 |
|--|------|------|
| Commencement of enforcement action | 4 | 4 |
| Inclusion in the SC's Investor Alert List | 273 | 315 |
| Blocking of websites with assistance from Malaysian Communication and Multimedia Commission (MCMC) | 153 | 146 |
| Facebook and Instagram Accounts Geo-Block | 81 | 95 |
| Request to block Telegram accounts | 180 | 153 |
| Social media interventions | 336 | 420 |
| Lodgement of police reports | 141 | 97 |
| Referrals to other agencies/foreign regulators | 235 | 128 |
| Issuance of Notices of Cease and Desist | 3 | 5 |

The SC Addresses Regulatory Concerns Over Unregistered Digital Asset Exchange Operators

The offering and trading of digital assets in Malaysia are regulated by the SC. Digital assets, which comprise of both, digital currencies and digital tokens, are prescribed as securities pursuant to the *Capital Markets and Services (Securities Regulations) (Digital Currencies and Digital Tokens) Prescription Order 2019* (Prescription Order), which came into force on 15 January 2019.

Anyone who wishes to trade in digital assets may do so through a Digital Asset Exchange. Any person who operates or maintains a Digital Asset Exchange (DAX) in Malaysia must be registered with the SC as a recognized market operator (RMO). And any person who intends to operate a DAX must comply with the *Guidelines on Recognized Markets* (RMO Guidelines) and will be subjected to ongoing requirements applicable to an RMO pursuant to the said RMO Guidelines.

A DAX that operates in Malaysia i.e. targets Malaysian investors without being registered with the SC will be in breach of the CMSA. The SC considers a DAX to be actively targeting Malaysian investors if its operator or the operator's representative directly or indirectly promotes the DAX in Malaysia. Examples of such promotions are having MYR denomination as option to trade on their platform, advertising the DAX in any publication in Malaysia, or sending any direct mail or email to Malaysian addresses to market or promote the DAX.

Following the coming into force of the Prescription Order in January 2019 the SC received 996 complaints and enquiries on unregistered DAX operators.

| | 2020 | 2021 | 2022 | 2023 | 2024 |
|--------------------------|------|------|------|------|------|
| Complaints and Enquiries | 117 | 241 | 76 | 343 | 219 |

These are mainly DAX operators that may be licensed or regulated by foreign regulators but were found to be soliciting Malaysian investors. There are instances where the DAX platforms are completely fake, with no real trading activities taking place. Investors are misled into believing they are participating in legitimate trades, while their money is being siphoned off by the scammers. These fraudulent platforms often provide no information about their location or any legitimate company backing, placing them beyond the SC's regulatory reach and making it difficult to track them down.

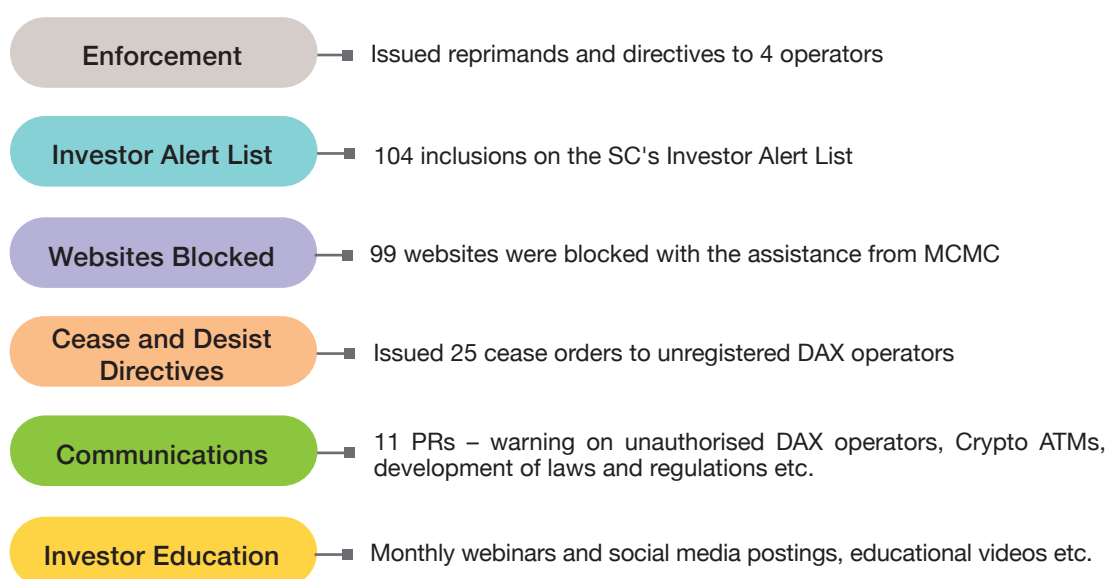
The SC received multiple complaints involving monetary losses / dispute from investors who invested through such unregistered DAX operators. Based on the information shared by complainants, most of these operators who targeted Malaysians were not responsive to the emails or calls made by the complainants seeking explanation. Therefore, Malaysians who invest with these operators may not have the requisite protection or recourse in the event of any disputes. For an orderly development of the RMO markets in Malaysia and to ensure investor protection, the SC has in place the requirements for a DAX to be properly registered.

In response to the prevalence of unauthorised DAX operators, the SC adopted a multi-pronged approach to suppress the concern via enforcement actions, investor alerts, blocking of websites (done through the assistance of the Malaysian Communications and Multimedia Commission), cease and desist directives, and investor education initiatives.

To date, the SC has taken enforcement actions against four unauthorised DAXs over the past years with the latest being in November 2024 against ByBit. These DAX operators rank among the largest by trading volume and have a significant global presence but were found to be soliciting Malaysian investors. Consideration on whether enforcement action should be initiated is always based on availability of evidence, the desired outcomes and whether there are alternative means to achieve the same outcome.

In the case of ByBit, the SC reprimanded ByBit pursuant to Section 354(3) of the CMSA and issued directives to disable their websites and mobile applications (in the Apple Store and Google Play Store). They were also required to immediately cease circulating, publishing, or sending any advertisements, whether via email or other means, to Malaysian investors. This action by the SC in 2024 is consistent with the actions that the SC has taken against Binance, Remitano (in 2020) and Huobi (in 2023), following the coming into force of the Prescription Order in January 2019.

The SC will continue to monitor and take such actions as necessary, including enforcement actions to protect Malaysian investors and to serve as a deterrent to those who seek to carry on their business in Malaysia illegally.



While the SC will continue to play its part, including monitoring and undertaking measures to detect and act against such illegal activities involving unregistered DAX, the public should also take responsibility and exercise judgment and caution. Investors who have been solicited to invest in a DAX, located in or outside Malaysia, which is not registered with the SC may report to the SC for appropriate action to be taken.