



UAE Introduces New VAT Regulations Affecting Virtual Assets: What Businesses Need to Know

On 6 September 2024, the UAE Cabinet issued Cabinet Decision No. 100 of 2024, significantly amending the [Federal Decree-Law No. 8 of 2017 on Value Added Tax](#). This announcement introduced amendments specifically addressing the VAT treatment of virtual assets and other financial services. These changes are designed to clarify how businesses should approach the taxation of digital assets, such as cryptocurrencies, as the UAE continues to adapt its tax laws to the evolving digital economy. The new rules are scheduled to come into effect on 15 November 2024, and businesses involved with virtual assets must ensure they comply with these updated regulations to avoid penalties.

Under the previous VAT framework, the treatment of virtual assets, including cryptocurrencies and other digital tokens, was not clearly defined. This ambiguity led to varying interpretations and inconsistencies in VAT reporting for businesses dealing with virtual currencies. With the Cabinet Decision No. 100 of 2024, virtual assets are now officially included under the definition of financial services, and specific guidance is provided on when these assets and the related services are subject to VAT.

The new regulations provide that virtual assets, defined as digital representations of value that can be traded or used for investment purposes, will be treated similarly to traditional financial products like stocks or bonds in terms of VAT. This change applies to services like the conversion, management, and transfer of virtual assets, which will now be taxable if conducted for an explicit fee, commission, or other financial consideration. On the other hand, if these services are offered without a direct fee or commission, they will remain VAT exempt, aligning with the treatment of traditional financial services.

Those companies that handle virtual assets, including cryptocurrency exchanges, wallet providers, and businesses using virtual assets as part of their operational models must adhere to these amendments to ensure compliance. Services related to virtual assets, such as conversion, management, and transfer, will now be taxable at 5% VAT if they involve explicit fees, commissions, or rebates. However, services provided without direct fees, like custody or management of virtual assets, will remain VAT-exempt. They will be required to charge VAT on services related to virtual assets where an explicit fee or commission is charged. This could lead to an increase in taxable income for businesses providing such services, as they now need to apply the standard VAT rate to these transactions.

When an exchange charges a commission for converting one cryptocurrency to another, these services will now attract VAT. Companies must ensure that they are prepared for this by updating their accounting systems and pricing models to reflect the VAT that must be collected on such transactions.

While the standard VAT rate of 5% remains unchanged, the significant difference lies in the scope of application for businesses dealing with virtual assets. Services that were previously not clearly subject to VAT, such as the transfer and conversion of virtual assets, will now attract the 5% VAT rate when conducted for explicit fees. Businesses must consider the impact on capital assets involving virtual assets. The amendments introduce rules for making VAT adjustments on capital assets, including virtual assets. For instance, if virtual assets form part of a company's capital, any changes in their taxable use will require an annual VAT adjustment. For buildings and real estate, this adjustment is spread over 10 years, while for other capital assets, such as virtual assets, the adjustment period is 5 years.

There is no specific percentage increase or decrease in the VAT rate itself; however, the expansion of taxable services and annual adjustments on capital assets may result in a noticeable financial impact for companies heavily involved in virtual asset transactions. The need to adjust for VAT on capital assets means that companies will have to account for potential increases in VAT liability if their asset usage shifts toward taxable activities.

The changes introduced by Cabinet Decision No. 100 of 2024 will come into effect on 15 November 2024, with just a month to prepare to implement these new amendments. Companies dealing with virtual assets to ensure that they have updated their tax compliance procedures will be revising their invoicing systems to accurately charge VAT on all taxable services related to virtual assets.

Businesses need to ensure they have systems in place to differentiate between services that are taxable and those that are exempt. For instance, services that do not involve an explicit fee, such as providing custody of virtual assets without direct compensation, will remain exempt from VAT. On the other hand, services such as trading or managing virtual assets for a commission will be subject to VAT, and businesses need to apply this distinction in their VAT reporting.

The introduction of Cabinet Decision No. 100 of 2024 has brought virtual assets into the same regulatory framework as traditional financial services and the UAE government has clarified the tax obligations for companies dealing with these digital assets, particularly for businesses that charge fees for converting, managing, or transferring virtual assets, as these services will now be subject to VAT. Virtual asset-related services are taxable under the new UAE VAT rules if they involve explicit fees, commissions, or discounts. Services offered without direct financial compensation remain VAT-exempt.

In the run-up to 15 November 2024, businesses must take the necessary steps to review their current service offerings and ensure that VAT is correctly applied to taxable transactions, and adjusting their internal accounting systems to reflect these changes. Companies should clearly understand how the new VAT adjustments on capital assets, including virtual assets, will affect their overall tax liabilities.

(Source: <https://tax.gov.ae//Datafolder/Files/Legislation/Executive%20Regulation%20of%20Federal%20Decree%20Law%20No%208%20of%202017%20-%20Publish%20-%2004%2010%202024.pdf>)

South Korean FSC Announces Establishment of Digital Asset Protection Foundation to Secure Safe Return of Funds Amid VASP Closures

On 25 September 2024, the South Korean Financial Services Commission (**SK FSC**) announced its authorization of the digital asset industry's plan to create the Digital Asset Protection Foundation, an entity aimed at safeguarding users' assets in the event of virtual asset service providers shutting down. This initiative, led by the Digital Asset Exchange Association (**DAXA**) aims to move toward protecting virtual asset users' rights and maintaining stability in the market. The foundation will be responsible for receiving, managing, and securely returning users' assets that were previously held by defunct exchange service providers after a structured consultation process.

The establishment of this foundation comes in response to growing concerns about the ability of VASPs to return users' assets following business closures. Despite previous efforts by financial authorities, such as issuing guidelines for VASP closures and conducting inspections on closed exchanges, the lengthy and complex process of

returning assets continues to create uncertainty for users. With ten out of twenty-two coin market exchange operators already out of business and three more having suspended operations, it has become clear that without a structured system in place, resuming business or recovering users' assets is highly unlikely for these operators.

The challenge is further complicated by the fact that many closed VASPs hold private keys to users' wallets, increasing the risk of asset loss or mismanagement. Recognizing the need for a more systematic and secure method for managing these assets, authorities emphasised the importance of creating a dedicated foundation to handle this task. The foundation, as a nonprofit entity, will step in where these VASPs can no longer operate, ensuring users' funds are securely managed and eventually returned.

DAXA has been instrumental in the development of this initiative, working under the FSC's guidance to build a solution that aligns with the industry's self-regulatory efforts. Once established, the foundation will engage in consultation with each exchange service provider to transfer users' funds and digital assets under its care. In the interest of efficiency and security, users' cash deposits will be stored in banks, while a designated KRW-based exchange service provider will manage their digital assets. This structure is designed to ensure a safe and transparent process, giving users confidence in the protection of their funds.

To further enhance the foundation's effectiveness, an operating committee will be formed, comprising representatives from the bank, the KRW-based exchange service provider, Korea Inclusive Finance Agency, Financial Security Institute, and private sector experts. This committee will oversee critical issues related to asset protection and ensure compliance with the Virtual Asset User Protection Act, as well as the established guidelines for VASP business closures.

Financial authorities will also play an active role in supporting the foundation's operations, facilitating smooth communication and asset transfer processes between the foundation and the closed VASPs. Additionally, for VASPs that are expected to terminate operations following a renewal of registration under the Act on Reporting and Using Specified Financial Transaction Information, authorities will guide them in transferring their customers' assets to the foundation.

Following FSC approval, the foundation will be officially established upon the completion of court registration, with operations expected to commence as early as October 2024. The foundation will immediately begin consultations with closed VASPs regarding asset transfers, providing users with a reliable mechanism for recovering their funds. The establishment of this foundation is seen as a critical move in protecting users' assets and promoting greater order in the virtual asset market. By minimising the disruption caused by VASP closures, it will also help maintain user confidence and prevent potential market instability.

(Source: <https://www.fsc.go.kr/eng/pr010101/83126?srchCtgr=&curPage=&srchKey=&srchText=&srch-BEGINDt=&srchEndDt=>)

HKVAX Secures Regulatory Licenses, Strengthening Its Position as a Leading Virtual Asset Platform in Hong Kong

On 2 October 2024, Hong Kong Virtual Asset Exchange (**HKVAX**) officially announced that it had obtained Type 1 (dealing in securities) and Type 7 (providing automated trading services) licenses from the Hong Kong's Securities and Futures Commission (**HK SFC**), along with a license under the Hong Kong's Anti-Money Laundering and Counter-Terrorist Financing Ordinance (**AMLO**). This development makes HKVAX the third regulated virtual asset platform in Hong Kong, joining the ranks of HashKey Group and OSL, which are currently the only operators permitted to serve retail customers in the territory.

HKVAX was established with a strong focus on combining traditional financial services with blockchain technology, providing a wide array of virtual asset services. These include over-the-counter (**OTC**) trading, a 24/7 trading platform, and asset custody with advanced security features such as multi-signature technology and wallet separation. The platform has a particular emphasis on Security Token Offerings (**STOs**) and Real-World Asset (**RWA**) tokenization, which aim to enhance asset liquidity and create new opportunities for professional investors. The newly obtained licenses will enable HKVAX to further integrate these offerings into a virtual asset ecosystem, which will support its expansion.

With the acquisition of these licenses, HKVAX has solidified its position in the regulated virtual asset market in Hong Kong. The Type 1 license enables the platform to deal in securities, while the Type 7 license allows it to provide automated trading services, both of which are governed by the Hong Kong's Securities and Futures Ordinance (**SFO**). Hong Kong's AMLO license ensures that the platform adheres to anti-money laundering (**AML**) and counter-terrorist financing (**CTF**) standards and HKVAX will implement Know Your Customer (**KYC**) protocols, alongside other security measures to protect investor assets and enhance market transparency.

The licensing process required HKVAX to demonstrate full compliance with several regulations, including the need for strong capital reserves, secure custody practices, and advanced cybersecurity protocols..

In a statement, Anthony Ng, Co-Founder and CEO of HKVAX, remarked, "We are part of a financial landscape revolution, aiming to establish Hong Kong as the STO and RWA center for Asia and beyond."

To strengthen its ecosystem, HKVAX has been forming partnerships with industry players, including brokers, Money Service Operators (**MSOs**), and Exchange Traded Fund (**ETF**) issuers to build a virtual asset infrastructure that supports the growth of Hong Kong's financial innovation sector. The company also plans to introduce end-to-end virtual asset management services, including consulting on asset tokenization, technical support, token issuance, secondary market trading, and comprehensive custody solutions. The company's focus on STOs and RWAs positions it well to capitalize on emerging trends in the global financial markets. HKVAX plans to enhance its services, particularly in the areas of STOs and RWAs, providing institutional and professional investors with more opportunities to engage in secure and transparent trading.

(Source: <https://www.hkvax.com/news/detail?diffId=1828727641257852928>)

G7 Competition Authorities and Policymakers Summit: Framework to Ensure Fair Competition in AI Markets

On 3 October 2024, the G7 Competition Authorities and Policymakers Summit met in Rome, Italy, to address the competitive challenges presented by the rapid advancement of artificial intelligence technologies, including Generative AI (GenAI). This gathering, hosted by the Italian Competition Authority, followed up on discussions initiated during the G7 Industry, Technology and Digital Ministerial Meeting in March 2024 and the Tokyo Summit in 2023. The discussions in Rome centered around ensuring that AI-driven innovations foster healthy competition while mitigating risks of market concentration and unfair practices. The US Justice Department's Antitrust Division and the Federal Trade Commission participated in the summit.

The **communiqué** discusses the transformative potential of AI for economies and societies along with its ability to increase productivity and spur innovation across multiple sectors. However, the communiqué also stresses that to fully reap the benefits of AI, it is crucial to maintain open and contestable markets. The G7 participants voiced concerns that certain characteristics of AI markets, particularly in the development of GenAI, could lead to the concentration of market power, stifling innovation and competition. These concerns include the high costs associated with AI development, economies of scale that favor large players, and network effects that could entrench incumbents. The accumulation of proprietary data and the creation of data feedback loops could further exacerbate these issues, making it difficult for new entrants to compete.

The communiqué notes that the availability of critical inputs, such as computing infrastructure, specialized chips, and AI talent, is increasingly controlled by a small number of firms which could create bottlenecks, limiting access for new entrants and heightening competition concerns. The partnerships between large AI companies and incumbent digital platforms, many of which already hold substantial market power, also raise alarms about the potential for these incumbents to consolidate their dominance across both digital and AI markets.

Throughout the discussions, the participants agreed that dominant firms with significant influence in digital markets might use their power to extend control over AI markets. Practices such as self-preferencing, bundling, and leveraging network effects could restrict consumer choices and raise barriers to entry for smaller competitors. The risk of collusion using AI algorithms, whether through pricing coordination or the sharing of sensitive competitive information, was also flagged as a potential concern. Such practices could harm consumers by facilitating price fixing or surveillance pricing, ultimately undermining competition and trust in AI-driven markets.

The communiqué expands the scope of the competition issues into broader societal concerns. AI's reliance on human-generated content, such as art, writing, and intellectual property, for its training raises questions about the protection of creators and the potential suppression of innovation in these areas. With a limited number of firms controlling the AI ecosystem, creators may be undercompensated, and new innovations could be stifled. Protecting consumer rights is another pressing issue, with the potential for AI-generated outputs to mislead or manipulate consumer decision-making. The sheer volume of data required for AI systems, coupled with concerns about privacy and data protection, reinforces the need for stringent compliance with existing rules and regulations to safeguard personal data and maintain public trust.

In response to these challenges, the communiqué outlines several guiding principles to ensure that AI markets remain open, fair, and conducive to innovation. It calls for proactive measures to prevent dominant digital platforms from exploiting their market positions and foreclosing competition by ensuring that AI chips and training data remain accessible to new entrants to foster a competitive environment. Openness and interoperability are key tenets, with the belief that consumers, businesses, and innovation will benefit from systems that allow for flexibility, switching, and diversity of models in the AI marketplace. Transparency, both in terms of AI's data usage and its limitations, is highlighted as essential for building trust among consumers and businesses. Authorities committed to remaining vigilant against anti-competitive practices, ensuring that AI technologies are developed and deployed responsibly and ethically.

The participants discussed the importance of enforcing competition laws with vigor and foresight, as AI markets are still in their early stages. By acting preemptively, competition authorities aim to prevent the entrenchment of market power and to ensure that competition remains robust as AI technologies continue to evolve. The need for tailored remedies that account for the specific dynamics of AI markets, such as network effects and data feedback loops, is acknowledged as essential to restoring competition when necessary.

The G7 competition authorities affirmed their intention to closely monitor market developments in AI and digital platforms, especially in relation to strategic partnerships and emerging market structures. Recognizing the rapid pace of technological change, they also underlined the importance of adaptive policies and regulations that keep pace with innovation while preserving the core principles of fair competition. Digital regulations and AI-specific frameworks are expected to complement traditional competition enforcement, with particular attention given to promoting access to key AI inputs, such as supercomputing capacity, which could alleviate some of the existing barriers to entry.

The communiqué also discusses the need for competition authorities to enhance their digital expertise, building the technological capabilities necessary to detect and address competition risks early. International cooperation was a recurring theme, with participants committing to sharing knowledge and best practices to stay ahead of the challenges posed by AI. The G7 members also discussed the importance of engaging with other international bodies, such as the OECD and the UN, to ensure that competition policy remains aligned with global developments in AI and digital markets.

As the G7 competition authorities look ahead to Canada's presidency in 2025, they reestablished their commitment to ongoing collaboration and knowledge-sharing as the rapidly changing digital landscape requires continuous dialogue and proactive enforcement to safeguard open, fair, and competitive AI markets.

(Source: <https://en.agcm.it/dotcmsdoc/pressrelease/G7%202024%20-%20Digital%20Competition%20Communiqu%C3%A9.pdf>, <https://www.justice.gov/opa/pr/justice-department-and-federal-trade-commission-meet-g7-enforcement-partners-rome-discuss>)

Singapore Enforces New Anti-Money Laundering Rules: Tightens Crypto Regulations to Combat Money Laundering

On 4 October 2024, the Singapore's Inter-Ministerial Committee (IMC) issued its [report](#), presenting the findings and recommendations following a comprehensive review of Singapore's Anti-Money Laundering framework. The report discusses in detail the areas of the AML system, assesses its effectiveness, and proposes improvements to strengthen Singapore's stance against money laundering activities which aim to align Singapore's regulatory measures with global best practices and ensure that the framework remains effective and responsive in emerging financial threats.

In background of this on 15 August 2023, the Monetary Authority of Singapore, in collaboration with government bodies such as the Singapore's Ministry of Finance, Singapore's Ministry of Home Affairs, Singapore's Ministry of Law, and the Singapore's Immigration and Checkpoints Authority, took steps to dismantle the money laundering network. This joint operation led to the arrest of ten individuals and the seizure of more than SG\$3 billion in assets. The case emphasized the need to strengthen Singapore's anti-money laundering framework, resulting in the establishment of the Inter-Ministerial Committee in November 2023 to review and fortify the country's defenses against financial crime.

The Inter-Ministerial Committee (**IMC**), established in November 2023, presented recommendations to strengthen Singapore's Anti-Money Laundering (**AML**) framework. These recommendations focus on three areas: Prevention, Detection, and Enforcement.

For strengthening of gatekeeper responsibilities entities such as financial institutions, corporate service providers (**CSPs**), real estate agents, and dealers in precious stones and metals are now required to conduct thorough Customer Due Diligence (**CDD**) to ensure that criminals are not able to misuse corporate structures or evade financial checks through weak oversight. The regulatory framework has also been expanded to give specific focus to bring more non-financial institutions and professionals under the AML regulatory umbrella to reduce opportunities for money laundering outside traditional financial channels. There is also an increased scrutiny on corporate structures so that companies cannot be used as shells for laundering money. The amendments to the Corporate Service Providers Act (**CSP Act**) prevent the establishment of shell companies without thorough checks.

The IMC also emphasized the importance of improving detection capabilities by enhancing data sharing and sense-making among different government agencies and has launched the Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases (**COSMIC**) platform. This platform allows financial institutions to share real-time data on suspicious individuals and transactions and creating a unified approach to detecting illicit financial activities. The IMC recommended the development of a National AML Verification Interface (**NAVIGATE**), which will facilitate cross-agency data sharing and analysis to ensure quicker detection of money laundering risks. The system will pool intelligence from various sectors to identify potential risks earlier and more effectively. The report also proposed expanding access to Suspicious Transaction Reports (**STRs**) for sector-specific agencies, such as ACRA and the Council for Estate Agencies (**CEA**).

To strengthen the enforcement front, the IMC recommended strengthening legal tools and frameworks to ensure that law enforcement agencies have the powers needed to prosecute money laundering offenses. Legislative amendments were passed under the Singapore's Anti-Money Laundering and Other Matters Act (**AMLOM Act**) in August 2024, which lowered the burden of proof in cases involving foreign criminal proceeds to streamline the prosecution process, particularly in cases involving complex, transnational money laundering schemes. The IMC also stressed the need to regularly review penalty frameworks to ensure they remain dissuasive and proportionate to the severity of the crime imposing stricter penalties on gatekeepers who fail to fulfill their AML obligations, holding them accountable for lapses in oversight.

The IMC recommended the Cross-Border Cash Reporting Regime (**CBCRR**) which proposed high penalties for undeclared cross-border cash movements and the introduction of electronic submissions for reporting designed to make it difficult for criminals to transport illicit funds across borders without detection and to serve as a deterrent against using physical cash as a method of laundering money, particularly in large sums.

To combat with Money Laundering threats, under the Singapore's Payment Services Act the cryptocurrency service providers and digital payment token service providers, which include cryptocurrency exchanges and wallet providers, are required to conduct robust Customer Due Diligence procedures, similar to those imposed on traditional financial institutions. Under Singapore's Financial Services and Markets Act, which was updated to broaden the scope of AML regulations to encompass virtual assets. Under this framework, MAS has included stablecoins within the AML/CFT regulatory perimeter and therefore stablecoins, as well as other forms of cryptocurrencies, must adhere to the same anti-money laundering measures as fiat currencies. MAS have implemented provisions that require service providers to comply with travel rule requirements which in principle obliges virtual asset service providers to ensure that information about the originator and beneficiary of cryptocurrency transactions is included and shared during a transfer.

(Source: <https://www.mas.gov.sg/-/media/mas-media-library/news/media-releases/2024/imc-report.pdf>, <https://www.mas.gov.sg/news/media-releases/2024/singapore-refreshes-the-tf-nra-and-national-strategy-for-cft>)

US CFTC Hosts Events During World Investor Week to Highlight Fraud Protection and Relationship Scams

On 4 October 2024, the United States' Commodity Futures Trading Commission (**CFTC**), through its Office of Customer Education and Outreach (**OCEO**), announced two upcoming events in observance of World Investor Week. These events are scheduled for 8 October 2024 and 9 October 2024 which aim to educate and spread awareness with the public on critical issues related to fraud protection, with a focus on emerging scams involving digital assets like cryptocurrency.

World Investor Week is an international initiative organized by the International Organization of Securities Commissions (**IOSCO**) to raise awareness about the importance of investor education and protection. From October 7 to 13, organizations from over 100 jurisdictions will come together to highlight pressing issues in investment, particularly around digital and technological advancements, crypto assets, and sustainable finance.

With the rapid growth of digital and crypto assets, fraudulent schemes have evolved, increasingly targeting unsuspecting individuals. A concerning trend is the rise of relationship investment confidence scams, often called romance investment fraud. These scams involve fraudsters building fake relationships with victims and persuading them to invest in fraudulent crypto schemes, ultimately stealing vast sums of money. Some of these scams have been traced back to organized crime syndicates abroad and have been linked to broader illegal activities such as human trafficking and money laundering.

The first event, titled Romance Investment Fraud: A Global-Scale Crypto Scam, will take place on 8 October 2024, from 12:30 p.m. to 1:30 p.m. EDT. This hybrid event will feature Dr. John Griffin, James A. Elkins Centennial Chair in Finance at the University of Texas, who will present his research, How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering. The term "pig butchering" refers to a scam where victims are "fattened up" with false promises of big investment returns, only to have all their assets stolen. The event will include a panel of federal regulators, discussing the scale of the problem, how to recognize the warning signs of these scams, and how to spread awareness to prevent further victims.

Registration for this event is free and open to the public, with in-person attendance options in Washington, D.C. and Austin, Texas, as well as virtual participation.

On October 9, 2024, at 2:00 p.m. EDT, the US CFTC will co-host a second event, a webinar titled Protect Yourself: NFA and CFTC Resources, alongside the National Futures Association (**NFA**), the self-regulatory organization for the U.S. derivatives industry. This webinar will educate participants on practical tools and resources available to protect themselves from fraud. Both events are designed to empower the public with information about how to avoid falling prey to fraudsters and how to identify high-risk individuals or schemes in the digital investment landscape.

(Source: <https://www.cftc.gov/PressRoom/PressReleases/8996-24>)

Monetary Authority of Singapore Issues Consultation Paper on Regulatory Approach for Digital Token Service Providers

On 4 October 2024, the Monetary Authority of Singapore (**MAS**) publishes a **Consultation Paper** on Proposed Regulatory Approach, Regulations and Notices for Digital Token Service Providers issued under the Financial Services and Markets Act 2022 outlining the proposed regulatory framework for Digital Token Service Providers (**DTSPs**). This new consultation paper is issued under the Singapore's Financial Services and Markets Act 2022 (**FSM Act**) which aims to ensure proper regulation of DTSPs providing services from or within the Singapore to customers inside and outside the country. The public is invited to provide feedback on these proposals, with submissions open until 4 November 2024.

The consultation paper introduces amendments to regulate the activities of DTSPs focusing on their operations abroad to prevent risks related to money laundering and terrorism financing, which are heightened in cross-border digital services. The consultation paper mandates the DTSPs to apply for a license under the FSM Act, even when they do not serve customers within Singapore so that DTSPs maintain high standards of compliance and do not harm Singapore's financial reputation.

Digital token services are defined in the FSM Act as any activity related to the transfer, storage, or trading of digital tokens. Digital tokens refer to either digital payment tokens, such as cryptocurrencies, or digital representations of capital markets products, as outlined in existing legislation. The consultation paper proposes provisions for DTSPs to comply with regulations that prevent the misuse of these digital assets for illegal purposes, including money laundering and terrorism financing. Previously, companies providing digital token services from Singapore to international customers were not subject to the same level of regulatory scrutiny as domestic services. With the proposed changes, all DTSPs, even those whose services are offered outside Singapore, must apply for a license under the FSM Act.

The application process involves demonstrating that the business model is economically viable and complies with international regulatory standards. DTSPs must appoint an executive director who is a resident in Singapore, to ensure local accountability and oversight. They are also required to maintain a permanent place of business within the country. MAS review applications on a case-by-case basis. Digital Token Service Providers are subject to licensing and ongoing requirements under the Singapore's Payment Services Act 2019 (**PS Act**), Singapore's Securities and Futures Act 2001 (**SFA**), and/or Singapore's Financial Advisor Act 2001 (**FAA**).

After receiving a license, DTSPs will need to meet ongoing regulatory requirements which includes the obligation to inform MAS of any significant changes in their business operations or model. MAS proposes that DTSPs be subjected to regular audits and be required to maintain comprehensive compliance frameworks including the appointment of compliance officers who must be suitably qualified to oversee the company's adherence to regulations.

DTSPs must implement proper governance structures to ensure that their operations are continually aligned with MAS's standards. DTSPs will be required to conduct thorough due diligence on their customers, including performing background checks and verifying the identity of both new and existing clients. In cases where DTSPs identify higher risks, such as transactions involving certain jurisdictions or anonymous customers, enhanced due diligence measures must be applied. MAS will require DTSPs to provide regular updates on any significant changes to their operations or business models. MAS proposes further amendments to the Financial Services and Markets Notices, including updates to the guidelines on reporting requirements, technology risk management, and cyber hygiene for DTSPs.

(Source: <https://www.mas.gov.sg/-/media/mas-media-library/publications/consultations/amld/2024/dtsp-consultation—final-for-publication.pdf>)

US SEC Files Market Manipulation Lawsuit Against CLS Global FZC LLC and Andrey Zhorzhes

On October 9, 2024, the United States' Securities and Exchange Commission (**US SEC**) filed a **complaint** against CLS Global FZC LLC and Andrey Zhorzhes, in the United States District Court for the District of Massachusetts, alleging a complex market manipulation scheme involving cryptocurrency assets. The SEC claims that CLS Global, which presents itself as a "market maker" for crypto assets, was, in fact, engaging in deceptive practices designed to artificially inflate the trading volume and prices of its clients' crypto assets, thereby misleading investors. Central to this case is the allegation that between August 23, 2024, and September 18, 2024, CLS Global conducted manipulative trades on the Uniswap platform, generating \$595,000 in artificial trading volume for a crypto asset known as NexFundAI, which accounted for 98% of the total trading activity during that period.

The lawsuit details how CLS Global advertised its services as offering advanced trading algorithms and market-making expertise to increase visibility and interest in its clients' assets. However, according to the SEC, what CLS Global provided was not market-making in the traditional sense but rather manipulative trading practices. These activities, including wash trading, created a false appearance of market demand for the crypto assets, tricking potential investors into believing there was significant organic interest in those tokens. Such deceptive volume inflation is crucial for new or thinly traded crypto assets to meet listing requirements on major trading platforms and to attract real investors.

The CLS Global's participation in an FBI sting operation, where the agency created a fake cryptocurrency project called NexFundAI to catch bad actors in the crypto industry. The FBI had created NexFundAI as a false token using Ethereum's ERC-20 standard and marketed it as a crypto asset that offered investment in AI projects. To further entrap CLS Global, they publicly promoted NexFundAI as an investment opportunity, fully intending to monitor how market manipulators like CLS Global would exploit it. Zhorzhes, unaware of the FBI's involvement,

negotiated a deal with the purported promoters of NexFundAI to inflate its trading volume. Under this agreement, CLS Global would generate false trading activity for NexFundAI in exchange for a monthly fee of \$4,000 paid in Tether. Between August 23 and September 18, 2024, CLS Global used 30 wallets to conduct 740 transactions, generating nearly \$600,000 in fake trading volume for NexFundAI, accounting for 98% of the total activity in that period. Believing NexFundAI to be a legitimate project, Zhorzhes and CLS Global entered discussions with individuals they thought were crypto promoters. These individuals, however, were undercover FBI agents, who deliberately orchestrated the scenario to uncover manipulation schemes. This was to be achieved through wash trading i.e. CLS Global's practice of trading the asset with itself to simulate active market participation and attract real investors.

The undercover FBI operation exposed how market makers like CLS Global deceive the public, falsely inflating the value of crypto assets and enticing real investors into purchasing what they believe to be high-demand tokens. By revealing these tactics through their sting operation, the SEC and FBI aim to clamp down on the widespread market manipulation practices plaguing the cryptocurrency industry.

The SEC alleges that this conduct violated several key provisions of U.S. securities laws, including Sections 17(a)(1) and (3) of the United States Securities Act of 1933 and Sections 9(a)(2) and 10(b) of the United States Securities Exchange Act of 1934, as well as Rule 10b-5 under the Exchange Act. These provisions prohibit fraudulent schemes in the offer, purchase, or sale of securities and bar market manipulation practices like wash trading. The SEC seeks permanent injunctions to prevent further violations, disgorgement of all ill-gotten gains, civil penalties, and an order prohibiting the defendants from participating in any securities transactions, except for Zhorzhes' personal accounts.

Jorge G. Tenreiro, Acting Chief of the Division of Enforcement's Crypto Asset and Cyber Unit (**CACU**) stated: "We remain concerned about the ease with which the market for a crypto asset can be manipulated and are committed to rooting out instances of such misconduct when it involves securities. The wrongdoers behind these schemes are profiting handsomely at the expense of investors that have been deceptively lured into these markets and lost their hard-earned savings."

(Source: <https://www.sec.gov/files/litigation/complaints/2024/comp-pr2024-166-cls.pdf>, <https://www.sec.gov/newsroom/press-releases/2024-166>)

U.S. SEC Filed a Complaint Against ZM Quant Investment Ltd. Alleging Crypto Market Manipulation and Demanding Jury Trial

On 9 October 2024, the U.S. Securities and Exchange Commission (**SEC**) filed a **complaint** against ZM Quant Investment Ltd., Baijun Ou, and Ruiqi Lau, in the United States District Court for the District of Massachusetts, alleging market manipulation of crypto assets and demanding a jury trial. In its complaint, the US SEC alleges that ZM Quant Investment Ltd. and its principals, Baijun Ou and Ruiqi Lau, manipulated crypto asset markets by artificially inflating the price and trading volume of various tokens. According to the SEC, these actions misled investors and created the illusion of robust market activity, while in reality, ZM Quant was engaging in wash trading and other manipulative practices. The SEC's complaint further outlines how ZM Quant's actions harmed market integrity and defrauded investors. The SEC seeks permanent injunctions, disgorgement of profits, civil penalties, and a ban on the defendants' participation in the securities markets, excluding personal trading.

From 2018-2023, ZM Quant advertised itself as a market maker since 2018, claiming to provide liquidity and support for over 1,100 tokens and 2,500 trading pairs. However, according to the SEC, ZM Quant was actually involved in manipulating the market for these assets by generating artificial trading volume through wash trading. Wash Trading is a manipulative method which involves buying and selling the same asset repeatedly to inflate trading volume and create the false appearance of market demand. Wash trades do not involve a change in beneficial ownership but are designed to mislead investors by suggesting that a security is actively traded.

In May 2024, ZM Quant was hired to manipulate the market for NexFundAI, a crypto asset developed as part of an FBI undercover operation. The NexFundAI team, working with the FBI, engaged ZM Quant in early 2024 to create artificial trading volume for the token. On May 31, 2024, ZM Quant generated \$4,600 in artificial trading volume for NexFundAI over a nine-hour period, accounting for 83.6% of the token's trading volume on the Uniswap platform.

From September 2021 to September 2023, ZM Quant manipulated the market for two crypto assets, Saitama and SaitaRealty, in exchange for monthly fees. In one instance, on May 26, 2023, after a warning from a trading platform about low trading volume, ZM Quant rapidly traded SaitaRealty, increasing its transaction quantity by 412,000,000,000 percent and inflating daily trading volume to billions of dollars within 24 hours.

The SEC's complaint alleges that ZM Quant and its principals violated U.S. securities laws, including the United States' Securities Act of 1933 and the United States' Securities Exchange Act of 1934.

ZM Quant is accused of engaging in fraudulent activities in connection with the offer or sale of securities in violation of Section 17(a) of the United States' Securities Act of 1933. Section 17(a) prohibits fraud, deceit, and misrepresentations in the offer or sale of securities. It has three sub-sections, with 17(a)(1) addressing the use of deceptive devices, and 17(a)(3) targeting any business practices that operate as a fraud on investors, whether intentional or negligent.

ZM Quant allegedly manipulated crypto asset prices and engaged in fraudulent trading practices, deceiving investors in violation of Section 10(b) of the United States' Securities Exchange Act of 1934 and Rule 10b-5. Section 10(b) is a broad anti-fraud provision, making it unlawful to use any manipulative or deceptive practices in connection with the purchase or sale of any security. Rule 10b-5 further prohibits any fraud or deceit, including the employment of schemes to defraud, making untrue statements, or engaging in practices that deceive investors. ZM Quant is also accused of manipulating trading volume and prices by creating artificial trading activity in certain crypto assets, thereby inducing others to trade based on false information in violation of Section 9(a)(2) of the United States' Securities Exchange Act of 1934. Section 9(a)(2) prohibits the creation of false market activity through manipulative transactions that artificially affect the price or trading volume of a security. It is designed to ensure that trading reflects genuine market interest rather than deceptive practices aimed at manipulating prices for personal gain.

The US SEC is seeking legal remedies, including Permanent Injunction, to prevent ZM Quant and its principals from continuing to engage in securities violations, the SEC is requesting a court order that permanently restrains the defendants from participating in any fraudulent activities related to securities, along with disgorgement of Ill-Gotten Gains and the US SEC is asking the court to order ZM Quant to return all profits obtained through its unlawful activities, along with prejudgment interest. The US SEC is also seeking financial penalties to punish ZM Quant for violating securities laws and to deter future misconduct and seeks ZM Quant and its principals be barred from participating in any future securities offerings, with the exception of personal transactions.

(Source: <https://www.sec.gov/files/litigation/complaints/2024/comp-pr2024-166-zm-quant.pdf>, <https://www.sec.gov/newsroom/press-releases/2024-166>)

This newsletter is for information purposes only

This newsletter and the information contained herein is not intended to be a source of advice or credit analysis with respect to the material presented, and the information and/or documents contained in this newsletter do not constitute investment advice.

Cryptocurrency markets are highly volatile and speculative in nature. The value of cryptocurrencies can fluctuate greatly within a short period of time. Investing in cryptocurrencies carries significant risks of loss. You should only invest what you are prepared to lose.

The content on this newsletter is for informational purposes only. You should not construe any such information or other material as legal, tax, investment, financial, or other advice. Nothing contained on our newsletter constitutes a solicitation, recommendation, endorsement, or offer to buy or sell any cryptocurrencies, securities, or other financial instruments.

We do not guarantee or warrant the accuracy, completeness, or usefulness of any information on this site. Any reliance you place on such information is strictly at your own risk. We disclaim all liability and responsibility arising from any reliance placed on such materials by you or any other visitor to this newsletter, or by anyone who may be informed of any of its contents.

Your use of this newsletter and your reliance on any information on the site is solely at your own risk. Under no circumstances shall we have any liability to you for any loss or damage of any kind incurred as a result of the use of the newsletter or reliance on any information provided on the newsletter. Your use of the newsletter and your reliance on any information on the site is governed by this disclaimer and our terms of use.

If you do not wish to receive this newsletter please let us know by emailing us at unsubscribe@charltonslaw.com

**CHARLTONS
QUANTUM**



Hong Kong Office

Dominion Centre 12th Floor
43-59 Queen's Road East
Hong Kong

enquiries@charltonslaw.com
www.charltonsqquantum.com
www.charltonslaw.com
Tel: + (852) 2905 7888
Fax: + (852) 2854 9596